



REFERENCIA	NOMBRE DE AUDITORIA	FECHA DE REALIZACIÓN		FECHA DEL INFORME
		INICIO	CIERRE	
A-P-GIDJ-01-20	Auditoria al proceso de Gestión Información de Defensa Jurídica del Estado	03/08/2020	04/09/2020	30/09/2020

PROCESO /AREA AUDITADA	AUDITOR LIDER / AUDITOR
Gestión de Información de Defensa Jurídica	LILIANA BARBOSA CARRILLO
EQUIPO DE AUDITORES	AUDITORES ACOMPAÑANTES
Ninguno	Ninguno

**1. OBJETIVOS:**

Evaluar el proceso de Gestión de Información de Defensa Jurídica en sus subprocesos y el Cumplimiento de controles con fin de minimizar riesgos alineados al marco regulatorio y de normatividad de la ANDJE basado en los procedimientos, planes de operación, documentación asociada y contratos establecidos.

**2. ALCANCE:**

Comprende la evaluación del proceso de Gestión de Información de Defensa Jurídica sobre las acciones del proceso adelantadas durante el periodo 1 de julio de 2019 y 31 de julio de 2020.

**3. CRITERIOS:**

- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales - <http://suin-juriscal.gov.co/viewDocument.asp?ruta=Leyes/1684507>
- Ley de Transparencia Ley 1712 de 2014 - <http://suin-uriscal.gov.co/viewDocument.asp?ruta=Leyes/1687091>
- Decreto 1069 de 2015. Decreto Único Reglamentario del Sector Justicia y del Derecho - <http://suin-juriscal.gov.co/viewDocument.asp?ruta=Decretos/30019870>
- Decreto 1008 de 2018, el cual modificó el Decreto 1078 de 2015, en su artículo 2.2.9.1.1.3 definió la seguridad de la información como principio de la Política de Gobierno Digital. - <http://suin-juriscal.gov.co/viewDocument.asp?ruta=Decretos/30019521>
- Decreto 1499 de 2017 modificó el Decreto 1083 de 2015 (Decreto Único Reglamentario del Sector de Función Pública), y adoptó el Modelo Integrado de Planeación y Gestión - MIPG. Decreto 1083 de 2015 (Función Pública) ARTÍCULO 2.2.21.5.2 Libro 2, Parte 2, Título 21, Capítulo 5.- <http://www.suin-juriscal.gov.co/viewDocument.asp?ruta=Decretos/30019891>
- Decreto Ley 4085 de 2011. Por el cual se establecen los objetivos y la estructura de la Agencia Nacional de Defensa Jurídica del Estado. <http://www.suin-juriscal.gov.co/viewDocument.asp?ruta=Decretos/1541296>
- Decreto Reglamentario 1377 de 2013 - <http://suin-juriscal.gov.co/viewDocument.asp?ruta=Decretos/1276081>
- Directiva presidencial 04 de 2018. Políticas en materia arbitral <http://www.suin-juriscal.gov.co/viewDocument.asp?id=30034913>
- Resolución 095 de febrero de 2018, por el cual se adopta el Nuevo Sistema Integrado de Gestión Institucional – SIGI – en la Agencia Nacional de Defensa Jurídica del Estado. SGS – SGSPI. [https://www.defensajuridica.gov.co/normatividad/normas-internas/resoluciones\\_2018/Lists/Resoluciones\\_2018/Attachments/3/res\\_095\\_26\\_febrero\\_2018.pdf](https://www.defensajuridica.gov.co/normatividad/normas-internas/resoluciones_2018/Lists/Resoluciones_2018/Attachments/3/res_095_26_febrero_2018.pdf)
- Marco de mejores prácticas en Tecnología alineados con COBIT 5, ITIL V3 2011 E ISO 27000:2013
- CONPES 3854 de 2016 y la Política de Seguridad Digital se desarrollan con la implementación del Modelo de Gestión de Riesgos de Seguridad Digital-MGRSD
- Circular externa 10 de 2015. Instructivo del Sistema Único de Gestión e Información Litigiosa del Estado – EKOGUI – Perfil Apoderado. - <https://www.defensajuridica.gov.co/normatividad/circulares/Lists/Circulares%202015/DispForm.aspx?ID=10&ContentTypeld=0x0100BC31D0691A776040A328A8DA6B4D40D7>



- Circular Externa No. 1 del 30 de abril de 2018. Buzones y correos electrónicos de la Agencia Nacional Jurídica del Estado y Registro de Arbitramentos públicos. -  
[https://www.defensajuridica.gov.co/normatividad/circulares/\\_layouts/15/listform.aspx?PageType=4&ListId=%7B1F143EAA%2D7D97%2D40A0%2DA751%2D768339C1339B%7D&ID=1&ContentTypeID=0x010039A91B07BED04E47863C55319FC0386B](https://www.defensajuridica.gov.co/normatividad/circulares/_layouts/15/listform.aspx?PageType=4&ListId=%7B1F143EAA%2D7D97%2D40A0%2DA751%2D768339C1339B%7D&ID=1&ContentTypeID=0x010039A91B07BED04E47863C55319FC0386B)
- Circular Externa No. 2 30 de abril de 2018. Directrices para el registro de procesos arbitrales en el nuevo módulo del Sistema Único de Gestión e Información de la Actividad Litigiosa del Estado EKOGUI.-  
<https://www.defensajuridica.gov.co/normatividad/circulares/Lists/circulares%202018/DispForm.aspx?ID=2&ContentTypeld=0x010039A91B07BED04E47863C55319FC0386B>
- Circular Externa No. 4 09 de Julio de 2018. Instructivo del Sistema Único de Gestión de Información Litigiosa del Estado EKOGUI. Perfil Jefe de Control Interno. Versión 5. -  
[https://www.defensajuridica.gov.co/normatividad/circulares/\\_layouts/15/listform.aspx?PageType=4&ListId=%7B1F143EAA%2D7D97%2D40A0%2DA751%2D768339C1339B%7D&ID=5&ContentTypeID=0x010039A91B07BED04E47863C55319FC0386B](https://www.defensajuridica.gov.co/normatividad/circulares/_layouts/15/listform.aspx?PageType=4&ListId=%7B1F143EAA%2D7D97%2D40A0%2DA751%2D768339C1339B%7D&ID=5&ContentTypeID=0x010039A91B07BED04E47863C55319FC0386B)
- Circular interna 13 de 2014. Aplicación Directiva Presidencial 04 del 11 noviembre de 2014, Políticas en materia arbitral
- Proceso, Procedimientos, políticas, guías, informes de Auditorias anteriores, Planes de Mejoramiento, Plan de Acción Institucional (PAI), Mapas de Riesgos e Indicadores.

#### 4. LIMITACIONES PARA EL DESARROLLO DE LA AUDITORIA:

Se presenta como limitación la condición de virtualidad, al desarrollar las actividades a través de trabajo en casa, como medida preventiva de cuarentena Obligatoria adoptada por el Gobierno Nacional ante la Emergencia de COVID 19.

#### 5. DOCUMENTOS EXAMINADOS:

- Mapa de riesgos generales para proceso de Gestión de Información Jurídica.
- Mapa de riesgos de Corrupción.
- Mapa de riesgos de Seguridad de la Información.
- Documento de caracterización GI-C-01 V5 Gestión de Información de Defensa Jurídica.
- GI-P-01 Procedimiento Registro de Información en el Sistema Único de Información Litigiosa del 05-02-2020 Versión 4.
- GI-P-02 Procedimiento Validación y Depuración de Información en el Sistema Único de Gestión e Información Litigiosa del Estado del 02-03-2020 Versión 3.
- GI-P-03 Procesamiento de Información en el Sistema Único de Gestión e Información Litigiosa del Estado del 21-02-2020 Versión 3
- GI-P-05 Procedimiento Auditar La Calidad De La Información A Una Muestra Estadísticamente Representativa De Procesos Judiciales del 19-02-2020 Versión 2
- GI-P-06 Procedimiento Gestionar Requerimientos Y Organizar El Requerimiento Del Sistema Único De Información Litigiosa Del Estado del 19-02-2020 Versión 1
- GI-P-07 Procedimiento Brindar Soporte Al Sistema Único De Gestión E Información Litigiosa Del Estado del 19-02-2020 Versión 2
- GI-P-08 Procedimiento Promover El Acceso, Uso Y Apropiación Al Sistema Único De Gestión E Información De La Actividad Litigiosa Del Estado del 19-02-2020 Versión 2
- GI-P-09 Procedimiento Realizar Desarrollo Y Puesta En Marcha De Los Requerimientos En El Sistema Único De Información Litigiosa Del Estado del 19-02-2020 Versión 1.
- GI-G-02 Guía De Registro De Procesos Judiciales En El Sistema eKOGUI
- GI-I-08 Instructivo de Soporte para las Entidades sobre el Diligenciamiento de Formatos para Solicitudes Masivas
- Documentación del proceso de Gestión de Información Jurídica que se encuentra en el repositorio \\srvstorage\DG1
- Documentación del proceso de Gestión de Información Jurídica que se encuentra en el repositorio [\\srvfs01\DG1\0515- Información Auditoria 2019.](#)



- Documentación de arquitectura del Sistema único de información litigiosa del Estado (eKOGUI) a través del sistema Enterprise Architect.
- Guía Administración de Riesgos Versión 3 fecha 21-09-2018
- Uso y Apropiación y Gestión de Cambio o Plan de Trabajo de Gestión de Cambio o Herramienta MantisBT o Listados de Asistencia Capacitaciones o Encuestas de Satisfacción Página web eKOGUI.
- Solicitud de información radicada No. 20191020005823.

## 6. PLAN DE MUESTREO

- Se verifica la información suministrada por correo y a través de Orfeo, por parte de los delegados de la Dirección de Gestión de Información de Defensa Jurídica, en lo referente a procedimientos, contratos y documentación asociada al sistema de información eKOGUI, se tiene en cuenta la fuente de información objeto de consulta por parte del auditor por acceso directo o a través de la solicitud al responsable del proceso.
- Se hace un levantamiento de información con los usuarios del sistema través de encuestas y/o entrevistas a los responsables asociados a los procedimientos.
- Se realizan consultas a los Sistemas de Información que soportan al proceso de Dirección de Gestión de Información.
- Se hacen seguimientos a los avances en relación con evaluaciones anteriores.

## 7. INFORME

### 7.1 FORTALEZAS

Se resalta el compromiso de todas las personas delegadas por parte de la Dirección de Gestión de Información para atender la auditoria como un asunto prioritario; así mismo se resalta su compromiso con la implementación del Sistema de Gestión Institucional para mejorar la satisfacción del usuario y demás partes interesadas.

### 7.2 CUMPLIMIENTO DE PRINCIPIOS

Esta Auditoria se desarrolló teniendo en cuenta el Modelo Integrado de Planeación y Gestión (MIPG) donde se definen siete dimensiones, las cuales articulan las 18 políticas que contempla este modelo, una de las dimensiones se llama "Control Interno" el cual se integra a través del MECI constituyéndose en el factor fundamental para garantizar de manera razonable el cumplimiento de los objetivos institucionales, también se evalúa y controla la gestión de la Agencia generando resultados que atiendan los planes de acción institucionales que buscan resolver las necesidades y problemas de los ciudadanos, con integridad y calidad en los servicios ofrecidos.

La Evaluación se llevó a cabo bajo los Lineamientos para la Administración de la Guía De administración De Riesgos identificando y gestionando los riesgos asociados al cumplimiento de los planes, programas, proyectos, metas y objetivos institucionales, donde se evidencia la Integración con los Sistemas de gestión de Calidad, el Sistema de Seguridad y Salud en el Trabajo y con el Sistema de Seguridad de la Información, también con los Riesgos de gestión, los Riesgos de Corrupción y los riesgos de seguridad digital donde la entidad asegura la ejecución de los planes y el logro de los objetivos para cumplir con la Misión y la Visión.

