Agencia Nacional de Defensa Jurídica del Estado

INFORME DE AUDITORIA INTERNA

FECHA DE EMISIÓN DEL INFORME	Día:	21	Mes:	12	Año:	2022
FECHA EJECUCIÓN DE LA AUDITORIA	Desde:	1/11/2022		Hasta:	30/11/2022	

Aspecto Evaluable (Unidad Auditable):	Auditoria al proceso de Gestión de Tecnologías de la Información (A-P-GTI-22)
Líder de Proceso:	Oswaldo Useche Acevedo.
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 febrero de 2022 y 31 de octubre de 2022.
Criterios de la Auditoría:	• Ley 1712 de 2014 Ley de Transparencia. • Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. • Ley 1955 de 2019 Plan nacional de desarrollo 2018-2022. • Ley 1978 de 2019 Se moderniza el sector de las Tecnologías de la Información y las Comunicaciones (TIC). • Ley 2052 de 2020 Servicios ciudadanos digitales - racionalización de trámites. • Ley 2080 de 2021 - Se reforma el Código de Procedimiento Administrativo y de lo Contencioso Administrativo. • Decreto Ley 4085 de 2011. Por el cual se establecen los objetivos y la estructura de la ANDJE. • Decreto 1069 de 2015. Decreto Único Reglamentario del Sector Justicia y del Derecho. • Decreto 1078 de 2015 – Decreto Único Reglamentario del Sector TIC. • 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 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. • 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. • Decreto 620 de 2020 - Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública - Sedes electrónicas. • Decreto 1244 de 2021 creación de la Oficina Asesora de Sistemas y Tecnologías de la información en la ANDJE. • Decreto 767 de 2022 - "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015. • Decreto 338 de 2022 - Fortalecer la Gobernanza de seguridad digital. • Decreto 088 de 2022 - Estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea.

	• Directiva presidencial 02 de 2019. Simplificación De La Interacción Digitalmente Los Ciudadanos Y El Estado - Portal Único GOV.CO. • Directiva presidencial 03 de 2021 Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos. • Resolución 746 de 2022 se fortalece el Modelo de Seguridad y privacidad de la información • Resolución 1519 de 2020 Información y seguridad Digital. • Resolución 2893 de 2020 Estandarizar ventanillas únicas, portales específicos de programas transversales, sedes electrónicas, trámites, OPAs y consultas de acceso a información. • 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. • 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. • Resolución 527 del 4 de agosto de 2022, por el cual se adopta el Nuevo Sistema Integrado de Gestión Institucional – SIGI – en la ANDJE. • Resolución 1126/21, Modifica la Resolución 2710 de 2017 Plazo de adopción protocolo IPv6. • 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. • CONPES 3975 de Política Nacional Para La Transformación Digital E Inteligencia Artificial • CONPES 3995 de 2020 Política Nacional De Confianza Y Seguridad Digital.

LIMITACIONES PARA EL DESARROLLO DE LA AUDITORIA:

No se presentaron.

PLAN DE MUESTREO:

Se verifica la información suministrada por el 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 a 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 el proceso de Gestión de Tecnologías de la Información.
2. Mapa de riesgos de Corrupción.
3. Mapa de riesgos de Seguridad de la Información.
4. Mapa de aseguramiento.
5. GTI-P-01 Procedimiento Gestión de solicitudes.
6. GTI-P-03 – V2 Solicitud y Aprobación de Nuevos Desarrollos o Mejoras de Software.
7. GTI-P-05 – V2 Gestión de Incidentes de Seguridad de la Información.
8. 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".

Se realiza la verificación del cumplimiento de las actividades y puntos de control establecidos en los Procedimientos GTI-P-01, GTI-P-03 y en la Guía GTI-G-12 en el marco de la adquisición, publicación y funcionamiento de los Sistemas de Información "*Comunidad Jurídica del Conocimiento", "Comprueba" y "Biblioteca de Defensa Jurídica (Biblioteca Virtual)"*, los cuales se encuentran publicados en la Página Web de la Agencia.

