INFORME DE AUDITORIA INTERNA

Agencia Nacional de Defensa Jurídica del Estado

FECHA DE EMISIÓN DEL INFORME	**Día:**	**14**	**Mes:**	**3**	**Año:**	**2022**
FECHA EJECUCIÓN DE LA AUDITORIA	**DESDE**	**1-2-2022**		**HASTA**	**28-2-2022**	

Aspecto Evaluable (Unidad Auditable):	Auditoria al proceso de Gestión de Tecnologías de la Información
Líder de Proceso:	Diana Lucia Herrera Riaño
Objetivo de la Auditoría:	Evaluar el proceso de Gestión de Tecnologías de la Información 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.
Alcance de la Auditoría:	Se evaluará el periodo comprendido entre el 1 de enero de 2021 y 30 de enero de 2022.
Criterios de la Auditoría:	Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales http://suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1684507 Ley de Transparencia Ley 1712 de 2014 –http://suin-uriscol.gov.co/viewDocument.asp?ruta=Leyes/1687091 Ley 1955 de 2019 Plan nacional de desarrollo 2018-2022 - Artículo 147 Transformación digital Artículo 148 Gobierno digital como política de gestión - http://www.secretariasenado.gov.co/senado/basedoc/ley_1955_2019.html Ley 2052 de 2020 Servicios ciudadanos digitales - racionalización de trámites https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=96145 Ley 2080 de 2021 - Por medio de la cual se reforma el Código de Procedimiento Administrativo y de lo Contencioso Administrativo https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=156590 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 juriscol.gov.co/viewDocument.asp?ruta=Decretos/1541296 Decreto 1069 de 2015. Decreto Único Reglamentario del Sector Justicia y del Derecho http://suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/30019870 Decreto 1078 de 2015 – Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones https://normograma.mintic.gov.co/mintic/docs/decreto_1078_2015.htm - Gov.co 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. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=83433 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-juriscol.gov.co/viewDocument.asp?ruta=Decretos/30019521

Agencia Nacional de Defensa Jurídica del Estado

Decreto Ley 2106 de 2019 - Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública - Sedes electrónicas https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=103352

Decreto 1244 de 8 de octubre de 2021 creación de la Oficina Asesora de Sistemas y Tecnologías de la información en la ANDJE https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=172308

Directiva presidencial 02 de 2019. Simplificación De La Interacción Digitalmente Los Ciudadanos Y El Estado - Portal Único GOV.CO - https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=91630

Directiva presidencial 03 de 2021 Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.https://www.beltranpardo.com/wp-content/uploads/2021/03/DIRECTIVA-PRESIDENCIAL-03-DEL-15-DE-MARZO-DE-2021.pdf

Resolución 1519 de 2020 Información y seguridad Digital https://gobiernodigital.mintic.gov.co/692/articles-160770_resolucion_1519_2020.pdf

Resolución 2893 de 2020 Estandarizar ventanillas únicas, portales específicos de programas transversales, sedes electrónicas, trámites, OPAs y consultas de acceso a información pública, así como en relación con la integración al Portal Único del Estado Colombiano, https://gobiernodigital.mintic.gov.co/692/articles-161263_Resolucion_2893_2020.pdf

Resolución 2160 de 2020 Por la cual se expide la Guía de lineamientos de los servicios ciudadanos digitales y la Guía para vinculación y uso de estos https://normograma.mintic.gov.co/mintic/docs/resolucion_mintic_2160_2020.htm

Resolución 500 de 2020 lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

Resolución 312 de 2021, 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/servicios-al-ciudadano/ley_transparencia/Paginas/default.aspx

Resolución 1126 de 2021, la cual modifica la Resolución 2710 de 2017 en cuanto al Plazo de adopción protocolo IPv6 https://gobiernodigital.mintic.gov.co/692/articles-176070_recurso_1.pdf

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. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854

CONPES 3995 de 2020 Política Nacional De Confianza Y Seguridad Digitalhttps://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

Marco de transformación digital - Gobierno digital https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/149186:MinTIC-publica-el-Marco-de-Transformacion-Digital-para-mejorar-la-relacion-Estado-ciudadano

Marco de mejores prácticas en Tecnología alineados con COBIT 5, ITIL V3 2011 E ISO 27000:2013

Guía de Conceptos y criterio mínimos para los documentos aportados al PAI/MIPG, referencia DE-G-05
Demás normatividad interna y externa aplicable

Guía de Conceptos y criterio mínimos para los documentos aportados al PAI/MIPG, referencia DE-G-05
Demás normatividad interna y externa aplicable

Agencia Nacional de Defensa Jurídica del Estado

LIMITACIONES PARA EL DESARROLLO DE LA AUDITORIA:

No se presentaron

PLAN DE MUESTREO:

Se verifica la información suministrada por correo y a través de Orfeo, por parte del Proceso, en lo referente a procedimientos y documentación solicitada, 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.

Se hacen seguimientos a los avances en relación con evaluaciones anteriores.

DOCUMENTOS EXAMINADOS:

1. Mapa de riesgos generales para proceso Gestión de Tecnologías de la Información.
2. Mapa de riesgos de Corrupción.
3. Mapa de riesgos de Seguridad de la Información.
4. Documento de caracterización GTI-C-01 V2 Gestión de tecnologías de la Información.
5. GTI-P-03 – V2 Solicitud y Aprobación de Nuevos Desarrollos o Mejoras de Software
6. GTI-P-05 – V2 Gestión de Incidentes de Seguridad de La Información
7. Guía Administración de Riesgos Versión 4 Preliminar

RESULTADOS DE LA AUDITORIA:

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

   El proceso de Gestión de tecnologías de la Información hace parte de los procesos transversales de la Entidad, definido mediante Ley 4085 de 2011 modificado por el Decreto 2269 de diciembre de 2019 y el Decreto 1244 de 2021 tiene como objetivo “Diseñar, implementar y administrar de forma efectiva, soluciones de tecnologías de información estratégicas y operativas, que apoyen el cumplimiento de la misión de la ANDJE”. A continuación, se revisan la caracterización y 2 de sus procedimientos, la revisión está orientada a validar los puntos de control existentes.

1.1 GTI-C-01 V2 Documento de caracterización

Se realiza la verificación de la Caracterización del Proceso con el Líder del Proceso y su equipo encontrando que:

Dentro de las 4 actividades registradas no aparece alguna que registre la generación de lineamientos, políticas y directrices para atender con las obligaciones establecidas en el Decreto 1244 de 2021

Que de los 3 Planes estratégicos a cargo del Proceso Gestión Tecnológica, que son el Plan Tecnologías de la Información y las Comunicaciones - PETI,- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información,- Plan de Seguridad y Privacidad de la Información únicamente está contemplado el PETI, quedando incompleto el marco conceptual

1.2 GTI-P-03 – V2 Solicitud y Aprobación de Nuevos Desarrollos o Mejoras de Software

Se realiza la verificación de la funcionalidad y puntos de control del Procedimiento con los ingenieros delegados por el Líder del Proceso en la gestión realizada y se evidencia conformidad por parte del Proceso Gestión Tecnológica. Sin embargo al verificar se encontraron proyectos de desarrollo de software a cargo de la DGI Y de la Dirección Estratégica, en los cuales no se evidencia el cumplimiento del procedimiento Gti-P-03_Solicitud y Aprobación De Nuevos Desarrollos o Mejoras

Al validar el seguimiento aportado por el Proceso GTI, corresponde al desarrollo del PETI y avances durante la vigencia, razón por la cual se recomienda socializar los lineamientos de obligatoriedad de centralización por parte de la Oficina de TI de todos los procesos de adquisición o desarrollo de software

1.3 GTI-P-05 – V2 Gestión de Incidentes de Seguridad de La Información

Se realiza la verificación de la funcionalidad y puntos de control del Procedimiento con los ingenieros delegados por el Líder del Proceso y se validan los puntos de control encontrando que:

Las fuentes de reporte se reducen a los colaboradores de la Agencia, por lo cual se recomienda incluir como fuente los agentes externos, los informes de auditoría entre otros.