Uno de los principios para tener en cuenta es el enfoque basado en procesos, el cual se sustenta en los criterios básicos de Gestión de Calidad establecidos en la Norma ISO 9001:2015. La aplicación de este principio propicia una gestión articulada al interior de la entidad, e implica la aplicación de controles a cada uno de los procesos y la disposición de recursos para alcanzar los resultados esperados con el máximo de eficiencia.

### 7.3 CONTENIDO

#### 7.3.1 Evaluación del cumplimiento de las acciones enunciadas en el Proceso y de sus documentos asociados.

El proceso de Gestión de Información de Defensa Jurídica hace parte de los procesos misionales de la Entidad, definido mediante Ley 4085 de 2011 y modificado por el Decreto 2269 de diciembre de 2019, tiene como objetivo "Gestionar, Producir y Administrar la información estratégica sobre la actividad litigiosa del Estado, que apoye la toma de decisiones de los actores que intervienen en la gestión del ciclo de defensa jurídica del Estado y de otros clientes estratégicos" y lo



desarrolla a través de la Gestión del ciclo de vida del desarrollo, administración, soporte, mantenimiento, capacitación y mejoramiento continuo del sistema de información misional eKOGUI, el cual tiene como funcionalidad centralizar y gestionar el ciclo de vida de la información litigiosidad del país.

A continuación, se revisan los 8 procedimientos que integran el Proceso Gestión de Información de Defensa Jurídica y que se encuentran documentados en el Sistema Integrado de Gestión Institucional – SIGI, la revisión está orientada a validar los puntos de control existentes.

**7.3.1.1 GI-P-01 - Registro de información en el sistema único de información litigiosa**

Se hace revisión del procedimiento GI-P-01 con los expertos delegados por parte de la Dirección de Gestión de Información de Defensa Jurídica, el cual tiene como objetivo Registrar la información de procesos judiciales y conciliaciones prejudiciales en el Sistema Único de Gestión e Información Litigiosa del Estado eKOGUI. Se validan los puntos de control encontrando cumplimiento en cada uno de ellos.

En revisión de los activos de información se validó que se encuentren contenidos en la matriz de activos de información del Proceso.

Se hace solicitud de evidencia del control existente y el Proceso responde que está en actualización, por exclusión de la Instancia de Selección, las evidencias son enviadas mediante de radicado de Orfeo No. 20204000000623 y de correo electrónico de 3 de septiembre de 2020.

**Gráfica 1: Pantallazo Aplicativo Orfeo**

RADICADO	TIPO	TERC	TAMAÑO (KB)	SOLO LECTURA	CREADOR	DESCRIPCIÓN	ARCHIVADO	NUMERADO ACCIÓN
20204000000623	pdf	5	85	3	OMAR DIRCEAU TELLEZ CAMELO	Resolución de radicado 20204000000623	2020-02-04 09:30:00 AM	
2020400000062300001	pdf		4307.684	3	OMAR DIRCEAU TELLEZ CAMELO	131127 - 2	2020-02-04 09:31:07 AM	
2020400000062300002	pdf		430.787	3	OMAR DIRCEAU TELLEZ CAMELO	131127 parte 1	2020-02-04 09:31:23 AM	
2020400000062300003	pdf		202.194	3	OMAR DIRCEAU TELLEZ CAMELO	131127 parte 2	2020-02-04 09:31:45 AM	
2020400000062300004	pdf		30.183	3	OMAR DIRCEAU TELLEZ CAMELO	131127	2020-02-04 09:32:04 AM	
2020400000062300005	pdf		181.302	3	WILLIAM HERNAN DE MONTOYA	RESPUESTA FINAL EN BLANCO	2020-03-26 11:40:27 AM	

**Fuente: Reunión auditoria Procedimiento GI-P-01**

Se recomienda complementar el inventario de activos de información con los “Reportes Generados Después de Las Auditorias”

**7.3.1.2 GI-P-02 - Validación y depuración de información en el sistema único de gestión e información litigiosa del estado**

Se hace revisión del procedimiento GI-P-02 con los expertos delegados por parte de la Dirección de Gestión de Información de Defensa Jurídica, el cual tiene como objetivo Validar y depurar la información registrada en el sistema con el fin de actualizarla y generar estadísticas confiables. Se validan los puntos de control encontrando cumplimiento en cada uno de ellos.

En revisión de los activos de información se validó que se encuentren contenidos en la matriz de activos de información del Proceso.

Se recomienda complementar los activos de información agregando “los Informe de resultados de validación”.

**7.3.1.3 GI-P-03 - Procesamiento de información en el sistema único de gestión e información litigiosa del estado**



Se hace revisión del procedimiento GI-P-03 con el experto delegado por parte de la Dirección de Gestión de Información de Defensa Jurídica, el cual tiene como objetivo Generar reportes sobre el comportamiento de la actividad litigiosa del Estado para apoyar la toma de decisiones estratégicas y atender requerimientos especiales de información, quien explica la funcionalidad del Procedimiento. Se validan el punto de control que es Respuesta a requerimientos de información internos y externos Aprobados

En revisión de los activos de información se validó que se encuentren contenidos en la matriz de activos de información del Proceso.

Se tiene definida la generación y entrega de informes de litigiosidad de tipo semanal (prejudiciales y judiciales), mensual y semestral (sectorial) en formato Excel, a partir de la Información cargada y reportada por las Entidades públicas en el sistema de información eKOGUI, para conocer el estado de la litigiosidad de la Nación. Para validar su cumplimiento y tiempos de respuesta, se realizaron solicitudes de información del 22 de octubre, 30 de diciembre, 13 de enero 2019 y 2 Solicitudes internas. El Proceso contestó a través de correo electrónico del 28 de agosto de 2020.

#### **7.3.1.4 GI-P-05 - Auditar la calidad de la información a una muestra estadísticamente representativa de procesos judiciales**

Se hace revisión del procedimiento GI-P-05 con los expertos delegados por parte de la Dirección de Gestión de Información, Comparar y evaluar la información suministrada por las entidades y organismos del orden nacional en el Sistema Único de Gestión e Información de la Actividad Litigiosa del Estado con respecto a la información de Rama Judicial. Se validan los puntos de control encontrando cumplimiento en cada uno de ellos.

En revisión de los activos de información se validó que se encuentren contenidos en la matriz de activos de información del Proceso.

Se recomienda actualizar la política de operación en el sentido de que no depende de la Dirección sino de asignación de recursos "Las actividades de este procedimiento se realizan una sola vez al año; se planea en el último trimestre del año y la ejecución va hasta el segundo trimestre del siguiente año. En caso de que se requiera de acciones de mejora, se llevarán a cabo siguiendo el procedimiento Acciones preventivas, correctivas y de mejora-MC-P-01" Esta recomendación es atendida dentro de la Auditoría y se aportan los correos de gestión de fecha 4 de septiembre realizada ante la Oficina de Planeación para hacer esta actualización.

#### **7.3.1.5 GI-P-06 - Gestionar requerimientos y organizar el requerimiento del sistema único de información litigiosa del estado**

Se hace revisión del procedimiento GI-P-06 con los expertos delegados por parte de la Dirección de Gestión de Información, el cual tienen como objetivo, Elaborar la documentación y el entendimiento técnico de los requisitos y coordinar las actividades para organizar y priorizar los mismos. Se validan los puntos de control encontrando cumplimiento en cada uno de ellos.

Se solicita acta y línea de entregable de un proyecto de 2019 dado que para 2020 no se han ejecutado proyectos de desarrollo, el Proceso respondió a través de correo electrónico de 2 de septiembre de 2020

En revisión de los activos de información se validó que se encuentren contenidos en la matriz de activos de información del Proceso.

#### **7.3.1.6 GI-P-07 - Brindar soporte al sistema único de gestión e información litigiosa del estado**

Se hace revisión del procedimiento GI-P-07 con los expertos delegados por parte de la Dirección de Gestión de Información, el cual tienen como objetivo Recibir, gestionar, solucionar y responder las solicitudes realizadas por los usuarios frente al Sistema Único de Gestión e Información Litigiosa del Estado eKOGUI. Se validan los puntos de control y se hacen las siguientes recomendaciones:

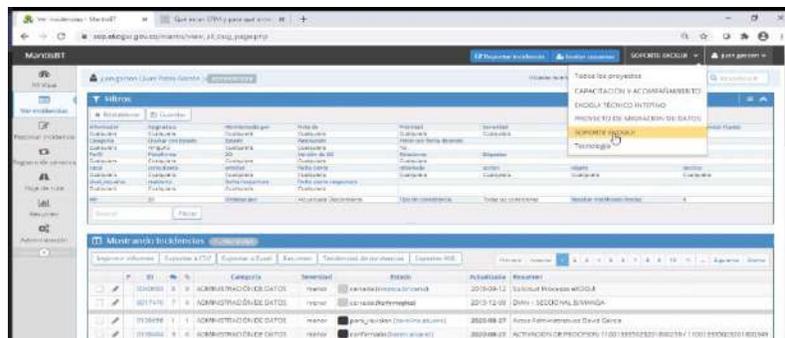
- Se recomienda crear una constancia de envío de correo de notificación de respuesta al usuario final

- Se recomienda conocer los resultados o crear encuestas de satisfacción frente al servicio recibido por parte de la mesa de ayuda, sistema EKOGUI
- Se recomienda definir un control para casos que superen los definidos dentro del procedimiento, se detectó un caso abierto por más de 1 mes.
- Se hace la observación frente a la necesidad de generar un control para medir los Tiempos de Respuesta de Servicio, temporalidad para la solución de los casos, importante definir estándares o políticas de desempeño y calidad de autoevaluación en el procedimiento.

Se hace revisión de los activos de información validando que se encuentren contenidos en la matriz de activos de información del Proceso

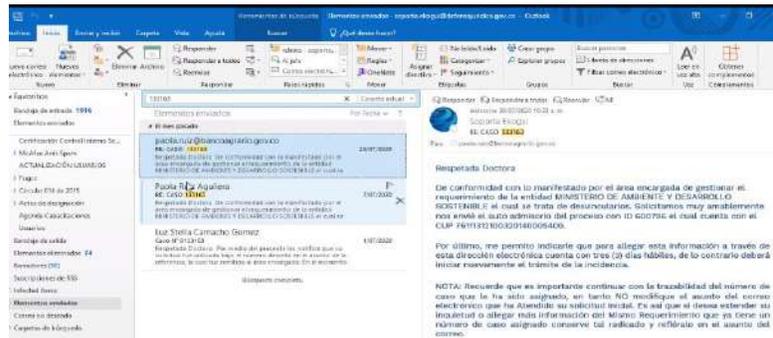
Se revisó la funcionalidad de la herramienta MANTIS a través de la cual se hacen los registros y seguimientos de las solicitudes realizadas.

Gráfica 2: Pantallazo Aplicativo Mantis



Fuente: Reunión auditoria Procedimiento GI-P-07

Gráfica 3: Pantallazo correo gestión de solicitudes Mantis



Fuente: Reunión auditoria Procedimiento GI-P-07

### 7.3.1.7 GI-P-08 - Promover el acceso, uso y apropiación al sistema único de gestión e información de la actividad litigiosa del estado

Se hace revisión del procedimiento GI-P-08 con los expertos delegados por parte de la Gestión de Información de Defensa Jurídica, el cual tiene como objetivo Gestionar el cambio del Sistema Único de Información Litigiosa del Estado entre sus diferentes usuarios. Se revisó la funcionalidad del procedimiento, validamos la utilización de los formatos, las encuestas y los informes generados en relación con las capacitaciones en el Sistema Único de Gestión e Información Litigiosa del Estado diligenciadas se verificó:

- GD-F-18 Formato verificación de asistencia
- GI-F-13 Formato encuesta de satisfacción de usuarios del servicio de capacitación en el Sistema Único de Gestión e Información Litigiosa del Estado diligenciadas



- Acta y documento de recomendaciones
- Boletines, noticias y actualización al portal
- Actualización de tutoriales y curso virtual

Se hace revisión de los activos de información validando que se encuentren contenidos en la matriz de activos de información del Proceso y se recomienda complementar con el Plan de trabajo.