Imagen N° 1 - Aplicativos publicados en Web

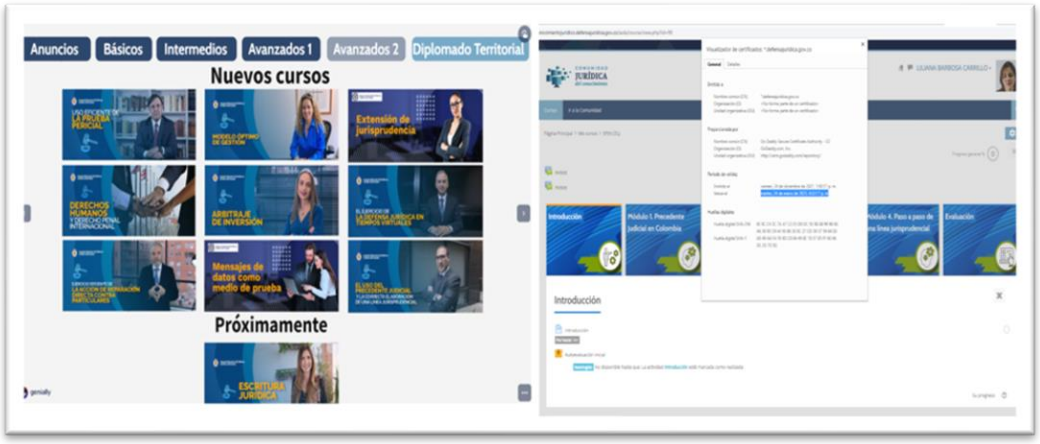
Fuente: Pagina Web Agencia

1.1 Comunidad Jurídica Del Conocimiento – Responsable Dirección de Políticas y Estrategias

Se verifican los 6 cursos entregados en la vigencia 2022 producto de las consultorías:

- 035-2021 Estructurar y virtualizar los contenidos de seis cursos bajo el alcance definido por la Agencia Nacional De Defensa Jurídica Del Estado y optimizar la plataforma de aprendizaje de la Comunidad Jurídica Del Conocimiento.
- 052-2021 Optimización del portal digital de la Comunidad Jurídica Del Conocimiento y desarrollo de herramientas e-learning para garantizar la cobertura, calidad e impacto de los programas especializados de entrenamiento en el Sistema De Defensa Jurídica Del Estado.

Imagen N° 2 - Cursos publicados en la CJC



Fuente: Pagina Web ANDJ

Se realiza la verificación de:

- El cumplimiento del Procedimiento GTI-P-03 *Solicitud Y Aprobación De Nuevos Desarrollos o Mejoras De Software*, evidenciando que no se sigue el lineamiento dado en los numerales del 6 al 18, al no contar con los soportes correspondientes a:

  - *Solicitud de servicio en el sistema de gestión de servicios de tecnología.*
  - *Formato Requerimiento de desarrollo GTI-F-09 diligenciado.*
  - *Aceptación verificación de Viabilidad del nuevo desarrollo.*
  - *Formato Análisis y propuesta de desarrollo GTI-F-12 aceptada.*

- El cumplimiento de la Guía para Desarrollo de Software Seguro Numeral 4. Desarrollo Técnico a continuación, se describen los lineamientos a tener presente para el desarrollo, mantenimiento o adquisición de software para la Agencia Nacional de Defensa Jurídica del Estado - ANDJE, para establecer requisitos de seguridad. Pruebas de Seguridad y Aceptación. Cuando se realizan cambios al sistema hacer pruebas:

  Aceptación de usuario.
  Autenticación.
  Autorización.
  Validación de Entrada de Datos.

  Pruebas periódicas:
  Pruebas de vulnerabilidades.
  Pruebas de estrés.
  Gestión de Cookies.
  Pruebas de carga.
  Hardening.

  Realizar por lo menos una vez las pruebas OWASP de:
  Pérdida de Autenticación y Gestión de Sesiones.
  Secuencia de Comandos en Sitios Cruzados (XSS).
  Configuración de Seguridad Incorrecta:

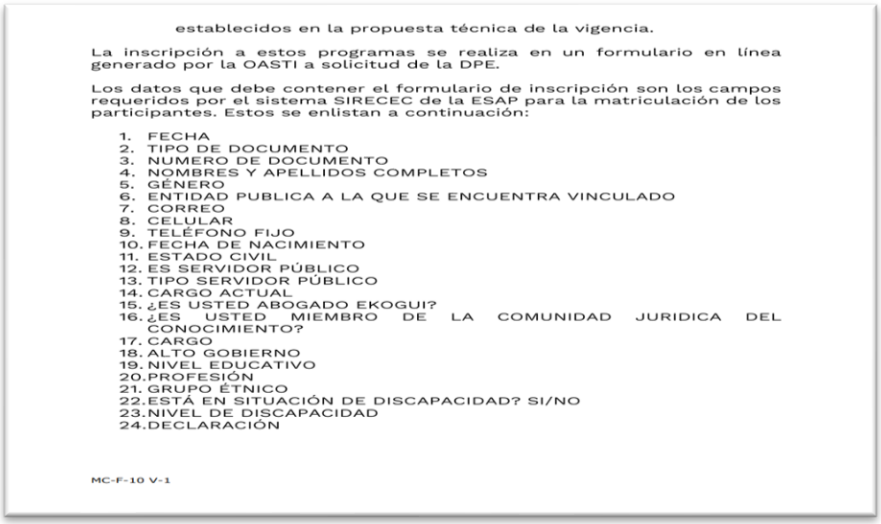
Exposición de Datos Sensibles.
Ausencia de Control de Acceso a las Funciones.
Falsificación de Peticiones en Sitios Cruzados (CSRF).
Uso de Componentes con Vulnerabilidades Conocidas.
A10–Redirecciones y reenvíos no validados.