Se recomienda implementar el formato de base de conocimientos de incidentes de seguridad de la información, como insumo número 1 para la etapa de análisis de incidentes en el Procedimiento.

Así mismo, se evidencia que como resultado de la auditoria de gestión al proceso de Gestión Documental se informó de un incidente de seguridad sobre la visualización de datos personales al cual no se le dio el tratamiento referido en el presente procedimiento.

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:

Tabla N° 1 Riesgos asociados al proceso Gestión de Tecnologías de la Información

IDENTIFICACIÓN DEL RIESGO		VALORACIÓN DEL RIESGO	Observaciones
RIESGO	**Tipo de riesgo**	**CONTROLES**	
Inadecuada conceptualización de los requerimientos para el desarrollo o mejoras de los sistemas de información.	Gestión	GTI P 03 Solicitud y aprobación de nuevos desarrollos o mejoras de software	Se evidencia la aplicación de los controles y el reporte del informe de acuerdo a la criticidad.
Adquisición, arrendamiento yo construcción de soluciones informáticas que no se encuentran alineadas con los objetivos estratégicos de la Entidad.	Gestión	Aprobación y validación de contratación a través del Comité de Contratación Resolución 308 de 09 de julio de 2019, Por medio de la cual se expide el reglamento del Comité de Contratación de la Unidad Administrativa Especial Agencia Nacional de Defensa Jurídica del Estado ANDJE	Se evidencia la aplicación de los controles y el reporte del informe de acuerdo a la criticidad.

Fuga de información para favorecer a un tercero	Corrupción	Aprobación a través del Comité Gestión y Desempeño institucional. Política de seguridad y privacidad de la información contenidas en el Manual de políticas de gestión y desempeño institucional de la agencia DEM02 GTII01 Instructivo de control de accesos a centro de atos Sistema de SIEM Gestor de eventos e información de Seguridad. Sistema de control de acceso de directorio activo para usuarios de la red. Sistema monitoreo a la infraestructura. Separación de ambientes informáticos para los sistemas misionales ekogui y Orfeo. Herramientas de cifrado de información. Herramientas de prevención de pérdida de datos.	Se evidencia la aplicación de los controles y el reporte del informe de acuerdo a la criticidad.
Posible pérdida de la confidencialidad, integridad y disponibilidad de la información de los servicios tecnológicos de la ANDJE, debido a exposición a vulnerabilidades informáticas por desactualización en: Servidores y/o Sistemas Operativos.	Seguridad	CONTROL: Herramienta de monitoreo y actualización SystemCenter RESPONSABLE: Asesor(a) de TI FRECUENCIA: Trimestral TIPO DE CONTROL: Preventivo NATURALEZA DEL CONTROL: Manual CONTROL DOCUMENTADO: NO CALIFICACIÓN DEL CONTROL: Los controles existen, son efectivos, pero no están documentados	Se evidencia la aplicación de los controles y el reporte del informe de acuerdo a la criticidad.
Posibles pérdidas de integridad y disponibilidad de la información digital de la Agencia debido a fallas en las copias de seguridad que se generan por no realizar pruebas periódicas de las mismas.	Seguridad	CONTROL: Herramienta de Backup RESPONSABLE: Asesor(a) de TI FRECUENCIA: Trimestral TIPO DE CONTROL: Preventivo NATURALEZA DEL CONTROL: Automático CONTROL DOCUMENTADO: SI: GTI-G-06 V-0 CALIFICACIÓN DEL CONTROL: Los controles existen, son efectivos, pero no están documentados	Se evidencia la aplicación de los controles y el reporte del informe de acuerdo a la criticidad.
Posible pérdida de confidencialidad, disponibilidad e integridad de los servidores y sistemas de información de la ANDJE por accesos no autorizados debido a la ausencia de lineamientos para la gestión de usuarios para prevenir la presencia de perfiles inadecuados.	Seguridad	CONTROL: Centro alterno RESPONSABLE: Asesor(a) de TI FRECUENCIA: Cuando aplique TIPO DE CONTROL: Preventivo 25% NATURALEZA DEL CONTROL: Automático 25% CONTROL DOCUMENTADO: SÍ EJECUCIÓN CONTROL: Se realizan copias de seguridad y se mantiene un centro alterno para contingencias que afecten a ORFEO y a Ekogui DESVIACIONES: visitas programadas EVIDENCIAS: Copias de seguridad y correos de comunicación con el centro alterno	Se evidencia una materialización de riesgos de seguridad de la información, por afectación a la confidencialidad del expediente, por una inadecuada gestión del sistema de información ORFEO. No se tienen establecidos controles que garanticen el cumplimiento necesario para mitigar el riesgo de este activo de información, por el desconocimiento o falta de compromiso por parte del personal responsable, para evitar aquellas situaciones que pueden afectar la disponibilidad, integridad y confidencialidad de la información.
Posible pérdida de la confidencialidad, integridad y disponibilidad de la información de los computadores de trabajo, sistemas de información y/o aplicativos de la ANDJE, debido a préstamo de contraseñas y/o equipos desatendidos afectando Confidencialidad, Integridad y Disponibilidad de la información.	Seguridad	CONTROL: Políticas de Seguridad de la Información RESPONSABLE: Asesor(a) de TI FRECUENCIA: No establecida TIPO DE CONTROL: Preventivo NATURALEZA DEL CONTROL: No hay CONTROL DOCUMENTADO: SÍ CALIFICACIÓN DEL CONTROL: No existen controles.	Se evidencia la aplicación de los controles y el reporte del informe de acuerdo a la criticidad.

Posible pérdida de la disponibilidad de los sistemas misioanles Ekogui y ORFEO por no contar con un plan de continuidad del negocio	Seguridad	CONTROL: Centro alterno RESPONSABLE: Asesor(a) de TI FRECUENCIA: Cuando aplique TIPO DE CONTROL: Preventivo 25% NATURALEZA DEL CONTROL: Automático 25% CONTROL DOCUMENTADO: SÍ EJECUCIÓN CONTROL: Se realizan copias de seguridad y se mantiene un centro alterno para contingencias que afecten a ORFEO y a Ekogui DESVIACIONES: visitas programadas EVIDENCIAS: Copias de seguridad y correos de comunicación con el centro alterno	Se evidencia la aplicación de los controles y el reporte del informe de acuerdo a la criticidad.
Posible pérdida de la confidencialidad, integridad y disponibilidad de la información de los servicios, infraestructura, portales y aplicaciones de la ANDJE por ataques informáticos por no contar con un servicio para realizar la gestión y monitoreo de la seguridad informática.	Seguridad	CONTROL: Firewall RESPONSABLE: Asesor(a) de TI FRECUENCIA: Diaria TIPO DE CONTROL: Preventivo 25% NATURALEZA DEL CONTROL: Automático 25% CONTROL DOCUMENTADO: No EJECUCIÓN CONTROL: Configuración de políticas en el Firewall DESVIACIONES: Monitoreo de TI EVIDENCIAS: Reportes del Firewall CONTROL: Antivirus RESPONSABLE: Asesor(a) de TI FRECUENCIA: Diaria TIPO DE CONTROL: Preventivo 25% NATURALEZA DEL CONTROL: Automático 25% CONTROL DOCUMENTADO: No EJECUCIÓN CONTROL: Monitoreo de la consola de admiración DESVIACIONES: Monitoreo de TI EVIDENCIAS: Reportes del antivirus	Se evidencia la aplicación de los controles y el reporte del informe de acuerdo a la criticidad.

Fuente: Elaboración propia

En la revisión de riesgos se encuentra una no conformidad por Materialización de riesgo en el Proceso Gestión documental y no tratamiento de Riesgo desde el Proceso de Gestión de Tecnología, al ser el responsable de la Gestión de Riesgos de Seguridad de la Información incumpliendo los principios para el tratamiento de datos personales: (⋯)g) Principio de seguridad: La información sujeta a Tratamiento por el Responsable del Tratamiento o encargado de Tratamiento se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando adulteración, perdida, consulta, uso o acceso no autorizado o fraudulento. Ley 1581 de 2012.