#### **7.3.1.7 GI-P-09 - Realizar desarrollo y puesta en marcha de los requerimientos en el sistema único de Información**

Se hace revisión del procedimiento con los expertos delegados por parte de la Dirección Gestión de Información de Defensa Jurídica, el cual tiene como objetivo Realizar el desarrollo de los requisitos y realizar las pruebas correspondientes hasta su correcta operación y puesta en producción. Se revisó la funcionalidad del procedimiento y para ello se solicita:

Línea de entregable de un proyecto de 2019 dado que para 2020 no se han ejecutado proyectos de desarrollo, el Proceso respondió a través de correo electrónico de 2 de septiembre de 2020

Gestión de usuarios realizada la solicitud de permisos de acceso se gestiona a través de la mesa de servicios del Proceso Gestión de Tecnología de la Información, quienes establecen los controles de acceso a la información requerida. Proceso dio respuesta a través de correo electrónico de 31 de agosto de 2020

Contingencia del Proceso para el sistema EKOGUI. Actualmente, se realiza por parte de la Dirección de Gestión de Información Backup de bases de datos diariamente, teniendo en cuenta que el eKOGUI cuenta con un repositorio de archivos en red, proporcionado por el proceso de Gestión de Tecnología de la Información. Este repositorio centraliza la información generada, procesada, transformada y extraída del por la Dirección de Gestión de Información. Evidencias a través de correo electrónico de 4 de septiembre de 2020

Se hace revisión de los activos de información validando que se encuentren contenidos en la matriz de activos de información del Proceso y se recomienda Incluir en activos de información el Código fuente.

#### **7.3.2 Riesgos asociados al Proceso, Corrupción y de Seguridad de la Información**

Se realiza la verificación de los riesgos establecidos por el Proceso Gestión de Información de Defensa Jurídica de Gestión, corrupción y seguridad de la Información basados en la Guía Administración De Riesgos generada por la Entidad, así:

##### **7.3.2.1 Riesgos de Proceso:**

###### **• Incumplimiento Del Plan De Desarrollo Del Sistema - Controles**

- Seguimiento a las Rutas de Trabajo definidas en el Plan de Desarrollo del Sistema
- Gestionar requerimientos y organizar el proyecto del sistema único de información litigiosa del estado GI-P-06.
- Procedimiento realizar desarrollo y puesta en marcha de los requerimientos en el sistema único de información litigiosa del estado GI-P- 09.
- Procedimiento realizar mantenimiento al sistema único de información litigiosa del estado GI-P-10.

Se validan los controles de proyectos realizado en 2019 dado que en 2020 no se han iniciado los proyectos de desarrollo en 2020

###### **• Perdida de imagen de la agencia ante las entidades usuarias del sistema. - Controles**

- Procedimiento gestionar requerimientos y organizar el proyecto del sistema único de información litigiosa del estado GIP06.
- Usuario Customer Management Services control de tráfico telefónico
- Procedimiento brindar soporte al sistema único de gestión e información litigiosa del estado GIP07



- Procedimiento realizar mantenimiento al sistema único de información litigiosa del estado GIP10. NO está
- Acuerdos de Niveles de Servicio ANS definidos

Se verifican los controles en los Estudios previos de los Contratación del Contac Center y el soporte al eKOGUI. Ajustándose a los objetivos del Proceso.

• **Registro de información errónea y o incompleta. - Controles**

- Procedimiento registro de información en el sistema único de información litigiosa GI-P-01

Se verifican los puntos de control definidos en el Procedimiento.

• **Generar información inconsistente. - Controles**

- Procedimiento procesamiento de información en el sistema único de gestión e información litigiosa del estado - GI-P-03
- Sistematización de procedimientos y optimización de la operación
- Protocolo generación reporte sectorial GIPT01
- Protocolo generación reporte mensual GIPT02
- Protocolo generación reporte semanal GIPT06

**Gráfica 3: Pantallazo Revisión trimestral**

Estuve revisando las cifras contrastando trimestral, sectorial y mensual entidades, las siguientes fueron las verificaciones que realice:

- (En este punto está concordando trimestral y sectoriales) Comparando las cifras en el insumo que utilice para montar el sharepoint de los sectoriales, en relación al Top por procesos.

Bases Sectoriales junio 2020 - Excel

cod_entid	entidad agrupada	procesos	part%	preten
405	ADMINISTRADORA COLOMBIANA DE PENSIONES	111.027	94,91%	\$3.652.457.092.813
356	FONDO DE PRESTACIONES SOCIALES DEL MAGISTERIO	61.033	89,04%	\$2.185.745.379.384
426	DIRECCION EJECUTIVA DE ADMINISTRACION JUDICIAL - NIVEL CENTRAL	23.726	65,47%	\$28.797.211.013.618
124	MINISTERIO DE DEFENSA NACIONAL	22.760	44,21%	\$49.834.948.504.207
433	UNIDAD ADMINISTRATIVA ESPECIAL DE GESTION PENSIONAL Y CONTRIBUCIONES PARAFISCALES DE LA PRO	22.744	49,56%	\$3.153.789.981.080
232	FISCALIA GENERAL DE LA NACION	21.628	59,68%	\$40.064.983.266.437
125	DIRECCION GENERAL DE LA POLICIA NACIONAL	20.531	39,88%	\$82.255.919.651.477
157	LA PREVISORA S.A. COMPANIA DE SEGUROS	7.554	16,46%	\$8.535.919.407.485
309	DIRECCION DE IMPUESTOS Y ADUANAS NACIONALES - DIAN	7.014	15,28%	\$26.548.659.047.054
114	CAJA DE RETIRO DE LAS FUERZAS MILITARES	6.913	13,43%	\$12.940.643.432.042



• (En este punto está concordando trimestral y sectoriales) Comparando las cifras en el insumo que utilice para montar el sharepoint de los sectoriales, en relación al Top por pretensiones.

**Fuente: Reunión auditoria Riesgos de Gestión**

Se validan los controles de generación de reportes. Ajustándose al objetivo del Proceso

### 7.3.2.2 Riesgos de CORRUPCIÓN

#### • Filtración de información estratégica, sensible y confidencial en favor de un tercero. - CONTROLES

- Controles de acceso al sistema con diferentes perfiles (Manual de usuarios)
- Cláusulas de confidencialidad en la información en los contratos
- Políticas de seguridad de la información.
- Módulo de auditoría de registro de usuarios.
- Mecanismos de trazabilidad de peticiones a través de Access Log e info log.
- Cláusula de Obligaciones Generales 7 y 8.
- DEMO01 Modelo Optimo de Gobierno de Información

#### • Registro de información en el sistema eKOGUI falsa o alterada por parte de los usuarios que ingresan y actualizan información en el sistema para favorecer un tercero. -CONTROLES

- GIP02 Validación de la información en el sistema único de gestión e información de la actividad litigiosa del estado.
- GIP01 Registro de información en el sistema único de información litigiosa.
- Controles de acceso al sistema con diferentes perfiles (Manual de usuarios).
- Auditorías automáticas del sistema.
- Mecanismos de trazabilidad de peticiones a través de Access Log e info log.
- GIP05 Auditar la calidad de la información a una muestra estadísticamente representativa de procesos judiciales

Se hacen una revisión de las evidencias correspondientes a los controles establecidos por el Proceso para los riesgos de Gestión y de Corrupción.

En la validación no se encuentra evidencia de reporte mensual de controles en el Sistema Integrado de Gestión Institucional – SIGI, como se establece en, la Guía de Administración de Riesgos en su Numeral 10 Gestión Y Corrupción 10. Seguimiento. *El líder del proceso realizará mensualmente el seguimiento, registrando los resultados de cada una de las actividades desarrolladas con el soporte correspondiente (acta, correo) etc., tanto en físico como en digital en la herramienta del Sistema Integrado de Gestión Institucional – SIGI.*



No se evidencia el detalle del cumplimiento del control DE-MO-01 Modelo Optimo de Gobierno de Información, definidos para mitigar el Riesgo de Corrupción, Filtración de información estratégica, sensible y confidencial en favor de un tercero. Guía Administración de Riesgos - Consideración para el Sistema de Gestión de Seguridad de la Información Tratamiento del Riesgo, El líder del proceso (dueño del riesgo) con el apoyo del profesional del SGSI, debe describir las acciones y el tiempo en que realizara el tratamiento para cada riesgo identificado. Seguimiento al Tratamiento del Riesgo. El responsable del Sistema de Gestión de Seguridad de la Información con el apoyo del profesional del SGSI, solicitara trimestralmente al líder del proceso (dueño del riesgo) los avances y evidencias de los tratamientos de los riesgos a cargo de su gestión.

Es preciso que el Proceso valide este control, dado que dentro del Modelo Optimo de Gobierno de Información se registra que La Dirección de Gestión de Información participa en las cuatro categorías de gestión:

- Gestiona el Sistema eKogui integralmente.
- Gestiona información producida por diferentes áreas de la Agencia y en especial aquella producida por otras entidades a través del CDJE.
- Crea nuevos activos de información y los gestiona para su utilización por parte de otras entidades interesadas y otras áreas de la Agencia.
- Gestiona el ciclo de vida de los datos registrados en el sistema eKogui.

Adicionalmente no se evidencia la propuesta y la actualización permanente del Modelo Optimo de Gobierno de Información que se encuentra publicado en Sistema Integrado de Gestión Institucional – SIGI. Este modelo designa los siguientes responsables **MODELO ÓPTIMO DE GOBIERNO DE INFORMACIÓN 2.5.2 Asignaciones específicas de responsabilidad en la Agencia-2.5.2.4 Oficina Asesora de Planeación La Oficina Asesora de Planeación se encarga de la creación y actualización permanente del Modelo de Gobierno de Información - MOGI. Y 2.5.2.6 Proceso de Gestión de Tecnologías de la Información - Proponer el Modelo de Gobierno de Tecnologías de la Información.**

Gráfica 4: Pantallazo correo gestión de solicitudes Mantis

Riesgo	Descripción	Nivel	Medidas	Nivel	Acción	Indicador	Acción	Fecha Inicio	Fecha Fin	Indicador	Responsable	E Avance
Gestión	INCUMPLIMIENTO DEL PLAN DE DESARROLLO DEL SISTEMA	EXTREMA	Seguimiento a las Rutas de organizar el proyecto del desarrollo y puesta en marcha mantenimiento al sistema	BAJA	1. Redefinición de las líneas base del sistema							
	PERDIDA DE IMAGEN DE LA AGENCIA ANTE LAS ENTIDADES USUARIAS DEL SISTEMA	EXTREMA	procedimiento gestionar Management Services control soporte el sistema único de mantenimiento al sistema Servicio ANS definidos de necesidades	ALTA	Reducir el riesgo							
Gestión	Registro de información errónea y/o incompleta.	EXTREMA	información en el sistema	MODERADA	Reducir el riesgo							
	Generar información inconsistente.	ALTA	de información en el sistema procedimientos y optimización sectorial GIPT01 Protocolo	MODERADA	1. Realizar corrección e informar a los							
Corrupción	Filtración de información	EXTREMA	sistema con diferentes perfiles (Manual de usuarios)	MODERADA	Reducir el riesgo							
	Registro de información en	EXTREMA	sistema con diferentes información en el sistema	BAJA	Reducir el riesgo							

Fuente: Sistema de Información de Gestión Institucional - SIGI

### 7.3.2.3 Riesgos de seguridad de la Información

El riesgo definido por la Dirección de Gestión de Información es *“Posible pérdida, modificación o fuga de información de las carpetas compartidas de DGI, debido a falta de un lineamiento para establecer los permisos de accesos y uso a estas carpetas. afectando Confidencialidad, Integridad y Disponibilidad de la información”.*

Gráfica 5: Mapa de Riesgos de Seguridad de la Información



4. VALORACIÓN DEL RIESGO						
DESCRIPCIÓN DE LOS CONTROLES	PROBABILIDAD	IMPACTO	NIVEL	OPCIONES DE TRATAMIENTO	CONTROLES MÁS EFECTIVOS A IMPLEMENTAR	
<p>Control:</p> <p>CONTROL: No existe RESPONSABLE: No existe RECURSOS: No existe PROCESO DE CONTROL: No existe AUTORIZACIÓN DEL CONTROL: No existe DOCUMENTACIÓN: No existe SUSCRIPCIÓN DEL CONTROL: NO EXISTEN CONTROLES.</p>	IMPROBABLE	<p>Impacto</p> <p>MODERADO</p> <p>-Afectación Riesgo del proceso Nivel de la Entidad. - Sanciones y/o multas a nivel de Control Interno para el Proceso. - Llamadas de atención a nivel Directivo.</p>	MODERADO	Reducir el Riesgo	Definir y administrar controles de niveles acceso de las carpetas compartidas de DGI.	