No se evidencia la aplicación de las pruebas citadas en las fases previas a la publicación en el portal web de la Agencia. En los documentos enviados por TI se evidencia el análisis de los contenidos ya publicados, pero no lo establecido en la Guía.

- Como son gestionadas las solicitudes realizadas por los usuarios y se evidencia que ingresan por el web master y se gestionan por correo electrónico. Situación que no corresponde a lo establecido en el Procedimiento **Gestión de solicitudes Código: GTI-P-01** Procedimiento Para Solicitud de Servicios de TI el Numeral 3. *Asignar la Solicitud (Profesional de Infraestructura y Profesional de Soporte Técnico); El sistema de gestión de servicios de tecnología asignará automáticamente la solicitud al área encargada dependiendo la categoría de la solicitud.* Evidenciando que, para la atención de solicitudes de cliente externo, usuarios de los servicios de la Agencia, no se cuenta con un protocolo de atención de solicitudes en el cual se pueda centralizar, revisar cuantos casos radican, tiempo de solución y satisfacción de los usuarios.

- Que la interacción en relación con la gestión de los cursos publicados en la CJC, entre la OASTI y la DPE, está enmarcada en los lineamientos registrados en la Guía **GP-G-03 Guía de Gobierno de Información Para la CJC**, al validar el cumplimiento del Numeral 6.1 *Gestión de Datos;* encontramos que los datos recolectados son los siguientes:

Imagen N° 3 - Gestión de Datos



establecidos en la propuesta técnica de la vigencia.

La inscripción a estos programas se realiza en un formulario en línea generado por la OASTI a solicitud de la DPE.

Los datos que debe contener el formulario de inscripción son los campos requeridos por el sistema SIRECEC de la ESAP para la matriculación de los participantes. Estos se enlistan a continuación:

1. FECHA
2. TIPO DE DOCUMENTO
3. NUMERO DE DOCUMENTO
4. NOMBRES Y APELLIDOS COMPLETOS
5. GÉNERO
6. ENTIDAD PUBLICA A LA QUE SE ENCUENTRA VINCULADO
7. CORREO
8. CELULAR
9. TELÉFONO FIJO
10. FECHA DE NACIMIENTO
11. ESTADO CIVIL
12. ES SERVIDOR PÚBLICO
13. TIPO SERVIDOR PÚBLICO
14. CARGO ACTUAL
15. ¿ES USTED ABOGADO EKOGUI?
16. ¿ES USTED MIEMBRO DE LA COMUNIDAD JURIDICA DEL CONOCIMIENTO?
17. CARGO
18. ALTO GOBIERNO
19. NIVEL EDUCATIVO
20. PROFESIÓN
21. GRUPO ÉTNICO
22. ESTÁ EN SITUACIÓN DE DISCAPACIDAD? SI/NO
23. NIVEL DE DISCAPACIDAD
24. DECLARACIÓN

MC-F-10 V-1

Fuente: Guía GP-G-03 Guía De Gobierno De Información Para la CJC

Los datos recolectamos son datos personales de carácter privado, esto eleva la criticidad del activo el cual está catalogado con criticidad media. Evidenciando el incumplimiento de los lineamientos de la *Modelo de Seguridad y Privacidad de la Información 11.3.2 Clasificación de Activos de Información. La clasificación de activos de información tiene como objetivo asegurar que la información recibe los niveles de protección adecuados, de acuerdo con sus características particulares.*