Se recomienda que la tipificación de los riesgos de Seguridad de la Información esté alineada con la tipificación realizada en los activos de información, manteniendo el hilo conductor para el tratamiento de riesgo.

3. Activos de información proceso Gestión de Tecnologías de la Información

Tabla No 2 Activos de información asociados al proceso Gestión de Tecnologías de la Información

ID	Nombre Activo de Información	Tipo de Activo	Confidencialidad	Integridad	Disponibilidad	Nivel de criticidad
1	SWITCH CORE	Hardware	MA	MA	MA	**MA**
2	software sistema monitoreo de infraestructura tecnológica	Software	M	B	B	**B**
3	software directorio activo	Software	A	A	A	**A**
4	software de gestión de servicios de ti	Software	B	B	B	**B**

Agencia Nacional de Defensa Jurídica del Estado

5	Dispositivo de Almacenamiento	Software	A	A	A	**A**
6	Software y Servidor de Almacenamiento de Backup	Software	MA	MA	MA	**MA**
7	Plataforma para servidores virtuales de eKogui App	Software	MA	MA	MA	**MA**
8	servidores virtuales base de datos de la agencia	Software	M	A	M	**M**
9	servidor antivirus y cifrado	Software	B	B	B	**B**
10	servidor virtual sistema de gestión documental orfeo	Software	A	A	A	**A**
11	Servidor Virtual Sistema Conciliador	Software	M	M	M	**M**
12	SERVIDOR VIRTUAL SIGI	Software	M	B	M	**B**
13	SERVIDOR VIRTUAL PORTAL WEB	Software	MA	MA	MA	**MA**
14	SERVIDOR VIRTUAL MOODLE	Software	B	B	B	**B**
15	SERVIDOR VIRTUAL SKYPE	Software	B	M	M	**B**
16	Servidor virtual de administración de virtualización	Software	B	B	B	**B**
17	Servidor Físico de Virtualización Vmware	Hardware	M	M	M	**M**
18	Servidor Físico de Virtualización Hyper-V	Hardware	M	M	M	**M**
19	Servidor Físico de File Server	Hardware	MA	MA	MA	**MA**
20	Servicio Telefonía IP	Servicio	B	M	M	**B**
21	Servicio Portal Web	Servicio	A	A	A	**A**
22	Evidencias Riesgos de Seguridad de la Información	Información	M	M	M	**M**
23	Licencias de Software	Información	MB	A	B	**B**
24	INVENTARIO DE ACTIVOS, CLASIFICACIÓN Y PUBLICACIÓN DE INFORMACIÓN	Información	MB	M	M	**B**
25	Hoja de Vida de Servidores	Información	MB	B	B	**MB**
26	FIREWALL	Hardware	A	A	A	**A**
27	Plan de capacitación MSPI	Información	M	M	M	**M**
28	Correo electrónico	Servicio	A	A	A	**A**
29	Cintas de Backups	Software	A	A	A	**A**
30	Certificado Digital	Servicio	A	A	A	**A**
31	Bases de Datos Intranet	Software	A	A	A	**A**
32	Base de Datos Orfeo	Software	A	A	A	**A**
33	Base de Datos de Gestión de Servicios de TI	Software	A	A	A	**A**
34	Base de Datos Biométricos	Software	A	A	A	**A**
35	Administración documentación Técnica del Sistema Gestión Documental-Orfeo	Información	MB	M	B	**B**

Fuente: Elaboración propia

Se evidencia que se realizó la actualización de activos de información atendiendo las recomendaciones de la Auditoría anterior.

4. Planes de Mejoramiento

Tabla N° 3 Planes de mejoramiento asociados al proceso Gestión de Tecnologías de la Información

No	Hallazgo	Fecha	Observación
433	No se evidencia reporte al líder del proceso de los controles de los riesgos con la periodicidad que pide la Guía administración de riesgos ANDJE, con el objetivo de monitorear la no materialización.	30/06/2021	Se verifica cumplimiento de acciones
434	Se identifica que la valoración de los activos de información del Proceso es baja y media. Tratándose del proceso de gestión de TI, el cual es crítico, la calificación debe corresponder a los criterios establecidos en la Política Nacional De Seguridad Digital, dado que este es el insumo para la Gestión de Riesgos, Gestión de incidentes y el Plan de Continuidad de Negocio	30/06/2021	Se verifica cumplimiento de acciones

435	Se evidencia que para los funcionarios que ya venían vinculados con la Agencia, no se realizó la actividad de control establecida en el procedimiento que corresponde a la creación de caso y validación de permisos.	31/05/2021	Se verifica cumplimiento de acciones
436	Debilidad en la definición del indicador, dado que para los indicadores 88-PAI-20 94-PAI-20 y 97-PAI-20 no hay definidos entregables tangibles con una periodicidad que abarque toda la vigencia que haya sido presentado y aprobado por el Comité de Desempeño Institucional en las fechas establecida	31/12/2021	Se verifica cumplimiento de acciones
437	No se evidencia el autodiagnóstico y porcentaje de estado y avance de cada uno de los productos entregables del Modelo de Seguridad y Privacidad de la Información habilitador de la de la Política de Gobierno Digital	15/12/2021	Se verifica cumplimiento de acciones
438	No se evidencia acto administrativo en el cual se den lineamientos frente a la obligatoriedad de que todos los procesos de la Agencia soliciten autorización al Proceso Gestión de TI para gestionar cualquier proceso de adquisición de bienes o servicios con componente tecnológico.	30/09/2021	Se verifica cumplimiento de acciones
439	En el Procedimiento Gestión de incidentes no se evidencia la inclusión de niveles de escalamiento para un manejo Post-incidente.	31/12/2021	Se verifica cumplimiento de acciones
440	No se evidencia seguimiento trimestral al riesgo de Seguridad de la información y presentación de este seguimiento y de los riesgos residuales al Comité de Gestión y Desempeño.	31/10/2021	Se verifica cumplimiento de acciones
441	Se evidencia debilidad en el plan de mejoramiento suscrito correspondiente a las acciones No. 300, 302 y 303, dado que se repiten las situaciones evidenciadas, por lo que es necesario reformular el plan de mejoramiento, incluyendo las acciones necesarias para cumplir con la Política de Gobierno Digital y de Seguridad Digital	31/12/2021	Se verifica cumplimiento de acciones
442	No se evidencia la alineación de Los planes Estratégico de Tecnologías de la Información y las Comunicaciones PETI; el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan de Seguridad y Privacidad de la Información, con la estructura planteada en el Manual Operativo de MIPG.	31/12/2021	Se verifica cumplimiento de acciones
443	No se evidencia un plan de trabajo que contenga las Fases II. Implementación del protocolo IPv6 - Desarrollo del Plan de implementación y la fase III. Pruebas de funcionalidad de IPv6, aprobado por la Alta Dirección	30/06/2022	Se están gestionando los Proceso de Contratación
444	No se evidencia la existencia de capacidad de Arquitectura Empresarial que responda a los lineamientos impartidos por el Documento Maestro Modelo de Arquitectura Empresarial (mintic.gov.co)	15/12/2021	Se verifica cumplimiento de acciones
445	No se evidencia un Plan Estratégico de Tecnología y Sistemas de Información (PETI) que este alineado con el Modelo de Arquitectura Empresarial	31/07/2021	Se verifica cumplimiento de acciones
446	No se evidencia la implementación del Modelo de Gobierno de Tecnologías de la Información. Tarea asignada al Proceso Gestión de Tecnologías de Información en el Modelo Óptimo De Gobierno De Información.	31/07/2022	Se están gestionando los Proceso de Contratación
447	No se evidencia la creación de un Grupo interno de trabajo conformado por los siguientes roles, ejercidos por personas o equipos de la ANDJE con el objetivo de implementar el Gobierno TI y Gobierno de información - Equipo ejecutivo como patrocinador. - Gerencia del programa y proyectos de Gobierno de Información. - Especialistas de Tecnologías de Información. - Especialistas en gestión de riesgos - Especialistas de las unidades de negocio - Especialistas en Seguridad de la Información - Especialistas en Gestión Documental, - Especialistas en Gestión de Procesos - Especialistas en regulaciones	30/06/2022	Se están gestionando los Proceso de Contratación
448	Se evidencia que la Agencia no cuenta con un área estratégica de las Tecnologías y Sistemas de la Información y las Comunicaciones, que haga parte del comité directivo y dependa del nominador o representante legal de la misma, que tenga en sus responsabilidades los ámbitos de Servicios Tecnológicos, Estrategia Ti, Gobierno Ti, Sistemas De Información, Uso y Apropiación Y Seguridad Digital	30/06/2022	Se están gestionando los Proceso de Contratación
449	Se evidencia que en la Entidad existe duplicidad en los lineamientos en aspectos relacionados con desarrollo de software en los Procedimientos GI-P-09 Realizar Desarrollo Y Puesta En Marcha De Los Requisitos En El Sistema Único De Información Litigiosa Del Estado y GTI-P-03 V-0 Solicitud Y Aprobación De Nuevos Desarrollos O Mejoras De Software, lo que impide la estandarización de metodología desatendiendo los Propósitos de la Política de Gobierno Digital y la Metodología de desarrollo de sistemas de Información.	30/09/2021	Se verifica cumplimiento de acciones
450	No se evidencia un documento de diagnóstico y plan del Marco de interoperabilidad, que cumpla con lo estipulado en - Habilitador 3 Marco de interoperabilidad.	10/12/2021	Se verifica cumplimiento de acciones
451	No se evidencio Plan De Continuidad De Negocio, Plan de trabajo o documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	30/03/2022	Se esta gestionando con el proceso contractual actual No. 068-2021