5. TRATAMIENTO DEL RIESGO					6. SEGUIMIENTO AL TRATAMIENTO DEL RIESGO		
CONTROLES ASOCIADO A: (NO. FOLIO) DEL	ACCIONES (PIMA)	FECHA INICIO	FECHA TERMINACIÓN	RESPONSABLE	TRIMESTRE (Enero, Mayo)	TRIMESTRE (Ago, Enero)	TRIMESTRE (Julio, Septiembre)
Control: ISO 27001	<p>Plan:</p> <p>P. Definir la manera de solicitar los permisos de control de acceso. R. Diligenciar la matriz de control de acceso. V. Verificación de la matriz diligenciada. A. Seleccionar la aplicación de permisos de acceso a Gestión de tecnología.</p>	<p>SEPTIEMBRE-25-2016</p> <p>SEPTIEMBRE-25-2016</p> <p>NOVIEMBRE-2016</p> <p>NOVIEMBRE-2016</p>	<p>SEPTIEMBRE-27-2016</p> <p>OCTUBRE-31-2017</p> <p>NOVIEMBRE-11-2016</p> <p>NOVIEMBRE-18-2016</p>	<p>ANIBICA MARIN-DEFOR DGI</p>			

Fuente Pagina Web Intranet

**Controles definidos**

- Definir y administrar controles de niveles acceso de las carpetas compartidas de DGI.
- A.9.1. Requisitos del Negocio para Control de Acceso.
- A.9.1.1. Política de Control de Acceso.
- A.9.2. Gestión de Acceso de Usuarios.
- A.9.2.1. Registro y cancelación del registro de usuarios.
- A.9.2.2. Suministro de acceso de usuarios.
- A.9.2.3. Gestión de derechos de acceso privilegiado.

Al realizar una verificación del seguimiento hecho por parte del Proceso a los riesgos de seguridad se evidencia que el Proceso no cuenta con una herramienta para hacer seguimiento a los riesgos de seguridad de la información. Situación que desatiende lo consignado en la Guía Administración de Riesgos - Consideración para el Sistema de Gestión de Seguridad de la Información. Tratamiento del Riesgo, El líder del proceso (dueño del riesgo) con el apoyo del profesional del SGSI, debe describir las acciones y el tiempo en que realizara el tratamiento para cada riesgo identificado. Seguimiento al Tratamiento del Riesgo. El responsable del Sistema de Gestión de Seguridad de la Información con el apoyo del profesional del SGSI, solicitara trimestralmente al líder del proceso (dueño del riesgo) los avances y evidencias de los tratamientos de los riesgos a cargo de su gestión.

Al realizar una verificación del seguimiento hecho por parte del Proceso a los riesgos de seguridad no se evidencia una herramienta para hacer este seguimiento, la responsabilidad de la gestión de riesgos de seguridad de la información en la Agencia definida en el *Manual de Políticas de Gestión y Desempeño Institucional de la Agencia* es de la Dirección de Gestión de Tecnologías de Información

En la revisión realizada no se evidencia el registro de los Riesgos de seguridad digital, en los cuales se incluyan riesgos para activos de tipo aplicaciones, servicios, servicios Web, redes, información física o digital, Tecnologías de la Información TI- o Tecnologías de la Operación -TO-, información, hardware, software, servicios y recurso humano, desde el punto de vista de la confidencialidad, la integridad y disponibilidad situación que va en contravía con la Guía Administración de Riesgos la cual en su metodología afirma que combina elementos de la Norma Técnica Colombiana NTC-ISO 31000 y la Guía para la Administración del Riesgo del Departamento Administrativo de la Función Pública. Anexo 4 Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas y Guía Roles y Responsabilidades del MSPi - la cual cita: de la Estrategia de Gobierno Digital del MINTIC. *La identificación y valoración de activos debe ser realizada por la Primera Línea de Defensa – Líderes de Proceso, en cada proceso donde aplique la gestión del riesgo de seguridad digital, siendo debidamente orientados por el responsable de seguridad digital o de seguridad de la información de la entidad pública.*

**7.3.3 Activos de información**

Se evaluó el registro de activos de información de la Dirección Gestión de Información de Defensa Jurídica, tomando como guía la Norma técnica ISO 27001 Gestión Integral de la Seguridad de la Información y El Decreto reglamentario 1081 de 2015 que señala el Registro de Activos de Información (Artículo 2.1.1.5.1.1) como uno de los instrumentos de gestión de información.

**Gráfica 5: Gestión integral de la seguridad de la información**



Fuente ISO 27001 Gestión integral de la Seguridad de la Información - SGSI

**Tabla 1. Activos de información Proceso Gestión de Información**

Nombre del Activo de Información	Descripción del Activo de Información	Valor estratégico	Tipo de activo	Procedimiento
Registros de Tutelas	Documento que contiene los registros de tutelas ingresados por Orfeo para realizar gestión interna en la Agencia.	4,57	Información	GI-P-01 - Registro de información en el sistema único de información litigiosa
Arbitramiento	Documento que contiene la información referente a trámites arbitrales reportados por las entidades a la Agencia para contribuir a la toma de decisiones de la Agencia.	4,02	Información	GI-P-01 - Registro de información en el sistema único de información litigiosa
Reportes sobre la Actividad Litigiosa del estado	Reportes que genera la Dirección de Gestión de Información a partir de registros de trámites judiciales en el Sistema eKOGUI y otras herramientas ofimáticas para apoyar la toma de decisiones de los actores que intervienen en la gestión del ciclo de defensa jurídica del estado.	3,62	Información - TRD	GI-P-03 - Procesamiento de información en el sistema único de gestión e información litigiosa del estado
Documento códigos de Programación de los reportes de información	Documentos que contienen el detalle de los códigos de programación de los reportes en el aplicativo SAS	4,09	Software	GI-P-03 - Procesamiento de información en el sistema único de gestión e información litigiosa del estado
Consultas diarias de procesos judiciales y conciliaciones extrajudiciales registradas en el sistema.	Documento que contiene la Información extraída del sistema eKOGUI previa a un proceso de depuración para su consulta diaria.	0,57	Información	GI-P-01 - Registro de información en el sistema único de información litigiosa
Informes Actividad Litigiosa del Estado	Documento que contiene los informes periódicos de la actividad litigiosa del Estado, por sectores administrativos para brindar información a las cabezas de cada sector.	3,76	Información - TRD	GI-P-03 - Procesamiento de información en el sistema único de gestión e información litigiosa del estado
Reportes Generados por el Sistema eKOGUI	Reportes que se han dispuesto para los usuarios con el fin de exportar la información registrada en el sistema correspondiente a la actividad litigiosa del estado con el fin de brindar información estadística a los interesados.	4,46	Servicio	GI-P-03 - Procesamiento de información en el sistema único de gestión e información litigiosa del estado



Base de datos Migración de información de la actividad litigiosa del estado	Base de datos que contiene la información registrada en el sistema eKOGUI mediante la solicitud de una migración masiva para mantener actualizada esta información en el sistema.	2,84	Software	GI-P-07 - Brindar soporte al sistema único de gestión e información litigiosa del estado
Documento encuesta Ciclo de Defensa Jurídica	Documento que contiene la Encuesta publicada en la página de la ANDJE, diligenciada por las entidades. La información recopilada se emplea para calcular indicadores para el BID.	3,54	Información	GI-P-08 - Promover el acceso, uso y apropiación al sistema único de gestión e información de la actividad litigiosa del estado

**Fuente Pagina Web Intranet**

Se valida el registro de activos de información identificando los campos requeridos en el Decreto 1081 de 2015 como lo son: Categorías o Series, Descripción Información, Medio de conservación y/o soporte, Información disponible o publicada, Nombre o título de la información, Idioma y Formato.

Así mismo se revisan los productos de cada uno de los 8 Procedimientos y se recomienda lo siguiente:

- Gestionar los activos de información, dado que son prerrequisito para la gestión de riesgos de seguridad de la información para poder tenerlos en cuenta al momento de la creación de la matriz de riesgos de seguridad Digital.
- Los activos catalogados como críticos, los cuales requieran un alto grado de disponibilidad deben estar contemplados en el alcance de la gestión de la continuidad del negocio.
- Cada vez que se reconozca un nuevo activo de información o se genere un cambio en alguno existente se recomienda realizar una revisión del riesgo para dicho activo, contemplando por cada activo su impacto, vulnerabilidades y amenazas, controles asociados, riesgo inherente y residual, con el fin de establecer planes de tratamiento por cada activo adecuado en el marco de la norma ISO 27001.

**7.3.4 Planes de Mejoramiento**

En revisión de las evidencias aportadas en los seguimientos a los planes de mejoramiento suscritos por parte de la Dirección de Gestión de Información se encontró:

**Tabla 2. Planes de mejoramiento Proceso Gestión de Información**

Hallazgo	Validación de Acción propuesta por la DGI
Acción Numero 286: Se evidenció en el procedimiento GI-P-10 V-1 realizar mantenimiento al Sistema Único De Información Litigiosa Del Estado los formatos gi-f-26 v-0 formato guía funcional usuario gi-f-27 v-0 formato diccionario de campos gi-f-29 v-0 formato de especificación de caso de prueba gi-f-30 v-0 formato especificación funcional Los cuales fueron dados de baja sin realizar la actualización del procedimiento y correspondiente notificación a la Oficina Asesora de Planeación.	Se eliminó el procedimiento y se incluyeron estas actividades en el procedimiento GI-P-9
Acción Numero 287: Se evidenció que el proceso de Gestión de Tecnologías no realiza el envío de copias de seguridad a custodia externa con una periodicidad definida, teniendo en cuenta que la evidencia presentada en la carpeta física relaciona los dos (2) últimos envíos de medios el 06 de junio de 2019 y el 12 de octubre de 2018 al proveedor Alpopular quien realiza la custodia de los medios.	Envío de copias evidencia fecha y periodicidad
	Se actualizo la guía GTI-G-06 en el ítem 4.2.5 CUSTODIA DE BACKUP Y PERIODICIDAD La entrega de los medios de cinta con la información respaldada, donde se priorizará la información de los sistemas misionales, será entregada antes del día 20 de cada mes al tercero con el cual se tenga contrato de almacenamiento y custodia de estos medios. Los envíos a custodia de información se realizan antes del día 20 de cada mes. Se adjuntas soportes de los últimos 3 meses.
Acción Numero 288: No se evidenció en el proceso de Gestión de Tecnologías restauraciones de servidores y/o información de ambientes productivos del sistema de información EKOGUI, que permitan garantizar el funcionamiento óptimo de las copias de seguridad realizadas a través del sistema de información Nevault.	Se desarrolla actividad de restauración en sistema de contingencia del sistema EKOGUI- Se ejecuta DRP de la plataforma EKOGUI 2 en el Centro de Datos de apoyo.