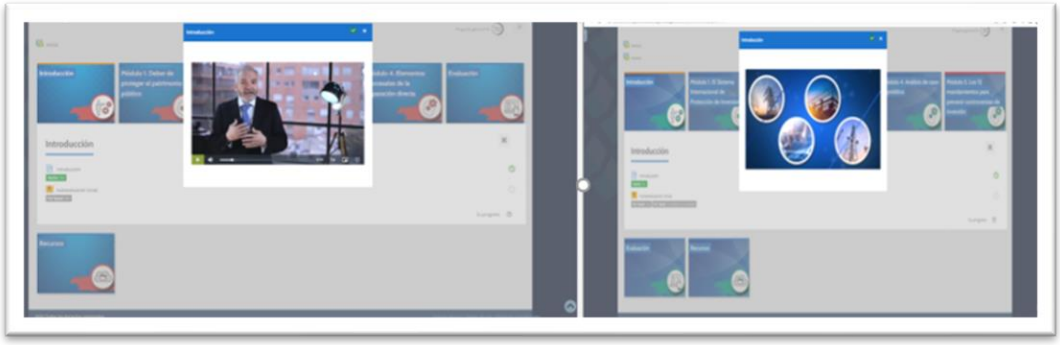
Imagen N° 4 - Activos de Información

Registro de Activos					Esquema de publicación			CALIFICACIÓN DE DATOS PERSONALES (Ley 1581 de 2012 y Ley 1266 de 2008)					Nivel de protección Seguridad				
ID	ESTADO	Fecha de Actualización (dd/mm/aaaa)	Título de la Categoría de información (Gestión Document	Nombre Activo de Información	Propietario	Responsable de la Producción de la Información	Responsable de la Información o custodio	Dato Público	Dato Privado	Dato Semiprivado	Dato Sensible	Dato personal de niños, niñas o adolescentes	Tipo de Activos de Información	Confidencialidad	Integridad	Disponibilidad	Nivel de Criticidad del Activo
AI01	ACTIVO	4/05/2022	GESTIÓN DE COMPETENCIAS INSTITUCIONALE	Portal Web de la Comunidad Jurídica del Conocimiento	CONTENEDORES C	Dirección de Políticas y Estrategias	CUST CDJC	PÚBLICO	PRIVADOS	No tiene datos Personales Semi-privados	No tiene datos Personales Sensibles	NIÑOS,NIÑAS Y ADOLECENTES	Servicios	Media	Media	Media	Media
AI02	ACTIVO	4/05/2022	GESTIÓN DE COMPETENCIAS INSTITUCIONALE	Modelo Óptimo de Gestión de la Defensa Jurídica	Gestión de Competencias Institucionales para la Defensa Jurídica	Dirección de Políticas y Estrategias	Gestión de Tecnologías de la Información	No tiene datos Personales Públicos	No tiene datos Personales Privados	No tiene datos Personales Semi-privados	No tiene datos Personales Sensibles	No tiene datos Personales Vulnerables	Información	Baja	Media	Media	Media
AI03	ACTIVO	4/05/2022	GESTIÓN DE COMPETENCIAS INSTITUCIONALE	Documentos de Resultados de Implementación MDG	Gestión de Competencias Institucionales para la Defensa Jurídica	Dirección de Políticas y Estrategias	Gestión de Tecnologías de la Información	No tiene datos Personales Públicos	No tiene datos Personales Privados	No tiene datos Personales Semi-privados	No tiene datos Personales Sensibles	No tiene datos Personales Vulnerables	Información	Baja	Media	Media	Media
AI04	ACTIVO	4/05/2022	GESTIÓN DE COMPETENCIAS INSTITUCIONALE	Comunidad Jurídica del Conocimiento	Gestión de Competencias Institucionales para la Defensa Jurídica	Subdirección de Acompañamiento a los Servicios	Gestión de Tecnologías de la Información.	- Datos generales (nombre, apellido, tipo de identificación,	No tiene datos Personales Privados	No tiene datos Personales Semi-privados	No tiene datos Personales Sensibles	No tiene datos Personales Vulnerables	Información	Media	Alta	Alta	Alta

Fuente: OASTI

- Se verifica el cumplimiento de la Resolución 1519 de 2021. Anexo *1 - 1.5 Criterios generales de accesibilidad web para contenidos audiovisuales web. Los sujetos obligados tendrán que adecuar los contenidos audiovisuales de sus sitios web bajo los siguientes requerimientos: ▪ Subtítulos o Closed Caption. A partir del 1 de enero del 2022, todos los sujetos obligados deberán incluir en el 100% de los contenidos audiovisuales (vídeos) nuevos la opción de subtítulos incorporados o texto escondido (closed caption) auto activable por los usuarios. Esta disposición no aplica para transmisiones en vivo y en directo*

Imagen N° 5 - Cursos publicados en la CJC



Fuente: Pagina Web ANDJ

Se evidenció el incumplimiento de lo establecido en el Anexo Técnico 1. Accesibilidad web: 1.1. Directrices de Accesibilidad Web, Se recomienda atender los lineamientos del anexo 2 de la resolución 1519 de 2021.

1.2 Comprueba – Innovación

En la revisión realizada, se encuentra que para la vigencia 2022 mediante contratos con el Proveedor QÜID LAB SAS se suscribieron consultorías así: **029-2020,** Objeto, estructurar el modelo de innovación de la ANDJE que responda a los objetivos estratégicos de la entidad, definiendo los pilares, la estructura interna, procesos internos, objetivos y proyectos que permitan a la entidad innovar de manera sistemática y Contrato de Consultoría. **033-2021,** Objeto, implementar el modelo de producción de la innovación de la ANDJE a través del desarrollo de dos ejercicios de innovación para optimizar el portafolio de productos y servicios de la agencia. Dentro de los cuales un entregable es la Herramienta COMPRUEBA.

Imagen N° 6 - Aplicativo publicado en Web- Comprueba

Fuente: Pagina Web Agencia

Se realiza la verificación de:

- El cumplimiento del Procedimiento GTI-P-03 Solicitud Y Aprobación de Nuevos Desarrollos o Mejoras de Software, evidenciando que no se sigue el lineamiento dado en los numerales del 6 al 18.