452	No se evidencia el autodiagnóstico y plan para el cumplimiento del Modelo Nacional de Gestión de Riesgos de Seguridad Digital. Documentos revisados y aprobados por la alta Dirección. Orientados a implementar la Política de Seguridad digital	31/12/2021	Se verifica cumplimiento de acciones

Fuente: Elaboración propia

En la revisión realizada se observa que las no conformidades relacionadas con IPV6, Continuidad de Negocio y Gobierno de datos, permanecen pendientes por resolver, superando los plazos, que, por buenas prácticas, no deben exceder un año a partir del Informe de la última auditoría realizada.

Para la acción 449 se evidencia que no ha sido eficaz la acción dado que en la revisión realizada se observa que no se aplica el procedimiento publicado por el Proceso de Gestión de Tecnología parte de la DGI y de Planeación Estratégica

5. Cumplimiento a indicadores (PAI, PAAC y Gestión)

Tabla N° 4 Indicadores asociados al proceso Gestión de Tecnologías de la Información

Indicador	(%)	Detallle
Indicador:119-PAI-21 "Agencia para el ciudadano". CRM para la gestión de usuarios de la Agencia, implementado.	5%	Dado que el proceso fue declarado desierto en el mes de octubre de 2021, se dan a conocer las actividades con corte al 31 de diciembre de 2021, se realizan términos de referencia para la adquisición de suscripciones a Dynamics y a su vez contratación de recurso humano para la parametrización y configuración, los cuales han quedado con la NOB (no objeción del BID) y adelantar la contratación por Colombia Compra Eficiente en la vigencia 2022. No se cumplieron las 4 metas propuestas para 2021.
Indicador:120-PAI-21 Programa "Se seguro" diseñado e implementado.	100%	Para la vigencia 2021 se lograron los objetivos planteados para el programa SE SEGURO en lo que respecta verificación controles para el apoyo de trabajo en casa y campañas de sensibilización para la prevención de incidentes de seguridad de la información.
Indicador:121-PAI-21 100% de implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información alineada con la metodología DAFP y ANEXO 4 de Lineamientos de riesgos Digitales.	100%	De los riesgos identificados se resalta lo siguiente: · Se migraron 24 riesgos ya existentes a la nueva metodología de riesgos. · Se identificaron 18 nuevos riesgos con la nueva metodología. · Se realizó por primera vez el ejercicio de riesgos con los procesos Control de la Gestión, Control interno Disciplinario y Gestión del conflicto jurídico Internacional. · Los procesos con mayor número de riesgos identificados son Gestión de tecnologías de la Información y Gestión de Información de Defensa Jurídica. · Los riesgos de los procesos de Gestión del Conflicto Jurídico Nacional y Control de la Gestión aún están en revisión. · En el mes de noviembre se dará a conocer los riesgos identificados al CIDG para su aprobación. · En el mes de diciembre ya fueron aprobados los riesgos por cada uno de los líderes de procesos. En comité de CIDG del 29 de octubre de 2021 los riesgos fueron presentados y aprobados por la alta dirección.
Indicador:122-PAI-21 Incrementar en 5 pp la calificación del Modelo de Seguridad y Privacidad de la Información.	100%	Para la vigencia 2021 se lograron los objetivos planteados para seguridad de la información en lo que respecta actualización de los controles de la Declaración de Aplicabilidad, actualización de los documentos para activos y riesgos, se verificaron controles para el apoyo de trabajo en casa, se identificaron nuevos riesgos y activos de información, se impulsaron campañas de sensibilización y todo lo anterior en el marco del Sistema de Gestión de Seguridad de la Información y como complemento para el programa SE SEGURO de trabajo en casa.

Indicador:123-PAI-21 Implementación y seguimiento del mapa de ruta de los proyectos e iniciativas de tecnología de información -PETI 2021-2024.	100%	Allí se observa que se tienen unos proyectos por estructurar y otros para la vigencia 2023, lo del 2021 se tienen en proceso precontractual y otros en ejecución. De acuerdo a la tabla anterior tenemos que para el indicador (Porcentaje PA ejecutado / Porcentaje PA programado) = 39% De lo cual tenemos como resumen: Cinco (9) adjudicados Doce (8) etapa precontractual Seis (6) por estructurar
Indicador:124-PAI-21 96% de las vulnerabilidades identificadas en 2021, subsanadas.	100%	No se identificaron brechas de seguridad en el portal web de la Agencia de categoría crítica por lo anterior no fue necesario hacer subsanaciones, sin embargo, para la vigencia 2022 se repetirá el ejercicio de análisis de vulnerabilidades incluyendo los siguientes elementos: • Sistemas de información Ekogui, Orfeo y Comunidad Jurídica • Portales (Internet e Intranet) • Infraestructura de comunicaciones y red (Firewalls y Access Point) • Servidores de apoyo (antivirus, bases de datos, aplicativos). • Carpetas compartidas (File Server).
Indicador:125-PAI-21 100% Identificación estrategia de continuidad del negocio FASE 1 para la Entidad.	100%	De manera preliminar se identificaron tres estrategias: 1. Tener un sitio alterno que soporte la infraestructura y sistemas críticos de la entidad. 2. Incorporar un modelo en la NUBE para todos los sistemas críticos de la entidad. 3. Tener un hibrido entre sitio alterno y nube para la infraestructura y sistemas críticos de la entidad. Por lo anterior, con la UT- PWC/ CROSS BORDER TECHNOLOGY se revisará en la vigencia 2022 cuál debe ser la estrategia que se debe documentar e implementar. En la vigencia 2021 se entregó este insumo a la UT- PWC/ CROSS BORDER TECHNOLOGY el cual será la base para documentar el Plan de Continuidad de la Agencia en la vigencia 2022.
Indicador:126-PAI-21 Infraestructura técnica para el monitoreo y prevención de ataques informáticos actualizada.	100%	Se incorporaron tres elementos al SOC los cuales ya están siendo monitoreados y se continua con la configuración de nuevos elementos.
Indicador:148-PAI-21 Calificación del Modelo de Seguridad y Privacidad de la Información	100%	Para la vigencia 2021 se lograron los objetivos planteados para seguridad de la información en lo que respecta actualización de los controles de la Declaración de Aplicabilidad, actualización de los documentos para activos y riesgos, se verificaron controles para el apoyo de trabajo en casa, se identificaron nuevos riesgos y activos de información, se impulsaron campañas de sensibilización y todo lo anterior en el marco del Sistema de Gestión de Seguridad de la Información y como complemento para el programa SE SEGURO de trabajo en casa. Con lo anterior se alcanzó la meta propuesta del 91%