<p>Acción Numero 289: No se evidenció en el sistema de información Orfeo el uso de las subseries 5 Controles de cambio a los requerimientos en el sistema eKOGUI de la serie 37 Administración Sistema de información y las subseries 3 Migración y 4 Plan de vigilancia de la serie 38.</p>	<p>La DGI, se realizó una entrega de documentos físicos y digitales en los meses de noviembre y diciembre a gestión documental, en lo relacionado a las subseries 5 Controles de cambio a los requerimientos en el sistema eKOGUI de la serie 37 Administración Sistema de información y las subseries 3 Migración y 4 Plan de vigilancia de la serie 38. Para tal fin, se adjuntan como soporte: Reporte entregado por gestión documental de la organización de los documentos entregados.</p>
<p>Acción Numero 290: Se evidenció que los activos de información del proceso de Dirección de Gestión de Información presentados, difiere de la información publicada en la Intranet de la Entidad. Lo cual no permite a la Oficina de Control Interno determinar cuál es la versión más actualizada.--&gt;Se realizara un repositorio único</p>	<p>Se verificó el nuevo registro de activos el cual cumple con los requisitos del Decreto reglamentario 1081 de 2015</p>
<p>Acción Numero 291: La falta de convenios impide el establecimiento de compromisos para mantener actualizada la información en el sistema eKOGUI, entre la Agencia y las entidades que más litigiosidad tienen, lo que ocasiona que ésta no sea confiable, efectiva y oportuna para prevenir el daño antijurídico. Inobservancia del principio 6 de la ley 489 de 1998 Principio de coordinación.</p>	<p>Se hace validación de las evidencias frente a las acciones propuestas.</p>

Se revisaron las evidencias frente a las acciones No. 286, 287, 289,290 y 291 en donde se validó el cumplimiento y la efectividad de las acciones propuestas.

Frente a la Acción Numero 288: Se evidencia que el proceso de Gestión de Tecnologías de información realizó la actividad de restauración en sistema de contingencia del sistema EKOGUI, se ejecutó DRP de la plataforma EKOGUI 2 en el Centro de Datos de apoyo, sin embargo, no se evidencia un Plan de Recuperación de desastres - DRP que vincule a los expertos o delegados de la DGI en este procedimiento, no se aporta evidencia de plan de pruebas, capacitación, mejoramiento y mantenimiento de este. Adicionalmente el documento no cuenta con la aprobación de la alta dirección, incumpliendo lo establecido en el Modelo de Seguridad y Privacidad de la Información (MSPI), Guía No. 10 Continuidad del negocio.

El DRP según lo establecidos por MINTIC en la Guía de Continuidad del negocio, basado en la gestión del riesgo, debe contemplar la valoración del riesgo, la apreciación de su impacto en el negocio y la posibilidad de ocurrencia, este Plan debe contemplar al menos los siguientes aspectos:

- Gobierno: roles y responsabilidades definidas para la administración del DRP involucrando a la alta gerencia.
- Asociación de las plataformas y requerimientos tecnológicos acorde con la definición de los procesos críticos para continuidad del negocio de la Agencia de acuerdo con unos criterios estratégicos y con evaluación de su impacto en la operación en caso de no estar disponibles.
- Análisis de riesgos de tecnología.
- Asociación con los resultados de los Análisis de impacto al negocio, donde se identifique para la tecnología relacionada con cada proceso crítico lo siguiente: tiempo objetivo de recuperación (RTO) y punto objetivo de recuperación (RPO).
- Definición de estrategia de tecnología: acorde con los resultados del análisis de riesgo y análisis de impacto al negocio la organización debe seleccionar e implementar una estrategia de tecnología que permita dar cubrimiento a los aspectos identificados.
- Definición del plan de recuperación de desastres (DRP) donde se indiquen las acciones antes, durante y después de un evento de desastre o crisis para puesta en marcha de la estrategia de DRP definida.
- Plan de pruebas: donde se definan pruebas y simulacros controlados de situaciones de desastre para probar la eficiencia del sistema
- Plan de capacitación y sensibilización del DRP para los empleados y actores involucrados.
- Mejoramiento y mantenimiento del DRP.

**7.3.5 Cumplimiento a indicadores (PAI, PAAC y Gestión)**

**Tabla 3: Indicadores PAI Proceso Gestión de Información**

PAI 2020 DGI	TECNOLOGIA
100% del plan de actividades (2 hitos definidos) para actualizar la información registrada en EKOGUI, implementado	



100% del plan de actividades (3 hitos definidos) para el aumento en el registro de condenas	
65% de avance en actividades del proyecto de acompañamiento para la explotación y actualización de información en 17 entidades intervenidas	
Funcionalidad para calcular e incluir campo de provisión contable sugerida en el módulo de actualización de judiciales implementada	XX
100% de los datos priorizados que se encuentran duplicados y con inconsistencias, depurados	
3 informes al nivel directivo de entidades con cifras de la evolución de la problemática litigiosa	
9 informes de evolución de litigios por entidad y tipo de acción, reportados	
2 análisis a partir de la información de EKOGUI desarrollados	
100% del plan de actividades (2 hitos definidos) para el desarrollo de una base de datos de litigios territoriales, desarrollados	XX
100% del plan de actividades (4 hitos definidos) para el desarrollo de 2 cubos multidimensionales para consultas dinámicas de procesos de judiciales y arbitramentos, desarrollado	XX
12 reportes de medición del indicador de Estabilización de EKOGUI, realizados	
126 eventos de capacitación para el uso del EKOGUI, desarrollados	
100% del plan de actividades (3 hitos definidos) para el desarrollo de implementaciones evolutivas, desarrollado Se modifica la meta pasando de 4 hitos a 3 hitos, así mismo se eliminan los entregables de mayo y junio	XX
2 herramientas implementadas para el fortalecimiento del Uso de EKOGUI	
100% del plan de actividades (3 hitos definidos) para el desarrollo del Módulo de calidad de datos, implementado	XX
100% del plan de actividades (3 hitos definidos) para la especificación del Módulo de extrajudicial, implementado	XX
11 reportes de registro y auditoría de tramites notificados	
100% del plan de actividades (3 hitos definidos) para el desarrollo de 1 piloto de servicio de interoperabilidad con una entidad de alta litigiosidad	XX
Documento con la caracterización de necesidades de interoperabilidad, entre los sistemas de información de la CGR, CSJ, Registraduría y Procuraduría con el sistema EKOGUI, desarrollado	

Fuente: Sistema Integrado de Gestión Institucional – SIGI

Se evidencian en los indicadores del PAI que el avance se concentra en el último trimestre del año.

Gráfica 6: Avance Indicadores PAI Proceso Gestión de Información 2020

RESULTADO ESPERADO 2020	RESULTADOS / ENTREGABLES INTERMEDIOS											
	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEPT	OCT	NOV	DIC
1. Aplicativo web para el seguimiento de la política de prevención, en producción.				Documento final de requerimientos elaborado					Especificación Fase I			Desarrollo (Código Fuente)
100% del plan de actividades (2 hitos definidos) para actualizar la información registrada en EKOGUI, implementado											(50%) Diagnóstico y	(50%) Resultado de calidad y
50% de avance en actividades del proyecto de acompañamiento para la explotación y actualización de información en 20 entidades intervenidas									20% de avance en la implementación del proyecto sobre las 20 entidades			50% de avance en la implementación del proyecto sobre las 20
Funcionalidad para calcular e incluir campo de provisión contable sugerida en el módulo de actualización de judiciales implementada												Funcionalidad para calcular e incluir campo de provisión contable
100% de los datos priorizados que se encuentran duplicados y con inconsistencias, depurados				Levantamiento línea de base de duplicidades y				30% de avance en la depuración de				100% de avance en la depuración de
3 informes al nivel directivo de entidades con cifras de la evolución de la problemática litigiosa					Reporte mensual 2020-I socializado	Reporte mensual 2020-II socializado	Reporte mensual 2020-III socializado	Reporte mensual 2020-IV socializado	Reporte mensual por entidad socializado	Reporte mensual por entidad socializado	Reporte mensual por entidad socializado	Reporte mensual por entidad socializado
3 informes de evolución de litigios por entidad y tipo de acción, reportados				Reporte mensual por entidad socializado	Reporte mensual por entidad socializado (mez vacante)			Reporte mensual por entidad socializado				
2 análisis a partir de la información de EKOGUI desarrollados								Resultados de análisis de parámetros comerciales				Resultados de optimización de
100% del plan de actividades (2 hitos definidos) para el desarrollo de una base de datos de litigiosidad territorial, desarrollados												(50%) Informe con descripción del
100% del plan de actividades (3 hitos definidos) para el desarrollo de 2 cubos multidimensionales para consultas dinámicas de procesos de judiciales y arbitramentos, desarrollado								(50%) Diseño y Arquitectura (Documento)				(50%) Diagnóstico del impacto en el sistema
12 reportes de medición del indicador de Estabilización de EKOGUI, realizados	Reporte de medición del indicador de Estabilización	Reporte de medición del indicador de Estabilización	Reporte de medición del indicador de Estabilización	Reporte de medición del indicador de Estabilización								
126 eventos para la apropiación del uso del EKOGUI, desarrollados				10		60				30		126
100% del plan de actividades (3 hitos definidos) para el desarrollo de implementaciones evolutivas, desarrollado									(33,3%) Especificación (Documento)	(33,3%) Diseño y Arquitectura		(33,3%) Desarrollo (Código Fuente)
2 herramientas implementadas para el fortalecimiento del Uso de EKOGUI						Herramientas para el diligenciamiento del			Herramientas para la generación de certificados de asistencia			
100% del plan de actividades (3 hitos definidos) para el desarrollo del Módulo de calidad de datos Fase I								(33,3%) Diseño y Arquitectura (Documento)				(33,3%) Desarrollo (Código Fuente)
11 reportes de registro y auditoría de tramites notificados		Registro y Auditoría de trámites	Registro y Auditoría de trámites notificados	Registro y Auditoría de trámites	Registro y Auditoría de trámites	Registro y Auditoría de trámites						
100% del plan de actividades (3 hitos definidos) para el desarrollo de 1 piloto de servicio de interoperabilidad con una entidad de alta litigiosidad									(33%) Especificación			(34%) Desarrollo (Código Fuente)
Documento con la caracterización de necesidades de interoperabilidad, entre los sistemas de información de la CGR, CSJ, Registraduría y									Documento con la caracterización de necesidades			

Fuente Entrevista desarrollo auditoria

Por lo anterior se recomienda incluir un porcentaje de avance, ya sea bimensual o trimestral, durante toda la vigencia, en la ejecución de las actividades registradas en el PAI, para minimizar los riesgos de Retraso o posible incumplimiento de estas, el mayor porcentaje de cumplimiento se concentra en el último trimestre.

**7.3.6 Cumplimiento MIPG - Política de Gobierno Digital**

**7.3.6 .1 Declaración de Aplicabilidad**

**Gráfica 7: Declaración De Aplicabilidad**

A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS				
A.14.1 Requisitos de seguridad de los sistemas de información				
A.14.11	Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	SI	Procedimientos, guías y lineamientos Dirección de Gestión de la Información
A.14.12	Seguridad de servicio de las aplicaciones en redes públicas	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación no autorizadas.	SI	Procedimientos, guías y lineamientos Dirección de Gestión de la Información
A.14.13	Protección de transacciones de los servicios de las aplicaciones	La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado la alteración no autorizada de mensajes, la divulgación no autorizada y la divulgación o reproducción de mensajes no autorizados.	SI	Procedimientos, guías y lineamientos Dirección de Gestión de la Información
A.14.2 Seguridad en los procesos de desarrollo y soporte				
A.14.21	Políticas de desarrollo seguro	Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	SI	Procedimientos, guías y lineamientos Dirección de Gestión de la Información
A.14.22	Procedimiento de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	SI	Procedimiento Gestión de Cambios Procedimientos, guías y lineamientos Dirección de Gestión de la Información
A.14.23	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	SI	Procedimiento Gestión de Cambios Procedimientos, guías y lineamientos Dirección de Gestión de la Información
A.14.24	Restricciones en los cambios a los paquetes de software	Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	SI	Procedimientos, guías y lineamientos Dirección de Gestión de la Información
A.14.25	Principios de construcción de los sistemas seguros	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de	SI	Procedimientos, guías y lineamientos Dirección de Gestión de la Información
A.14.26	Ambiente de desarrollo seguro	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	SI	Manual De Políticas Institucionales Y De Desarrollo Administrativo: 6.4.11 POLÍTICA DE SEPARACIÓN DE AMBIENTES DE DESARROLLO, PRUEBAS Y PRODUCCIÓN Procedimientos, guías y lineamientos Dirección de Gestión de la Información
A.14.27	Desarrollo contratado externamente	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	SI	Procedimientos, guías y lineamientos Dirección de Gestión de la Información

**Fuente Pagina Web Intranet**

Se evidenció que el proceso Gestión de Información implemento controles propios que permiten realizar el proceso de desarrollo con métricas de seguridad conforme a lo esperado. Sin embargo, se evidencia falta de articulación con la Declaración de Aplicabilidad en la cual se definen los responsables de definir los mecanismos de seguimiento de estos controles.