- El cumplimiento de la Guía para Desarrollo de Software Seguro numeral 4. Desarrollo Técnico. A continuación, se describen los lineamientos a tener presente para el desarrollo, mantenimiento o adquisición de software para la Agencia Nacional de Defensa Jurídica del Estado - ANDJE, para establecer requisitos de seguridad. *Pruebas de Seguridad y Aceptación: Cuando se realizan cambios al sistema hacer pruebas.* No se evidencia la aplicación de las pruebas citadas en las fases previas a la publicación en el portal web de la Agencia. En los documentos enviados por TI se evidencia el análisis de los contenidos ya publicados, no de los análisis en etapas previas.

- Como son gestionadas las solicitudes realizadas por los usuarios y se evidencia que ingresan por el web master y se gestionan por correo electrónico. Situación que no corresponde a lo establecido en el Procedimiento **Gestión de solicitudes Código: GTI-P-01** Procedimiento Para Solicitud de Servicios de TI el Numeral 3. "*Asignar la Solicitud (Profesional de Infraestructura y Profesional de Soporte Técnico); El sistema de gestión de servicios de tecnología asignará automáticamente la solicitud al área encargada dependiendo la categoría de la solicitud".* Evidenciando que, para la atención de solicitudes de cliente externo, usuarios de los servicios de la Agencia, no se cuenta con un protocolo de atención de solicitudes en el cual se pueda centralizar, revisar cuantos casos radican, tiempo de solución y satisfacción de usuarios

- El cumplimiento de la Resolución 1519 de 2021. Anexo 1 - 1.5 Criterios generales de accesibilidad web para contenidos audiovisuales web.

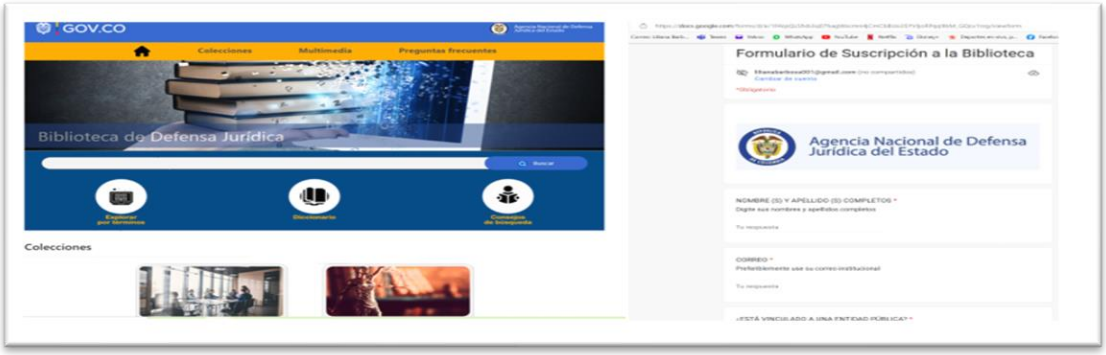
Imagen N° 7 - Comprueba ¿Cómo funciona?

Fuente: Pagina Web Agencia

1.3 Biblioteca Jurídica – Comunicaciones

En la revisión realizada se encuentra que mediante contrato con el proveedor Sociedad Para la Gestión del Conocimiento el Acceso a la Información y la Lectura Lectio SAS, se suscribió el contrato 057-2021, "*Desarrollo, Puesta En Producción y Posicionamiento De La Biblioteca Digital De la Agencia Como Herramienta de Conocimiento Abierto en Defensa Jurídica del Estado.*" Dentro de la descripción del producto está: "*El sitio responde al lenguaje de programación .Net que utiliza esquemas para el desarrollo de la página maestra asociando estilos de cascada utilizados conforme al manual de imagen corporativa de la Agencia. Por otra parte, para los resultados de búsqueda y la visualización de los contenidos se empleó el código en Javascript para hacer más liviano y fácil de usar el sitio*".

Imagen N° 8 -Biblioteca de Defensa Jurídica



Fuente: Pagina Web Agencia

Se realiza la verificación de:

- El cumplimiento del Procedimiento GTI-P-03 Solicitud Y Aprobación de Nuevos Desarrollos o Mejoras de Software, evidenciando que no se sigue el lineamiento dado en los numerales del 6 al 18.

- El cumplimiento de la Guía para Desarrollo de Software Seguro Numeral 4. Desarrollo Técnico. A continuación, se describen los lineamientos a tener presente para el desarrollo, mantenimiento o adquisición de software para la Agencia Nacional de Defensa Jurídica del Estado - ANDJE, para establecer requisitos de seguridad. *Pruebas de Seguridad y Aceptación. Cuando se realizan cambios al sistema hacer pruebas*: No se evidencia la aplicación de las pruebas citadas en las fases previas a la publicación en el portal web de la Agencia. web. En los documentos enviados por TI se evidencia el análisis de los contenidos ya publicados, no de los análisis en etapas previas.