Fuente: Elaboración propia

6. Seguimiento Contractual

Se realiza una validación de la contratación realizada por el Proceso *Gestión de Tecnologías de la Información*

Tabla N° 5 Contratación asociados al proceso Gestión de Tecnologías de la Información

No.	DESCRIPCIÓN	MONTO	ESTADO
1	135. Contratar servicios para realizar la gestión y monitoreo de la Seguridad Informática sobre la plataforma tecnológica de la Agencia Nacional de Defensa Jurídica del Estado a través de un Centro de Operaciones de Seguridad (SOC); así mismo la prestación del servicio de análisis de vulnerabilidades (Ethical hacking) de los diferentes activos de software y hardware de la entidad, mediante el uso y aplicación de metodologías y herramientas especializadas.	$ 520.400.000	Ejecutado

Agencia Nacional de Defensa Jurídica del Estado

2	136. Contratar el servicio de consultoría para optimizar el Modelo de Gestión de Seguridad y Privacidad de la información y sistema de continuidad del negocio con base en lo definido en la norma técnica ISO27001, ISO 22301 y los lineamientos del gobierno nacional en materia de seguridad y privacidad de la información y Gobierno Digital.	$ 220.000.000	Ejecutado
3	201. Adquirir las licencias de Power BI Embebed para poder publicar y dar acceso a los usuarios del sistema eKOGUI de las consultas y cruces de la información a través de los cubos multidimensionales desarrollados.	$ 45.000.000	Ejecutado
4	217. Prestar servicios profesionales como consultor especializado en tecnología para apoyar y asesorar en el levantamiento de requisitos técnicos y adquisiciones en materia de tecnologías de la información y comunicaciones de la Agencia Nacional de Defensa jurídica del Estado.	$ 84.000.000	Ejecutado
5	239. Prestar servicios profesionales especializados para apoyar desde la secretaria general TI en el diagnóstico, análisis, formulación, seguimiento de las iniciativas de las áreas misionales de la agencia en relación con las tecnologías de la cuarta revolución industrial 4.0 y de las priorizadas en el PETIC.	$ 42.290.000	Ejecutado
6	120. Prestar servicios profesionales para apoyar a la Agencia Nacional de Defensa Jurídica del Estado, en la ejecución de actividades relacionadas con el soporte, administración y mantenimiento de la plataforma colaborativa y de comunicaciones Microsoft SharePoint.	$ 57.000.000	Ejecutado
7	121. Adquirir Servicios BPO y/o Mesa de ayuda de tecnología que permita garantizar la operación de los sistemas misionales y de apoyo, por medio de Acuerdo Marco en la Tienda Virtual del Estado Colombiano para la Entidad.	$ 240.000.000	Ejecutado
8	122. Renovar licencias de uso SAS, así como la prestación del servicio de asistencia y soporte técnico de las mismas.	$ 113.000.000	Ejecutado
9	123.Renovar el licenciamiento Microsoft con los productos de ofimática en su modalidad de licenciamiento Open Gov Lic/SA y de comunicaciones unificadas Microsoft Teams, con los respectivos derechos de actualización y servicio en la nube.	$ 125.000.000	Ejecutado
10	124. Adquirir y renovar el licenciamiento Microsoft con los productos de ofimática en su modalidad de licenciamiento Open Gov Lic/SA, con los respectivos derechos de actualización.	$ 200.000.000	Ejecutado
11	125. Renovación del soporte y garantía de las licencias para el sistema eKogui como son Enterprise Architect Corporate Edition y Jira Software de acuerdo a las especificaciones técnicas establecidas por la Entidad.	$ 20.000.000	Ejecutado
12	127. Prestar servicios profesionales para apoyar a la Agencia Nacional de Defensa Jurídica del Estado en la administración, mantenimiento y soporte técnico del sistema de gestión documental ORFEO, así como en los desarrollos que sobre esta plataforma requiera la Entidad.	$ 75.000.000	Ejecutado
13	128. Contratar los servicios de conectividad para la Agencia Nacional de Defensa Jurídica del Estado, a través de la tienda virtual del Estado, de acuerdo con los requerimientos técnicos exigidos por la Agencia.	$ 35.000.000	Ejecutado
14	132. Renovar licencias y actualización del uso de DLP, antivirus, así como la prestación del servicio de asistencia y soporte técnico de las mismas.	$ 71.000.000	Ejecutado
15	197. Adquirir Servicios BPO y/o Mesa de ayuda de tecnología que permita garantizar la operación de los sistemas misionales y de apoyo, por medio de Acuerdo Marco en la Tienda Virtual del Estado Colombiano para la Entidad.	$ 130.000.000	Ejecutado
16	198. Adquirir licenciamiento Microsoft Office 365 E1 con los productos de correo y teams en su modalidad de licenciamiento por suscripción.	$ 5.500.000	Ejecutado
17	242. Prestar servicios profesionales para apoyar a la Agencia Nacional de Defensa Jurídica del Estado en la administración, mantenimiento y soporte técnico del Sistema de Gestión Documental ORFEO, así como en los desarrollos que sobre la plataforma requiera la Entidad.	$ 20.000.000	Ejecutado
18	251. Renovar suscripción de software Adobe Creative Cloud y adicionar una nueva licencia para la elaboración de las actividades misionales de producción del material gráfico y audiovisual necesario para la divulgación de la información de la Entidad.	$ 10.000.000	Ejecutado
19	162. Adquirir una solución CRM, en la modalidad de software como servicio (SAAS), para fortalecer el relacionamiento de la ANDJE con sus actores: entidades públicas del orden nacional, territorial, ciudadanos y otros grupos de valor, en su rol de líder del Sistema de Defensa Jurídica del Estado	$ 1.797.392.370	Sin ejecutar
20	98. Adquirir, implementar y poner en funcionamiento un software que permita la automatización de los trámites de Secretaría General	$ 200.000.000	Sin ejecutar

21	207. Diseñar el modelo de Gobierno y Gestión TIC, Framework de Información, definición del Modelo de Gobierno de Datos, diseño de la Arquitectura de Referencia y de solución para los Sistemas de Información de la ANDJE	$ 592.000.000	Sin ejecutar
22	216. Adquirir direccionamiento IPV6 para la transición de las aplicaciones de la Agencia de IPV4 al nuevo protocolo	$ 20.000.000	Sin ejecutar
23	218. Adquirir licencias de Balsamiq Mockups como aplicación de escritorio a nombre de la Agencia Nacional de Defensa Jurídica del Estado	$ 1.300.000	Sin ejecutar
24	231. Adquirir una solución CRM, en la modalidad de software como servicio (SAAS), para fortalecer el relacionamiento de la ANDJE con sus actores: entidades públicas del orden nacional, territorial, ciudadanos y otros grupos de valor, en su rol de líder del Sistema de Defensa Jurídica del Estado	$ 530.000.000	Sin ejecutar
25	241. Adquirir licencias de Balsamiq Mockups como aplicación de escritorio a nombre de la Agencia Nacional de Defensa Jurídica del Estado	$ 1.500.000	Sin ejecutar
	Total	$ 5.155.382.370	

Fuente: Elaboración propia

Se evidencia que del 100% del presupuesto incluido en el Plan Anual de Adquisiciones de 2021 se ejecutó un 39%, esto equivale a la no ejecución de 7 procesos de 25 planeados. Recalcando que estos 7 procesos no se logró su ejecución por temas precontractuales (procesos desiertos 4, terminación mutuo acuerdo 1 y por análisis optimización de presupuesto y alineación con la Arquitectura empresarial de la entidad 2) que son variables que no controla la Agencia.