En la Declaración de Aplicabilidad en el control A.14 Adquisición, Desarrollo Y Mantenimiento De Sistemas - A.14.1 *Requisitos de seguridad de los sistemas de información*, establece que la Agencia lo adopta mediante Procedimientos, guías y lineamientos definidos por la Dirección de Gestión de la Información.

Al consultar el Sistema Integrado de Gestión Institucional – SIGI, no se evidencian lineamientos por parte de la Dirección de Gestión de Información DGI en donde se definan los Requisitos de seguridad de los sistemas de información para la Agencia Nacional de Defensa Jurídica del Estado.

En la Declaración de Aplicabilidad A.14 Adquisición, Desarrollo Y Mantenimiento De Sistemas - A.14.2 *Seguridad en los procesos de desarrollo y soporte Control definido* establece que la Agencia lo adopta mediante Procedimiento de Gestión de Cambios; Procedimientos, guías y lineamientos Dirección de Gestión de la Información.

Al consultar el Sistema Integrado de Gestión Institucional – SIGI, encontramos los procedimientos GI-P-09 *Realizar Desarrollo y Puesta en Marcha de los Requerimientos en el Sistema Único de Información Litigiosa del Estado* y el GI-P-07 *Brindar Soporte al Sistema Único de gestión e Información Litigiosa del Estado*, los cuales tienen como alcance el EKOGUI.



No se evidencia en el Sistema Integrado de Gestión Institucional - SIGI lineamientos por parte de la Dirección de Gestión de Información en donde se definan Seguridad en los procesos de desarrollo y soporte, con alcance para Agencia Nacional de Defensa Jurídica del Estado

Se recomienda llevar a cabo una articulación entre los responsables de Gobierno de información (no sé si aplique), Seguridad de la información, Gobierno de datos (no sé si aplique) y el Proceso Gestión de Información dado que se evidencia una debilidad al momento de definir los responsables de establecer controles y sus mecanismos de seguimiento.

### **7.3.6.2 Modelo de Arquitectura Empresarial - Estructura organizacional**

Al realizar la revisión del Plan de Acción Institucional (PAI) del Proceso Gestión de Información, se evidencia que tienen 7 actividades que corresponden a proyectos de TI, para los cuales no fue posible revisar su inclusión en el Plan Estratégico de tecnologías de Información PETI, por no contar con un Plan para 2020 en el cual se encuentren consolidado los proyectos y presupuestos. Lo cual va en contravía de lo señalado en el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones 1008 de 2018 y el Modelo de Gestión y Gobierno de TI el cual permite generar las capacidades institucionales de TI que se requieren para prestar servicios de TI a los usuarios de cada entidad mediante el uso adecuado de las tecnologías de la información y las comunicaciones en su numeral 6.1.5. *MGGTI.LI.ES.05 – Gestión del presupuesto de TI La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe realizar de manera periódica el seguimiento y control de la ejecución del presupuesto de TI. El presupuesto deberá identificar el presupuesto asignado a la operación de TI y el presupuesto asignado a los proyectos de transformación incluidos en el PETI.*

Al validar en los documentos línea del intercambio de información y gestión de información de la Gestión de Información de Defensa Jurídica no se evidencia la existencia de un Marco de Interoperabilidad según lo establecido en La Política de Gobierno Digital con el Marco de interoperabilidad para Gobierno Digital en los -Elementos de Gobernanza de la Interoperabilidad. Define que la estructura debe contemplar los siguientes elementos:

- Contrato de descripción del servicio de intercambio Monitoreo y disponibilidad del servicio
- Procesos de Gobierno
- Procesos gobernados de interoperabilidad
- Proceso de Gestión del portafolio de servicios de intercambio
- Proceso ciclo de vida del servicio de intercambio
- Proceso de gestión de soluciones de interoperabilidad
- Proceso Ciclo de vida de solución de interoperabilidad

Al hacer una revisión de los siguientes documentos **Decreto 2269 de 2019 Estructura de la Agencia; Resolución 095 del 26 de febrero de 2018 adopción de MIPG; Manual De Políticas De Gestión y Desempeño Institucional De La Agencia; Modelo Óptimo De Gobierno De Información** y la **Declaración de aplicabilidad de controles MISP**, los cuales son fundamento, entre otros, de la estructura y funcionalidad de la Agencia Nacional de Defensa Jurídica del Estado, en el ámbito de Gestión de información y Gestión de seguridad de la información

Se evidencia una desarticulación frente a la asignación de responsables, definición de responsables de definir controles y hacer seguimientos en los temas correspondientes. Esto va en contravía de lo establecido en:

El **Modelo de Arquitectura Empresarial establecido por MINTIC**, en el Marco de Referencia de Arquitectura V.2., 6.2. Dominio de gobierno de TI 6.2.1. *MGGTI.LI.GO.01 - Esquema de Gobierno de TI La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir e implementar un esquema de Gobierno TI alineado con la estrategia misional y con el Modelo Integrado de Planeación y Gestión, que estructure y dirija el flujo de las decisiones de TI. El esquema de Gobierno de TI deberá identificar los roles, los procesos y los recursos necesarios para habilitar las capacidades de TI. Esta implementación debe liderada conjuntamente por la alta dirección de la entidad y la Dirección de Tecnologías de la Información o quien haga sus veces.*

El **Manual De Gobierno Digital** que implementa la Política de Gobierno Digital - Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2) Responsables De La Política "Como responsables de la política de Gobierno Digital, los representantes legales (ministros, directores, gobernadores y alcaldes, entre otros), deben

garantizar el desarrollo integral de la política como una herramienta transversal que apoya la gestión de la entidad y el desarrollo de las políticas de gestión y desempeño institucional del Modelo Integrado de Planeación y gestión”

El **Decreto Único Reglamentario de Función Pública 1083 de 2015** en el artículo 2.2.35.4. establece que (...) *El director, Jefe de Oficina o Coordinador de Tecnologías y Sistemas de la Información y las Comunicaciones, o quien haga sus veces, hará parte del Comité Institucional de Gestión y Desempeño y responderá directamente al representante legal de la entidad.*

Se recomienda que desde la Oficina de Planeación se coordine la gestión correspondiente para que, enmarcados en los lineamientos definidos en la Política de Gobierno Digital con sus Modelos de Seguridad y Privacidad de la Información, marco de Referencia de Arquitectura y Servicios Ciudadanos Digitales, logre la articulación y alineación de los lineamientos que definen responsables y alcance de dichos lineamientos en la Agencia Nacional de Defensa Jurídica del Estado.

### 7.3.7 Funcionalidad del EKOGUI

En el desarrollo de la Auditoria se solicitó perfil para dos roles del sistema EKOGUI, Perfil de consulta y Perfil de Abogado.

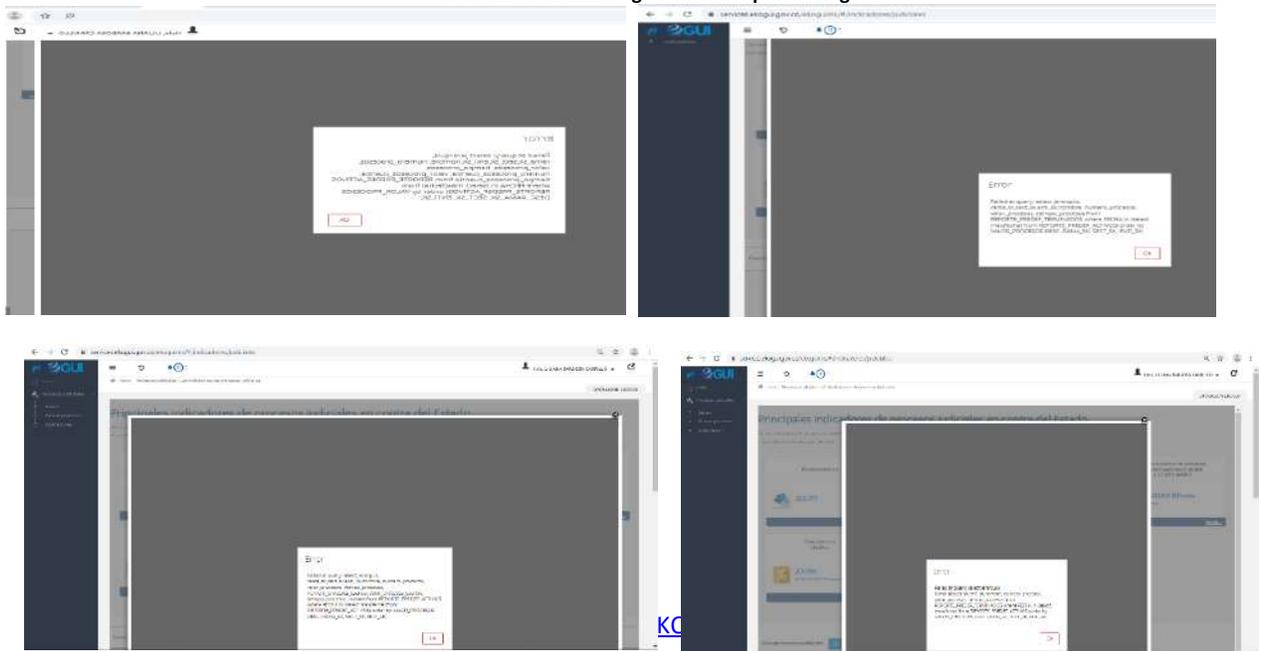
#### 7.3.7.1 Validación con el Perfil de consulta

Se hace una validación con el Perfil de consulta en ambiente de Producción de la funcionalidad de los Módulos procesos judiciales y Procesos Arbitrales.

En el menú “Indicadores”, <https://services.eKOGUI.gov.co/eKOGUIms/#/indicadores/judiciales> se valida la generación de reportes predefinidos evidenciando indisponibilidad en los siguientes reportes:

Procesos activos y Procesos terminados, se revisaron en diferentes fechas a lo largo del desarrollo de la Auditoria, descartando periodos de mantenimiento. Fechas de revisión agosto 24, Septiembre 1, 2 ,3 y 4 de 2020.