- Como son gestionadas las solicitudes realizadas por los usuarios y se evidencia que ingresan por el web master y se gestionan por correo electrónico. Situación que no corresponde a lo establecido en el Procedimiento **Gestión de solicitudes Código: GTI-P-01** Procedimiento Para Solicitud de Servicios de TI el Numeral 3. "*Asignar la Solicitud (Profesional de Infraestructura y Profesional de Soporte Técnico); El sistema de gestión de servicios de tecnología asignará automáticamente la solicitud al área encargada dependiendo la categoría de la solicitud."* Evidenciando que, para la atención de solicitudes de cliente externo, usuarios de los servicios de la Agencia, no se cuenta con un protocolo de atención de solicitudes en el cual se pueda centralizar, revisar cuantos casos radican, tiempo de solución y satisfacción de usuarios.

- El cumplimiento de la Resolución 1519 de 2021. Anexo 1-1.5 Criterios generales de accesibilidad web para contenidos audiovisuales web.

Imagen N° 9 - Multimedia

Fuente: Biblioteca de Defensa Jurídica

De la revisión realizada se evidencia que existen por parte de la OASTI los lineamientos, sin embargo, no se evidencia la aplicación de estos en el hacer de las áreas que tienen a cargo los sistemas de información, razón por la cual se recomienda definir controles que permitan ampliar el alcance de los lineamientos emitidos.

2. Proceso Gestión De Incidentes De Seguridad De La Información

Se encontró en la revisión efectuada que se tiene contratado el análisis y tratamiento de las vulnerabilidades a través del contrato BID 067 de 2021 cuyo objeto es *"Prestar 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)"*; sin embargo, se observa debilidad en la realización de las pruebas en las etapas previas a la entrega desde las diferentes áreas que gestionan desarrollos para este caso particular La Dirección de Políticas e Innovación. Por lo anterior, se recomienda atender lo establecido Gestión De Incidentes De Seguridad de la Información GTI-P-05, para dar cumplimiento a la implementación de las Políticas e Gobierno Digital y de Seguridad Digital, y su habilitador transversal - Seguridad de la información: "*que busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad y disponibilidad y privacidad de los datos; Habilitador soportado en el Modelo de Seguridad y Privacidad de la Información –MSPI*".

3. Riesgos asociados al Proceso, Corrupción y de Seguridad de la Información

Se realiza la verificación de los riesgos establecidos por el Proceso 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

Tipo	Riesgo	Controles	
Corrupción	Fuga de información pública-reservada y publica clasificada a nivel digital por el servidor público	Política de seguridad y privacidad de la información contenidas en el Manual de políticas de gestión y desempeño institucional de la agencia DEM02	

	responsable de su administración para favorecer a un tercero	GTII01 Instructivo de control de accesos a centro de datos Sistema de SOC Centro de Monitoreo de Eventos de Seguridad (SIEM, Gestor de eventos e información de Seguridad, Sistema monitoreo a la infraestructura.) Sistema de control de acceso de directorio activo para usuarios de la red. Separación de ambientes informáticos para los sistemas misionales ekogui y Orfeo. Herramientas de cifrado de información.	
		Herramientas de prevención de pérdida de datos.	
Gestión	Posibilidad de pérdida económica y reputacional por Adquisición, arrendamiento y/o construcción de soluciones informáticas que no se encuentran alineadas con los objetivos estratégicos de la Entidad debido a No involucrar al área de tecnología en todos los requerimientos de las áreas con temas de tecnologías y/o no se emiten lineamientos desde TI para estructuración de proyectos de TI	CONTROL 1: Descripción 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 Cada vez que se requiera	
		CONTROL 2: Descripción Actividad 5 y 6 Aprobación PAI, PETI a través del Comité Gestión y Desempeño institucional. Cada vez que se requiera [DE-P-09] FORMULACIÓN Y SEGUIMIENTO DE LOS PLANES Y PROGRAMAS @ V5 2020-09-23	
		CONTROL 3: Descripción Actividad 9. Seguimiento a los proyectos incorporados en el PETI	
	Posibilidad de pérdida reputacional por quejas de los usuarios y/o sanciones de entes de control debido a pérdida de disponibilidad de los servicios y sistemas de información, causados por incidentes de seguridad	CONTROL 1 Descripción Sistema de SOC Centro de Monitoreo de Eventos de Seguridad (SIEM, Gestor de eventos e información de Seguridad, Sistema monitoreo a la infraestructura.) Cada vez que se requiera	
	Posibilidad de pérdida reputacional por requerimientos de usuarios internos de la Agencia debido a Errores de concepto al analizar las especificaciones en la fase inicial del proyecto para el desarrollo o mejoras de los sistemas de información	CONTROL 1 Descripción Actividad 2 [GTI-P-03] SOLICITUD Y APROBACIÓN DE NUEVOS DESARROLLOS O MEJORAS DE SOFTWARE @ V2 2021-11-05	
		CONTROL 2 Descripción Actividad 6, 12, 14 y 15 [GTI-P-03] SOLICITUD Y APROBACIÓN DE NUEVOS DESARROLLOS O MEJORAS DE SOFTWARE @ V2 2021-11-05	