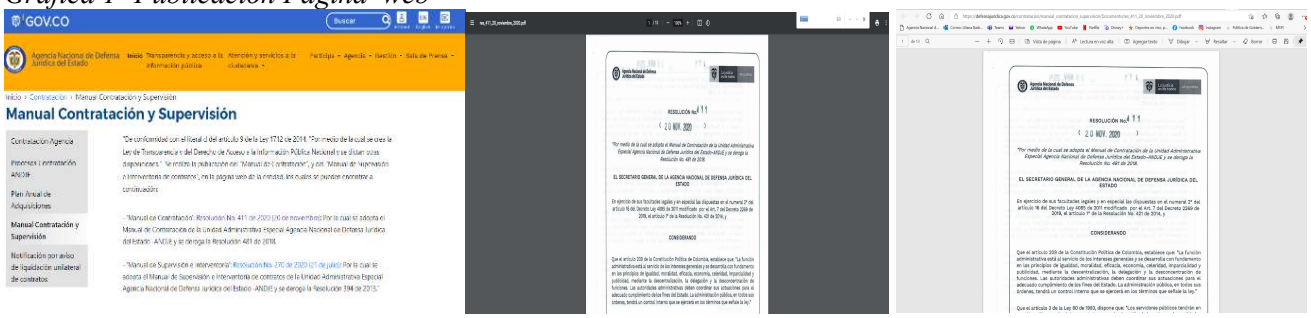
7. Seguimiento al cumplimiento de la Resolución 1519 de 2020

7.1 Seguimiento Anexo 1 - Accesibilidad Pagina Web De La Agencia Nacional De Defensa Jurídica Del Estado

7.1.1. En el marco del cumplimiento a las disposiciones de Ley de Transparencia y Acceso a la Información Pública, de la Política de Gobierno Digital y específicamente, lo concerniente a criterios de accesibilidad referidos por la Norma Técnica Colombiana de Accesibilidad de Sitios Web (NTC) 5854, se evidencia en el presente análisis el estado actual de la página web de la ANDJE y su nivel de cumplimiento del Nivel AA de accesibilidad, verificando el cumplimiento con el estándar

7.1.2. Verificando el "*Numeral 3.3. Documentos Pdf: Debe garantizarse que en el proceso de creación del documento PDF se ha etiquetado. Esto significa que mediante un proceso automático o manual se ha hecho que cada elemento (párrafo, tabla, lista, título, etc.) es realmente el elemento que corresponde y cuente con sus parámetros y características. Los documentos PDF no etiquetados no es posible leerlos con lectores de pantalla. La mejor opción para lograr la accesibilidad es que el etiquetado se haga desde la conformación original del documento. En el procesador de textos puede indicarse el guardado en formato PDF a través de la opción Guardar como … y eligiendo este formato puede encontrarse por Opciones, "Etiqueta de la estructura para accesibilidad", cuya opción debe estar activada, con lo que se almacenará el etiquetado y el documento abrirá directamente en el lector de estos archivos sin necesidad del proceso de etiquetado automático.3.4. Documentos y plantillas para presentaciones*"

Grafica 1- Publicación Pagina web

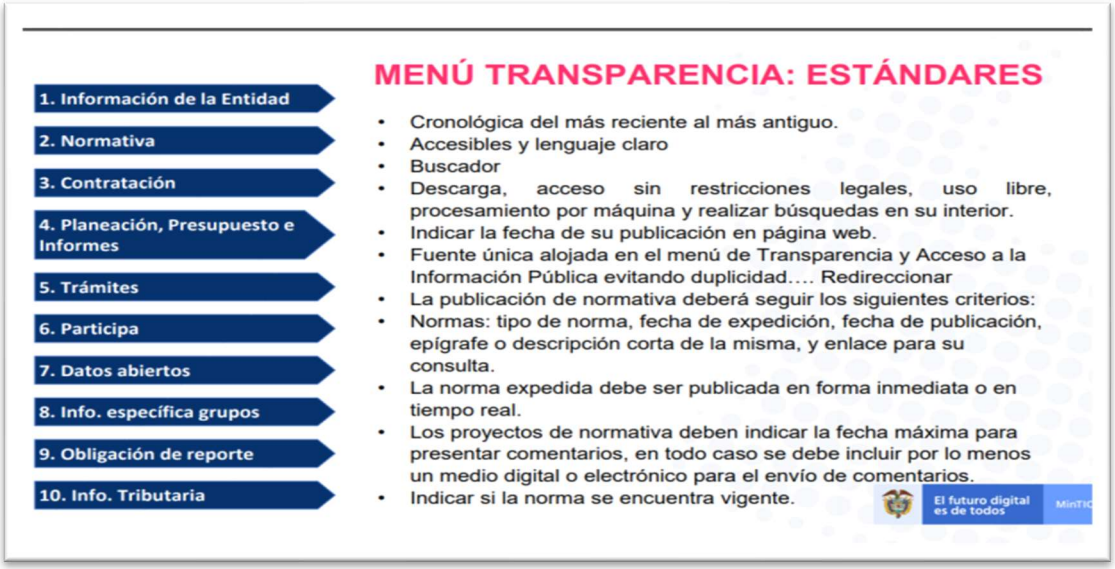


Fuente Pagina web ANDJE

Se evidencia que no es posible realizar la búsqueda en los documentos publicados. res_411_20_noviembre_2020.pdf (defensajuridica.gov.co); res_270_21_julio_2020.pdf (defensajuridica.gov.co)

7.2 Seguimiento Anexo 2 Estándares de publicación y divulgación de contenidos e información

La Resolución 1519 de 2020 tiene por objeto expedir los lineamientos que deben atender los sujetos obligados para cumplir con la publicación y divulgación de la información señalada en la Ley 1712 del 2014, estableciendo los criterios para la estandarización de contenidos e información. Cumpliendo con los siguientes estándares:

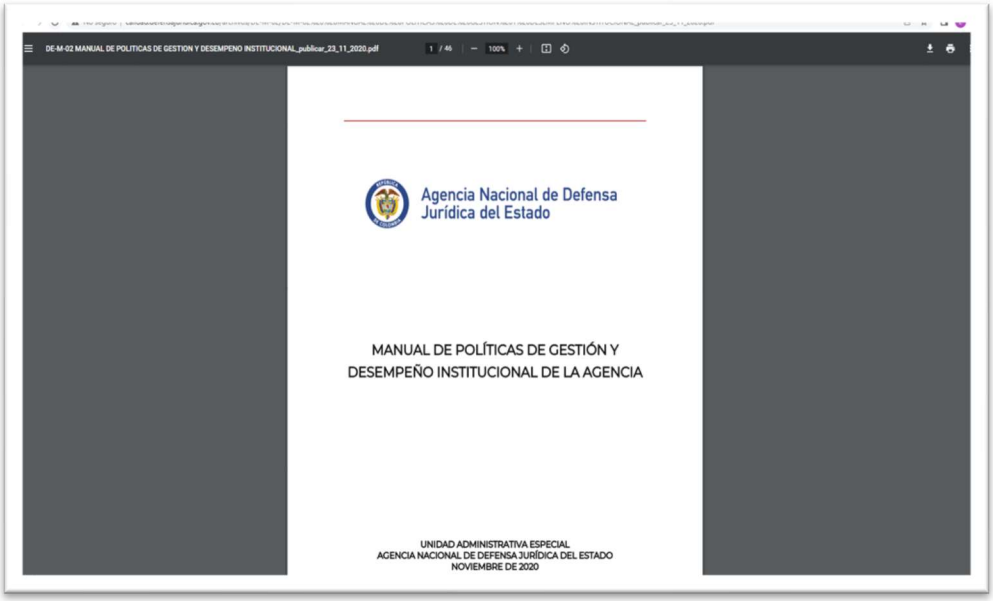


Fuente MINTIC

7.3 Seguimiento Anexo 3 Seguridad Digital

Con respecto a lo establecido en el anexo 3 que contiene las condiciones mínimas técnicas y de seguridad digital aplicables a los sujetos obligados en sus sitios web, se observó que una de las condiciones mínimas establece: "Garantizar conexiones seguras a través de uso de certificados, SSL (HTTPS para la confianza de usuarios) ", lo cual no está siendo aplicado teniendo en cuenta los problemas que se presentan al descargar archivos servidos a través de HTTP utilizando como navegador Google Chrome, Se adjunta imagen donde se evidencia que el manual de políticas, se encuentra sin certificados de seguridad como se observa en la siguiente imagen. http://calidad.defensajuridica.gov.co/archivos/DE-M-02/DE-M-02%20%20MANUAL%20DE%20POLITICAS%20DE%20GESTION%20Y%20DESEMPENO%20INSTITUCIONAL_publicar_23_11_2020.pdf