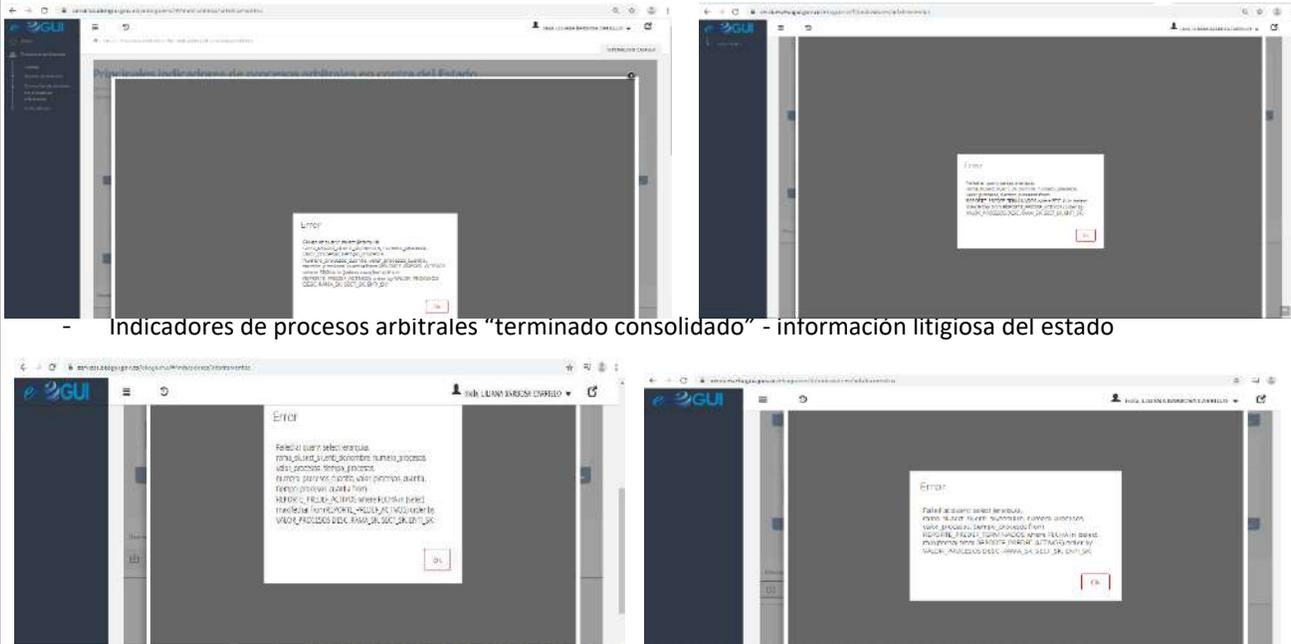
Gráfica 7: Pantallazos generación reporte eKogui



#### Módulos de Procesos Arbitrales

En el Menú “Indicadores”, <https://services.eKOGUI.gov.co/eKOGUIms/#/indicadores/arbitramentos> se valida la generación de reportes predefinidos evidenciando indisponibilidad en los siguientes reportes: Indicadores de procesos arbitrales “Activo consolidado” y procesos arbitrales “terminado consolidado”.

Gráfica 8: Pantallazos generación reporte eKogui



- Indicadores de procesos arbitrales "terminado consolidado" - información litigiosa del estado

Fuente: <https://services.eKOGUI.gov.co/eKOGUIMS/#/indicadores/arbitramentos>

### 7.3.7.2 Validación con Perfil de Abogado

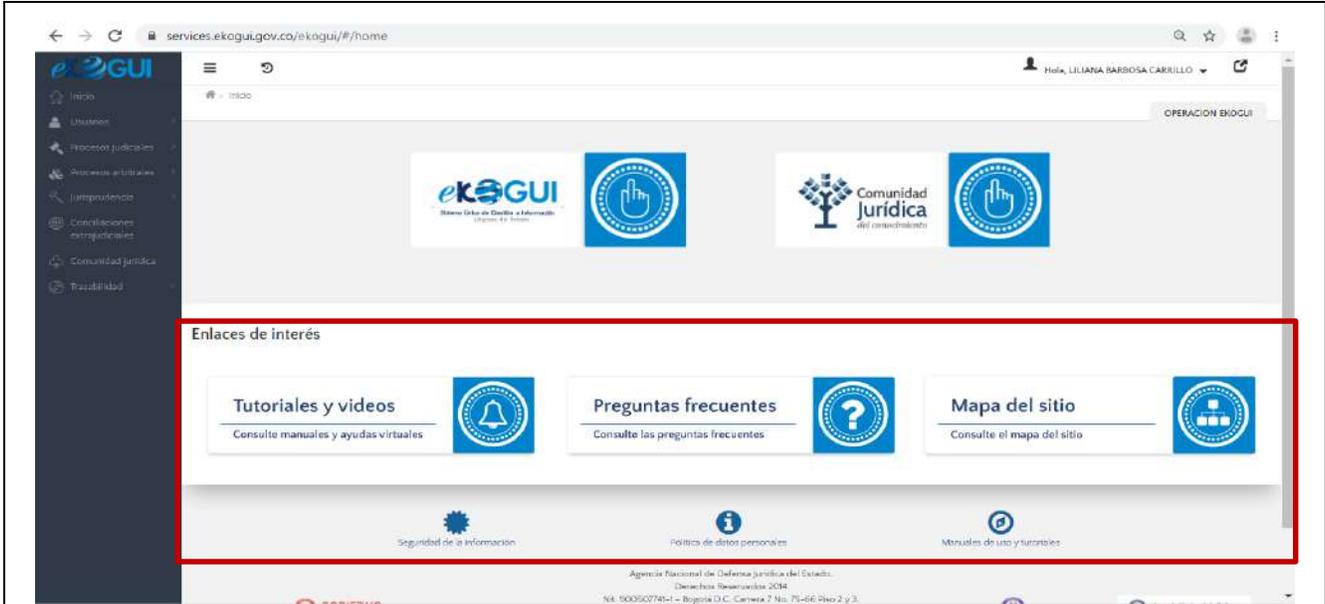
La validación con este perfil se realiza en ambiente de soporte <https://sop.eKOGUI.gov.co/eKOGUI/#/home>. A los módulos Procesos Judiciales e Indicadores de procesos arbitrales, fechas de revisión agosto 24, Septiembre 1, 2, 3 y 4 de 2020.

Gráfica 9: Pantallazos generación reporte eKogui - Procesos Judiciales



Fuente: <https://sop.eKOGUI.gov.co/eKOGUI/#/home>





Fuente: <https://services.eKOGUI.gov.co/eKOGUI/#/home>

Al verificar la funcionalidad del eKogui, se evidenció la indisponibilidad en la generación de Reportes de los Módulos *Procesos judiciales* y *Procesos Arbitrales* y en Reportes predefinidos -*Indicadores de procesos arbitrales "Activo consolidado"* y Reportes predefinidos -*Indicadores de procesos arbitrales "Terminado consolidado"* Así mismo la no disponibilidad de los enlaces de interés *Tutoriales y videos*, *Preguntas Frecuentes* y *Mapa del sitio*. Situación que denota incumplimiento con el Objetivo del Proceso: *Gestionar, Producir y Administrar la información estratégica sobre la actividad litigiosa del Estado, que apoye la toma de decisiones de los actores que intervienen en la gestión del ciclo de defensa jurídica del Estado y de otros clientes estratégicos.*

### 7.3.8 Seguimiento Contractual (Asociado al EKOGUI)

Se realiza una validación en la contratación realizada por el Proceso Gestión de Información de Defensa Jurídica, se evidencia que los contratos se están realizando en el segundo semestre lo que denota una reincidencia frente a una recomendación de la anterior auditoria: *Se recomienda a la Dirección de Gestión de Información tener especial cuidado con el impacto de la falta de proveedores y personal contratista que apoya la línea de producción cuando se finalizan los contratos. Específicamente al inicio de año, toda vez que se podría afectar el plan de trabajo, soporte y las capacitaciones proyectadas a las Entidades usuarias del sistema de información eKOGUI.*

Es necesario que Proceso Gestión de Información de Defensa Jurídica realice los procesos de planeación contractual de manera anticipada para garantizar el recurso humano necesario para el cumplimiento de los objetivos del Proceso desde el inicio de la vigencia alineado con lo establecido en MGGTI.G.GEN.01 – Documento Maestro del Modelo de Gestión y Gobierno de TI 6.1.4. MGGTI.LI.ES.04 - *Gestión de los proyectos con componentes de TI. La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe participar de forma activa en la concepción, planeación y desarrollo de los proyectos de la institución que incorporen componentes de TI.*



**8. DESCRIPCIÓN DEL (LAS) NO CONFORMIDADES (S)**

Para la elaboración del informe final se tienen en cuenta los comentarios y observaciones brindadas por los diferentes responsables mediante Radicado Numero 20204000010353 y las mesas de trabajo realizadas con cada uno de ellos durante el 23 y 24 de septiembre de 2020.

REQUISITO	NO CONFORMIDAD	OBSERVACIONES
GI-P-07 V-1 BRINDAR SOPORTE AL SISTEMA UNICO DE GESTION E INFORMACIÓN LITIGIOSA DEL ESTADO		Se evidenció la necesidad, en los procedimientos revisados, de generar un control para medir los Tiempos de Respuesta de Servicio, la temporalidad para la solución de los casos, siendo importante definir estándares o políticas de desempeño y calidad de autoevaluación en el procedimiento.
GUIA DE ADMINISTRACION DE RIESGOS "(...) para ello el líder de Proceso deberá guardar evidencias de esta gestión" (...) <i>SEGURIDAD. 13.5.4 Responsabilidades (...) Monitoreo de los riesgos. El líder del proceso (dueño del riesgo) será el responsable de monitorear los riesgos aceptados y residuales, para ello deberá guardar evidencias de esta gestión.</i>		Al realizar la validación de los controles se observa debilidad del control del riesgo de seguridad de la información definido, dado que al momento de validarlo, no se contaba con la evidencia de esta gestión. <b>TI-MSPI</b>
MGGTI.G.GEN.01 – Documento Maestro del Modelo de Gestión y Gobierno de TI 6.1.4. MGGTI.LI.ES.04 - <i>Gestión de los proyectos con componentes de TI. La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe participar de forma activa en la concepción, planeación y desarrollo de los proyectos de la institución que incorporen componentes de TI.</i>		Es necesario que Proceso Gestión de Información de Defensa Jurídica realice los procesos de planeación contractual de manera anticipada para garantizar el recurso humano necesario para el cumplimiento de los objetivos del Proceso desde el inicio de la vigencia - DGI – Secretaria General
Guía De Administración De Riesgos en su Numeral 10 <i>GESTION Y CORRUPCION 10. Seguimiento. El líder del proceso realizará mensualmente el seguimiento, registrando los resultados de cada una de las actividades desarrolladas con el soporte correspondiente (acta, correo) etc., tanto en físico como en digital en la herramienta del Sistema</i>		No se evidencia el detalle del cumplimiento del control DE-MO-01 Modelo Optimo de Gobierno de Información, definidos para mitigar el Riesgo de Corrupción, Filtración de información estratégica, sensible y confidencial en favor de un tercero.
MODELO ÓPTIMO DE GOBIERNO DE INFORMACIÓN 2.5.2 <i>Asignaciones específicas de responsabilidad en la Agencia-2.5.2.4 Oficina Asesora de Planeación La Oficina Asesora de Planeación se encarga de la creación y actualización permanente del Modelo de Gobierno de Información - MOGI. Y 2.5.2.6 Proceso de Gestión de Tecnologías de la Información - Proponer el Modelo de Gobierno de Tecnologías de la Información.</i>		No se evidencia la propuesta y la actualización permanente del Modelo Optimo de Gobierno de Información que se encuentra publicado en Sistema Integrado de Gestión Institucional – SIGI.  Esta observación es de responsabilidad de: La Oficina de Asesora de Planeación y del Proceso Gestión de Tecnologías de la Información.