		CONTROL 3 Descripción Actividad 18 [GTI-P-03] SOLICITUD Y APROBACIÓN DE NUEVOS DESARROLLOS O MEJORAS DE SOFTWARE @ V2 2021-11-05	
Seguridad	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.	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	
	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.	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	
	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.	CONTROL: Política General de Control de Acceso RESPONSABLE: Asesor(a) de TI FRECUENCIA: No establecida TIPO DE CONTROL: Preventivo NATURALEZA DEL CONTROL: No hay CONTROL DOCUMENTADO: SÍ	
	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.	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.	
	Posible pérdida de la disponibilidad de los sistemas misionales Ekogui y ORFEO por no contar con un plan de continuidad del negocio	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	

	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.	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

Fuente: Elaboración propia

3.1 Riesgos de Gestión y de Corrupción

- Se verifican los controles y se identifica que, si bien están definidos, no se describe el entregable y la periodicidad de implementación por lo cual se recomienda complementar la Matriz de riesgos de seguridad de la Información con información faltante, para cumplir con el diseño de controles establecido en la Guía de diseño de controles del DAFP.

3.2 Riesgos de seguridad

Se evidencian las siguientes situaciones en los controles establecidos:

- Procedimiento GTI-P-03 actividad 2, como control, las actividades citadas no tienen el alcance, esa actividad está solamente para ORFEO se recomienda actualizar el Procedimiento ampliando el alcance.

- Backup en cinta - 3.4.12 Política de copias de respaldo. • Deberá existir una bitácora de administración y control de copias de respaldos que permita conocer qué información está respaldada y almacenada en las bóvedas de seguridad del sitio externo. Se evidencia la ausencia de un plan o protocolo definido.

Imagen N° 10 - Micrositio MSPI

Fuente: Intranet institucional.

- La Matriz de riesgos de seguridad de información publicada es de 2020, se recomienda la actualización correspondiente:

Imagen N° 11 - Cursos publicados en la CJC

Fuente: Daruma

- La guía relacionada en el sitio corresponde a 2018, la Guía vigente corresponde a 2021 se recomienda la actualización correspondiente.

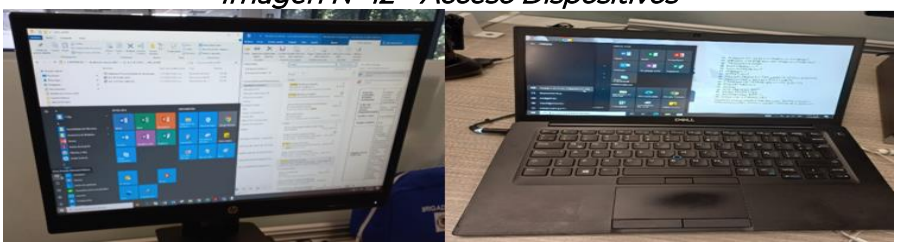
- Se verifican los controles establecidos por el proceso y en relación con los riesgos de seguridad y privacidad de la información, se observó que, aunque fueron identificados y se tienen consolidados, no se encuentran publicados en la herramienta para gestión de riesgos de la Agencia DARUMA, situación que no facilita a los responsables de los seguimientos realizar los reportes correspondientes. Así mismo se recomienda actualizar la matriz de riesgos en el sentido de describir los controles de acuerdo a lo establecido en la Guía Administración De Riesgos MC-G-02.

4. Declaración de aplicabilidad - Riesgos de seguridad

4.1 Simultaneo de logueo mismo usuario en dos dispositivos

Se evidencia la posibilidad de acceso a dos dispositivos con el mismo usuario, incumpliendo lo establecido en el Control 9.4.2 Procedimientos seguros de inicio de sesión: Cuando sea requerido por la política de control de accesos se debería controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de log-on.

Imagen N° 12 – Acceso Dispositivos



Fuente: Elaboración propia.

4.2 Dispositivos externos, política, restricción

Se evidencia la posibilidad de conexión a los equipos de dispositivos de almacenamiento externo (USB, discos duros) situación que no corresponde con lo establecido en el numeral *8.3 Manejo de los soportes de almacenamiento.* El objetivo es evitar la divulgación, modificación, retirada o destrucción de activos no autorizada almacenada en soportes de almacenamiento. La falta de control en los soportes de almacenamiento externo permite la materialización de potenciales amenazas, entre otras posibles, como:

- *Daños físicos (agua, fuego, polución, accidentes, destrucción de equipos, polvo, corrosión, congelación).*
- *Afectaciones por radiación (electromagnéticas, térmicas,).*
- *Compromiso de información (intercepción, espionaje en proximidad, robo de equipos o documentos, recuperación desde medios reciclados o desechados, manipulación de hardware, manipulación de software, detección de posición, …).*
- *Fallos técnicos (Falla o mal funcionamiento del equipo, saturación del sistema de información, mal funcionamiento del software, exposición de la mantenibilidad del sistema de información…).*
- *Acciones no autorizadas (Uso no autorizado de equipos, copia fraudulenta del software, uso de software falsificado o copiado, corrupción de datos, comportamientos no autorizados, procesamiento ilegal de datos, …).*

Controles:

- ***8.3.1 Gestión de soportes extraíbles:*** Se deberían establecer procedimientos para la gestión de los medios informáticos removibles acordes con el esquema de clasificación adoptado por la organización.
- ***8.3.2 Eliminación de soportes:*** Se deberían eliminar los medios de forma segura y sin riesgo cuando ya no sean requeridos, utilizando procedimientos formales.
- ***8.3.3 Soportes físicos en tránsito:*** Se deberían proteger los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización.