Grafica 4 - Conexiones seguras



Fuente Pagina web ANDJE

7.4 Seguimiento Anexo 4 Requisitos mínimos de publicación de datos abiertos

Se verifica y existe el plan de apertura, mejora y uso de datos abiertos incluye las siguientes actividades - Identificar Analizar Priorizar y Programar

8. Seguimiento Resolución 500

Se verifica y la Agencia tiene un plan para adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital.

Se recomienda implementar la Guía de borrado seguro para que sea aplicada en ambiente de desarrollo, actualmente está en ambiente de producción

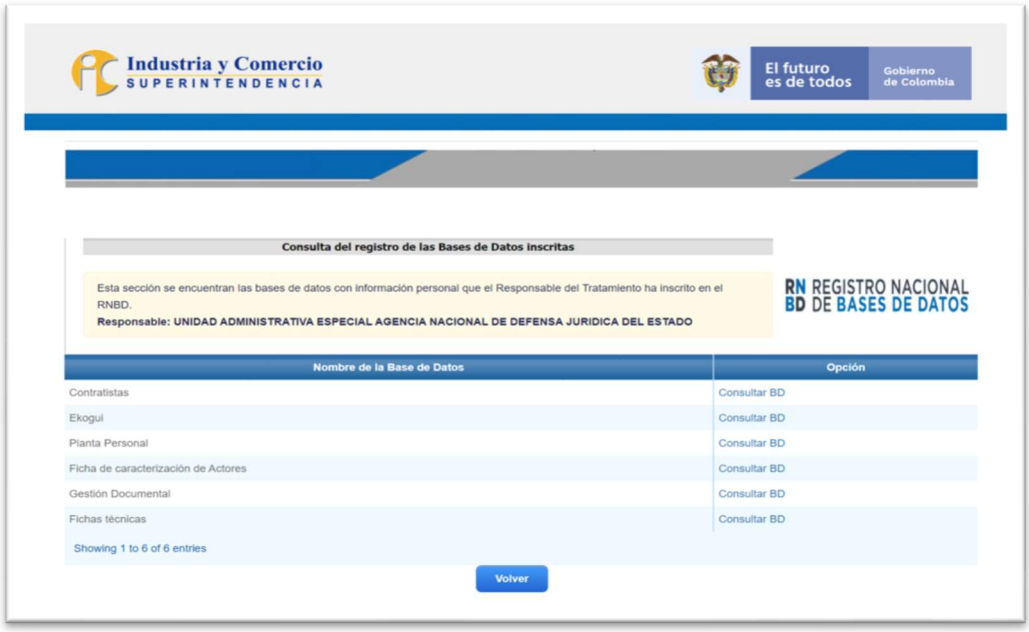
9. Verificación del Normograma

Según el procedimiento de mejora continua se debe realizar una actualización mensual, si aplica. Al verificar en SIGI la última actualización del normograma de Gestión de Tecnologías de la Información es de 2020.

10. Inscripción de bases de datos en la SIC

Referente al registro nacional de bases de datos que se reporta ante la SIC (https://rnbd.sic.gov.co/sisi/consultaTitulares/baseDatos/199042/) las que están registradas son las siguientes:

Grafica N° 5 Registro Bases De Datos



Fuente Pagina SIC

Teniendo en cuenta que según La *Ley 1581 de 2012 o Régimen General de Protección de Datos Personales se deben registrar son aquellas que contengan datos personales cuyo Tratamiento automatizado o manual se realice por personas naturales o jurídicas, de naturaleza pública o privada, en el territorio colombiano o fuera de él, en este último caso, siempre que al Responsable del Tratamiento o al Encargado del Tratamiento le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.*

Dado lo anterior faltaría la base de datos de la comunidad jurídica del conocimiento

11.Cumplimiento recomendaciones FURAG

Tabla N° 7 Recomendaciones FURAG

#	Política	Recomendaciones
1	Gobierno Digital	Utilizar técnicas de analítica de datos para soportar la toma de decisiones en la entidad (analítica prescriptiva).
2	Gobierno Digital	Incorporar, en el esquema de gobierno de tecnologías de la información (TI) de la entidad, la estructura organizacional del área de TI.
3	Gobierno Digital	Adoptar en su totalidad el protocolo IPV6 en la entidad.
4	Gobierno Digital	Elaborar un plan de direccionamiento para la adopción del Protocolo de Internet versión 6 (IPV6) en la entidad.

5	Gobierno Digital	Elaborar un plan de contingencias para la adopción del Protocolo de Internet versión 6 (IPV6) en la entidad.
6	Gobierno Digital	Elaborar un documento de diseño detallado de la implementación del Protocolo de Internet versión 6 (IPV6) en la entidad.
7	Gobierno Digital	Elaborar informes de las pruebas piloto realizadas para la implementación del Protocolo de Internet versión 6 (IPV6) en la entidad.
8	Gobierno Digital	Elaborar informes de activación de políticas de seguridad para la implementación del Protocolo de Internet versión 6 (IPV6) en la entidad.
9	Gobierno Digital	Elaborar un documento de pruebas de funcionalidad para la implementación del Protocolo de Internet versión 6 (IPV6) en la entidad.
10	Gobierno Digital	Elaborar un acta de cumplimiento a satisfacción de la entidad sobre el funcionamiento de los elementos intervenidos en la fase de implementación del Protocolo de Internet versión 6 (IPV6).
11	Gobierno Digital	Utilizar tecnologías emergentes de cuarta revolución industrial para mejorar la prestación de los servicios de la entidad, como tecnologías de desintermediación, DLT (Distributed Ledger Technology), cadena de bloques (Blockchain) o contratos inteligentes, entre otros.
12	Gobierno Digital	Utilizar tecnologías emergentes de cuarta revolución industrial como el análisis masivo de datos (Big data) para mejorar la prestación de los servicios de la entidad.
13	Gobierno Digital	Utilizar tecnologías emergentes de cuarta revolución industrial como la inteligencia artifical (AI) para mejorar la prestación de los servicios de la entidad.
14	Gobierno Digital	Utilizar tecnologías emergentes de cuarta revolución industrial como el internet de las cosas (IoT) para mejorar la prestación de los servicios de la entidad.
15	Gobierno Digital	Utilizar tecnologías emergentes de cuarta revolución industrial como la robótica para mejorar la prestación de los servicios de la entidad.
16	Gobierno Digital	Utilizar tecnologías emergentes de cuarta revolución industrial como la automatización robótica de procesos para mejorar la prestación de los servicios de la entidad.
17	Gobierno Digital	Ejecutar al 100% los proyectos de TI que se definen en cada vigencia.
18	Gobierno Digital	Emplear diferentes medios digitales en los ejercicios de participación realizados por la entidad.
19	Gobierno Digital	Utilizar medios digitales en los ejercicios de rendición de cuentas realizados por la entidad.
1	Seguridad Digital	Fortalecer las capacidades en seguridad digital de la entidad a través de convenios o acuerdos de intercambio de información para fomentar la investigación, la innovación y el desarrollo de temas relacionados con la defensa y seguridad nacional en el entorno digital.
2	Seguridad Digital	Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como realizar la identificación anual de la infraestructura crítica cibernética e informar al CCOC.
3	Seguridad Digital	Efectuar evaluaciones de vulnerabilidades informáticas.
4	Seguridad Digital	Realizar retest para verificar la mitigación de vulnerabilidades y la aplicación de actualizaciones y parches de seguridad en sus sistemas de información.
5	Seguridad Digital	Realizar periódicamente ejercicios simulados de ingeniería social al personal de la entidad incluyendo campañas de phishing, smishing, entre otros, y realizar concientización, educación y formación a partir de los resultados obtenidos.