<p>Guía Administración De Riesgos - Consideración Para El Sistema De Gestión De Seguridad De La Información Tratamiento Del Riesgo, <i>El líder del proceso (dueño del riesgo) con el apoyo del profesional del SGSI, debe describir las acciones y el tiempo en que realizara el tratamiento para cada riesgo identificado. SEGUIMIENTO AL TRATAMIENTO DEL RIESGO. El responsable del Sistema de Gestión de Seguridad de la Información con el apoyo del profesional del SGSI, solicitara trimestralmente al líder del proceso (dueño del riesgo) los avances y evidencias de los tratamientos de los riesgos a cargo de su gestión.</i></p>		<p>No se evidencia periodicidad en seguimiento a los controles implementados para los riesgos de seguridad de la información.</p> <p>Esta observación es de responsabilidad del Proceso Gestión de Tecnologías de la Información – MSPI</p>
<p>Guía Administración De Riesgos - Consideración Para El Sistema De Gestión De Seguridad De La Información Tratamiento Del Riesgo. <i>El líder del proceso (dueño del riesgo) con el apoyo del profesional del SGSI, debe describir las acciones y el tiempo en que realizara el tratamiento para cada riesgo identificado. SEGUIMIENTO AL TRATAMIENTO DEL RIESGO. El responsable del Sistema de Gestión de Seguridad de la Información con el apoyo del profesional del SGSI, solicitara trimestralmente al líder del proceso (dueño del riesgo) los avances y evidencias de los tratamientos de los riesgos a cargo de su gestión.</i></p>	<p>En la validación del seguimiento y control a los riesgos del Proceso, no se encuentra evidencia de reporte mensual de controles en el Sistema Integrado De Gestión Institucional – SIGI (Responsable DGI – Oficina Asesora de Planeación)</p>	
<p>Guía Administración De Riesgos la cual en su metodología afirma que combina elementos de la Norma Técnica Colombiana NTC-ISO 31000 y la Guía para la Administración del Riesgo del Departamento Administrativo de la Función Pública. Anexo 4 Lineamientos Para La Gestión De Riesgos De Seguridad Digital En Entidades Públicas Y Guía Roles Y Responsabilidades Del Mspi - la cual cita: <i>de la Estrategia de Gobierno Digital del MINTIC. La identificación y valoración de activos debe ser realizada por la Primera Línea de Defensa – Líderes de Proceso, en cada proceso donde aplique la gestión del riesgo de seguridad digital, siendo debidamente orientados por el responsable de seguridad digital o de seguridad de la información de la entidad pública.</i></p>	<p>Se evidencia que la DGI no tiene identificados los Riesgos de seguridad digital, en los cuales se incluyan riesgos para activos de tipo aplicaciones, servicios, servicios Web, redes, tecnologías de la información TI- o tecnologías de la operación -TO-, hardware, software, servicios y recurso humano, desde el punto de vista de la confidencialidad, la integridad y disponibilidad.. Que apliquen al proceso, según la criticidad identificada para sus activos de información</p> <p>Esta no conformidad es de responsabilidad del Proceso Gestión de Información de Defensa Jurídica y del Proceso Gestión de Tecnologías de la Información - MSPI.</p>	



<p>Modelo de Seguridad y Privacidad de la Información (MSPI), Guía N° 10 Continuidad del negocio.</p>	<p>No se evidencia un Plan de Recuperación de desastres - DRP que contenga aspectos como Plan de pruebas, de capacitación, de mejoramiento y de mantenimiento. Adicionalmente no se evidencia en el documento la aprobación de la alta dirección.</p> <p>Esta no conformidad es de responsabilidad del Proceso Gestión de Información de Defensa Jurídica, Proceso Gestión de Tecnologías de la Información – MSPI y de la Oficina Asesora de Planeación y/o la Secretaria General, según corresponda.</p>	
<p>DECLARACIÓN DE APLICABILIDAD en el control A.14 Adquisición, Desarrollo Y Mantenimiento De Sistemas - A.14.1 Requisitos de seguridad de los sistemas de información, establece que la Agencia lo adopta mediante Procedimientos, guías y lineamientos definidos por la Dirección de Gestión de la Información.</p>	<p>no se evidencian lineamientos por parte de la Dirección de Gestión de Información DGI en donde se definan los Requisitos de seguridad de los sistemas de información para la Agencia Nacional de Defensa Jurídica del Estado.</p> <p>Esta no conformidad es de responsabilidad del Proceso Gestión de Información de Defensa Jurídica y del Proceso Gestión de Tecnologías de la Información - MSPI.</p>	
<p>DECLARACIÓN DE APLICABILIDAD A.14 Adquisición, Desarrollo Y Mantenimiento De Sistemas - A.14.2 Seguridad en los procesos de desarrollo y soporte Control definido establece que la Agencia lo adopta mediante Procedimiento de Gestión de Cambios; Procedimientos, guías y lineamientos Dirección de Gestión de la Información.</p>	<p>No se evidencia en el Sistema Integrado De Gestión Institucional - SIGI lineamientos por parte de la Dirección de Gestión de Información en donde se definan Seguridad en los procesos de desarrollo y soporte, con alcance para Agencia Nacional de Defensa Jurídica del Estado. Encontramos el procedimiento <i>GI-P-09 Realizar Desarrollo Y Puesta En Marcha De Los Requerimientos En El Sistema Único De Información Litigiosa Del Estado</i> y el <i>GI-P-07 Brindar Soporte Al Sistema Único De gestión E Información Litigiosa Del Estado</i>, los cuales tienen como alcance el EKOGUI.</p> <p>Esta no conformidad es de responsabilidad del Proceso Gestión de Información de Defensa Jurídica y del Proceso Gestión de Tecnologías de la Información - MSPI.</p>	



<p>Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones 1008 de 2018 y el Modelo de Gestión y Gobierno de TI el cual permite generar las capacidades institucionales de TI que se requieren para prestar servicios de TI a los usuarios de cada entidad mediante el uso adecuado de las tecnologías de la información y las comunicaciones en su numeral 6.1.5. <i>MGGTI.LI.ES.05 – Gestión del presupuesto de TI La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe realizar de manera periódica el seguimiento y control de la ejecución del presupuesto de TI. El presupuesto deberá identificar el presupuesto asignado a la operación de TI y el presupuesto asignado a los proyectos de transformación incluidos en el PETI. Y Manual Operativo del Modelo Integrado de Planeación y Gestión</i></p>	<p>Al realizar la revisión del Plan de Acción Institucional (PAI) del Proceso Gestión de Información, se evidencia que tienen 7 actividades que corresponden a proyectos de TI para los cuales no fue posible revisar su inclusión en el Plan Estratégico De tecnologías De Información, por no contar con un Cronograma en el cual se encuentren consolidado estos los proyectos con sus respectivos presupuestos y tiempos de ejecución.</p> <p>Esta no conformidad es de responsabilidad del Proceso Gestión de Tecnologías de la Información</p>	
<p>Política de Gobierno Digital con el Marco de interoperabilidad para Gobierno Digital en los - Elementos de Gobernanza de la Interoperabilidad. Define que la estructura debe contemplar los siguientes elementos:</p> <ul style="list-style-type: none"> <li>• Contrato de descripción del servicio de intercambio Monitoreo y disponibilidad del servicio</li> <li>• Procesos de Gobierno Procesos gobernados de interoperabilidad</li> <li>• Proceso de Gestión del portafolio de servicios de intercambio Proceso ciclo de vida del servicio de intercambio</li> <li>• Proceso de gestión de soluciones de interoperabilidad</li> <li>• Proceso Ciclo de vida de solución de interoperabilidad</li> </ul>	<p>Al validar en los documentos línea del intercambio de información y gestión de información de la Gestión de Información de Defensa Jurídica no se evidencia la existencia de un Marco de Interoperabilidad</p> <p>Esta no conformidad es de responsabilidad del Proceso Gestión de Información de Defensa Jurídica, del Proceso Gestión de Tecnologías de la Información y de la Oficina Asesora de Planeación y/o la Secretaria General, según corresponda.</p>	
<p>Modelo de Arquitectura Empresarial establecido por MINTIC, en el Marco de Referencia de Arquitectura V.2., 6.2. Dominio de gobierno de TI 6.2.1. <i>MGGTI.LI.GO.01 - Esquema de Gobierno de TI La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir e implementar un esquema de Gobierno TI alineado con la estrategia misional y con el Modelo Integrado de Planeación y Gestión, que estructure y direcciona el flujo de las decisiones de TI. El esquema de Gobierno de TI deberá identificar los roles, los procesos y los recursos necesarios para habilitar las capacidades de TI. Esta implementación debe liderada conjuntamente por la alta dirección de la entidad y la Dirección de Tecnologías de la Información o quien haga sus veces.</i></p>	<p>Al hacer una revisión de los siguientes documentos: Decreto 2269 de 2019 Estructura de la Agencia; Resolución 095 del 26 de febrero de 2018 adopción de MIPG; Manual De Políticas De Gestión y Desempeño Institucional De La Agencia; Modelo Óptimo De Gobierno De Información y la Declaración de aplicabilidad de controles MISIP, Los cuales son fundamento, entre otros, de la estructura y funcionalidad de la Agencia Nacional de Defensa Jurídica del Estado, en el ámbito de Gestión de información y Gestión de seguridad de la información. Se evidencia una desarticulación frente la asignación de responsables de definir controles y hacer seguimientos en los temas correspondientes.</p>	



	Esta no conformidad es de responsabilidad de la Oficina Asesora de Planeación y/o la Secretaria General, según corresponda.	
Objetivo del Proceso: Gestionar, Producir y Administrar la información estratégica sobre la actividad litigiosa del Estado, que apoye la toma de decisiones de los actores que intervienen en la gestión del ciclo de defensa jurídica del Estado y de otros clientes estratégicos.	Al verificar la funcionalidad del eKogui, se evidenció la indisponibilidad en la generación de Reportes de los Módulos Procesos judiciales y Procesos Arbitrales y en Reportes predefinidos -Indicadores de procesos arbitrales “Activo consolidado” y Reportes predefinidos -Indicadores de procesos arbitrales “Terminado consolidado” Así mismo la no disponibilidad de los enlaces de interés Tutoriales y videos, Preguntas Frecuentes y Mapa del sitio	

**9. RECOMENDACIONES:**

<p>La Oficina de Control Interno en el marco de la auditoria recomienda:</p> <ul style="list-style-type: none"> <li>• Complementar el inventario de activos de información con los “Reportes Generados Después de Las Auditorias” -GI-P-01.</li> <li>• Complementar los activos de información agregando “los Informe de resultados de validación”- GI-P-02.</li> <li>• Crear una constancia de envío de correo de notificación de respuesta al usuario final - Procedimiento GI-P-07.</li> <li>• Conocer los resultados o crear encuestas de satisfacción frente al servicio recibido por parte de la mesa de ayuda, sistema EKOGUI - GI-P-07.</li> <li>• Definir un control para casos que superen los plazos definidos dentro del procedimiento - GI-P-07.</li> <li>• Complementar el inventario de activos de información con el Código fuente - GI-P-09.</li> <li>• Gestionar los activos de información, dado que son prerrequisito para la gestión de riesgos de seguridad de la información para poder tenerlos en cuenta al momento de la creación de la matriz de riesgos de seguridad Digital.</li> <li>• Se recomienda que para los activos catalogados como críticos, los cuales requieran un alto grado de disponibilidad deben estar contemplados en el alcance de la gestión de la continuidad del negocio.</li> <li>• Cada vez que se reconozca un nuevo activo de información o se genere un cambio en alguno existente , que afecte el cumplimiento de los objetivos del Proceso, se recomienda realizar una revisión del riesgo para dicho activo, contemplando por cada activo su impacto, vulnerabilidades y amenazas, controles asociados, riesgo inherente y residual, con el fin de establecer planes de tratamiento por cada activo adecuado en el marco de la norma ISO 27001.</li> <li>• Incluir un porcentaje de avance, ya sea bimensual o trimestral, durante toda la vigencia, en la ejecución de las actividades registradas en el PAI, para minimizar los riesgos de Retraso o posible incumplimiento de estas, el mayor porcentaje de cumplimiento se concentra en el último trimestre.</li> <li>• A la Oficina Asesora de Planeación validar la periodicidad de seguimiento de controles de riesgos registrados en la Guía De Administración De Riesgos.</li> <li>• Que desde la Oficina de Planeación y/o Secretaria General se coordine la gestión correspondiente para que, enmarcados en los lineamientos definidos en la Política de Gobierno Digital con sus Modelos De Seguridad Y Privacidad De La Información, Marco De Referencia De Arquitectura y Servicios Ciudadanos Digitales, se logre la articulación entre los Modelos de Gobierno de información, Seguridad de la información, Gobierno de datos y el Proceso Gestión de Información, definiendo responsables y alcances en la Agencia Nacional de Defensa Jurídica de Estado.</li> </ul>
--

<p><b>Firma Auditor Designado y Equipo Auditor</b> Informe realizado Electrónicamente por: Liliana Barbosa Carrillo <b>Gestora Oficina de Control Interno</b> No. Radicado: 20201020011163</p>
--

<p><b>Firma Jefe de Control Interno ANDJE</b> Informe Firmado Electrónicamente por: Luis Eberto Hernández León <b>Jefe Oficina de Control Interno</b> No. Radicado: 20201020011163</p>
--