Fuente: Elaboración Propia

El Decreto 1083 de 2015, compilatorio del Decreto Único Sectorial de Función Pública, estableció los lineamientos generales para la integración de la Planeación y la Gestión Pública. En este se estipula la adopción del Modelo Integrado de Planeación y Gestión como instrumento de articulación y reporte de la planeación.

Considerando que el Formulario Único Reporte de Avances de la Gestión (FURAG) es una herramienta en línea de reporte de avances de la gestión, como insumo para el monitoreo, evaluación y control de los resultados institucionales y sectoriales

La Resolución 1126 de 2021 la cual modifica la Resolución 2710 de 2017 en cuanto al Plazo de adopción protocolo IPv6 el cual debe responder a los siguientes criterios.

Grafica N° 6 – Requerimientos IPV6

Fuente MINTIC

Agencia Nacional de Defensa Jurídica del Estado

PRINCIPALES SITUACIONES DETECTADAS/ RESULTADOS DE LA AUDITORÍA / RECOMENDACIONES:

Para la elaboración del informe final se tienen en cuenta los comentarios y observaciones brindadas por el Proceso en mesa de trabajo realizad el día 27 de febrero de 2022.

N°	REQUISITO	NO CONFORMIDAD	OBSERVACIONES
1	Decreto 1244 de 2021 ISO 9001 2015 - Una herramienta comúnmente usada es la caracterización de procesos**,** herramienta usada para describir cómo funciona un proceso y así dar cumplimiento a los requisitos de la norma.		Se evidencia que en la Caracterización no se registra actividad para la generación de lineamientos, políticas y directrices. Así mismo, en la Caracterización, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, - y el Plan de Seguridad y Privacidad de la Información no están incluidos.
2	GTI-P-05 Gestión de Incidentes de seguridad	Se evidencia que como resultado de la auditoria de gestión al proceso de Gestión Documental se informó de un incidente de seguridad de la información, por afectación a la privacidad y confidencialidad de los expedientes asociados o relacionados de Talento Humano con datos personales, a través del Informe de Auditoría, al cual no se le dio el tratamiento referido en el presente procedimiento.	
3	Guía Administración De Riesgos MC-F-10 V-0	Se evidencia una materialización de riesgos de seguridad de la información, por afectación a la Privacidad y confidencialidad del expediente digital de Talento Humano relacionado con datos personales, por una inadecuada gestión del sistema de información ORFEO. No se tienen establecidos controles que garanticen el cumplimiento necesario para mitigar el riesgo de este activo de información, por el desconocimiento o falta de compromiso por parte del personal responsable, para evitar aquellas situaciones que pueden afectar la disponibilidad, integridad y confidencialidad de la información.	
4	MANUAL OPERATIVO DE MIPG - Los aspectos clave para el Sistema de Control Interno SCI a tener en cuenta por parte de la 1ª Línea: (…). El seguimiento a los indicadores de gestión de los procesos e		Se observa que las no conformidades relacionadas con IPV6, Continuidad de Negocio y Gobierno de datos, permanecen pendientes por resolver, superando los plazos, que, por buenas

	institucionales, según corresponda. La formulación de planes de mejoramiento, su aplicación y seguimiento para resolver los hallazgos presentados.		prácticas, no deben exceder un año a partir del último Informe de la auditoria.
5	Resolución 1519 Anexo 1 3.3. Documentos Pdf Debe garantizarse que en el proceso de creación del documento PDF se ha etiquetado. Esto significa que mediante un proceso automático o manual se ha hecho que cada elemento (párrafo, tabla, lista, título, etc.) es realmente el elemento que corresponde y cuente con sus parámetros y características.	Se evidencia que en dos documentos descargados no es posible realizar la búsqueda dentro del documento. res_411_20_noviembre_2020.pdf (defensajuridica.gov.co) res_270_21_julio_2020.pdf (defensajuridica.gov.co)	
6	Resolución 1519 - Anexo 3 Seguridad Digital	Se evidencia que al descargar el documento de la página web de la Agencia, baja con mensaje de sitio no seguro, desatendiendo los requerimientos de seguridad establecidos en el Anexo 3. http://calidad.defensajuridica.gov.co/archivos/DE-M-02/DE-M-%20%20MANUAL%20DE%20POLITICAS%20DE%20 GESTION%20Y%20DESEMPENO%20INSTITUCIONAL_publicar_23_11_2020.pdf	
7	Decreto Único 1074 de 2015, capítulo 26, reglamentó la información mínima que debe contener el RNBD y los términos y condiciones bajo los cuales se deben inscribir en éste las bases de datos sujetas a la aplicación de la Ley 1581 de 2012.	No se evidencia el Registro de base de datos de la comunidad jurídica del conocimiento ni lineamiento que consigne una verificación y seguimiento de las bases publicadas.	
8	Decreto 1008 de 2018 y el Modelo de Gestión y Gobierno de TI 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.	Se evidencia que del 100% del presupuesto incluido en el Plan Anual de Adquisiciones de 2021 se ejecutó un 39%, esto equivale a la no ejecución de 7 procesos de 25 planeados. Recalcando que estos 7 procesos no se logró su ejecución por temas precontractuales (procesos desiertos 4, terminación mutuo acuerdo 1 y por análisis optimización de presupuesto y alineación con la Arquitectura empresarial de la entidad 2).	

RECOMENDACIONES:

- Se recomienda incluir en el Procedimiento de Gestión de Incidentes como fuente de ingreso de reportes a los agentes externos, los informes de auditoría entre otros.
- Se recomienda implementar el formato de base de conocimientos de incidentes de seguridad de la información, como insumo número 1 para la etapa de análisis en el Procedimiento de Gestión de Incidentes.
- Se recomienda que la tipificación de los riesgos de Seguridad de la Información esté alineada con la tipificación realizada en los activos de información, manteniendo el hilo conductor para el tratamiento de riesgo.
- Se recomienda documentar en un proceso o documentos del Proceso la obligatoriedad de pruebas de testeo o ethical hacking de todas las aplicaciones nuevas.
- Se recomienda actualizar el normograma, actualización mensual según procedimiento de mejora continua,
- se recomienda socializar los lineamientos de obligatoriedad de centralización por parte de la Oficina Asesora de Sistemas y Tecnologías de Información de todos los procesos de adquisición o desarrollo de software
- Se recomienda atender las recomendaciones realizadas en el informe de FURAG correspondiente a la Política de Gobierno Digital con el objetivo de subir en los índices de calificación.

CONCLUSIONES DE LA AUDITORÍA

Dentro del proceso de auditoria se pudo concluir:

Que los controles establecidos para la administración del proceso Gestión de Tecnologías de la Información, cumplen con el objetivo para el cual fueron diseñados, por tanto, son adecuados para reducir la posibilidad de materialización de riesgos.

El cumplimiento de las actividades del control por parte del Proceso, lo que contribuye a la mejora continua.

Se resalta el compromiso del Grupo de trabajo responsable del Proceso, en calidad y oportunidad, para atender la auditoria como un asunto prioritario.

Para constancia se firma en Bogotá D.C., a los 14 del mes de marzo de 2022

Luis E. Hernández León
Jefe de la Oficina de Control Interno
Elaboro: Liliana Barbosa Carrillo - Gestor