4.3 Exposición de claves

Se evidenció la vulnerabilidad de clave inicial asignada, situación que no corresponde a lo establecido en el control 9*.2.4 Gestión de La Información de Autenticación Secreta de los Usuarios,* control definido para garantizar que se mantiene la confidencialidad de la información secreta de acceso (p. ejemplo contraseñas). Gestionar la información de autenticación supone controlar: Incluir cláusulas en contratos y condiciones de puesto de trabajo sobre el mantenimiento del secreto de las contraseñas o información de autenticación; Obligación de cambiar contraseñas iniciales después de su primer uso; Identificar al usuario antes de entregar las contraseñas y obtener acuse de recibo; Uso de contraseñas seguras, no compartidas; Uso de medios seguros de comunicación (Correos cifrados etc.); Cambiar contraseñas a personal externo después de que han realizado sus trabajos (instalaciones de software etc.)

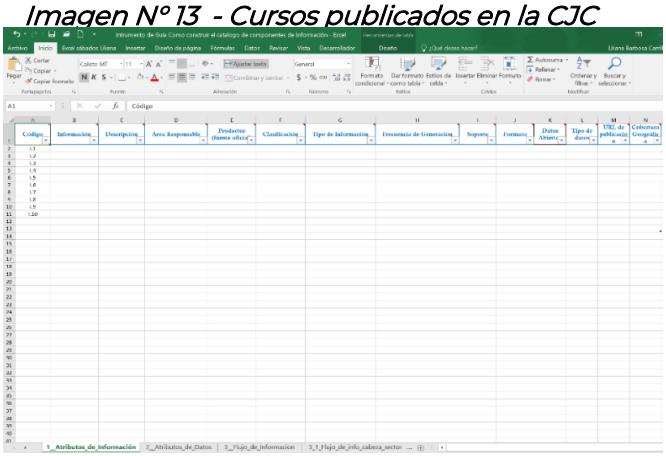
5. Catálogo de Componentes de Información:

Guía G.INF.07- cómo construir el Catálogo de Componentes de Información, teniendo en cuenta que Mediante Decreto 1008 de 2018 "*Por el cual se establecen los lineamientos generales de la política de Gobierno Digital*" en su Artículo 2.2.9.1.2.2. Manual de Gobierno Digital. Establece que, "*Para la implementación de la Política de Gobierno Digital, las entidades públicas deberán aplicar el Manual de Gobierno Digital que define los lineamientos, estándares y acciones a ejecutar por parte de los*

sujetos obligados de esta Política de Gobierno Digital", de la cual hace parte integral la Guía Inf.07.

El catálogo de componentes de información representa el punto de partida para la construcción de la arquitectura de información y la base para iniciar procesos de calidad de información de la entidad e interoperabilidad entre entidades.

Imagen N° 13 - Cursos publicados en la CJC



Fuente: Elaboración propia

En la validación realizada no se evidencia el diligenciamiento del catálogo de componentes de información

6. Planes de Mejoramiento

Tabla N° 2 Planes de mejoramiento asociados al proceso Gestión de Tecnologías de la Información

No	Descripción	Tipo
2022	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.	Observaciones
	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.	No Conformidad
	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.	No Conformidad
	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 último Informe de la auditoria.	Observaciones
	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)	No Conformidad
	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-	No Conformidad

	%20%20MANUAL%20DE%20POLITICAS%20DE%20 GESTION%20Y%20DESEMPENO%20INSTITUCIONAL_publicar_23_11_2020.pdf	
	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.	No Conformidad
	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).	No Conformidad

Fuente: Elaboración propia

En la revisión realizada se observó la suscripción del plan y el desarrollo de las actividades. Así mismo, en relación con el DRP y el BCP se observa que aún no se encuentra implementado y es una situación que vienen desde el año 2020; frente a las acciones propuestas se han presentado reprogramaciones y no es posible validar los productos dado que a la fecha no se encuentran oficializados, estos documentos deben ser aprobados por la alta dirección, socializados e implementados.

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

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

PLAN ACC: NOMBRE	MACRO-ACTIVIDAD: NOMBRE
PA220-008	123-PAI Herramienta de gestor de clientes implementado
PA220-008	124-PAI Modelo de Gobierno de Datos, Gestión TI, Arquitectura de Referencia y Fortalecimiento de las capacidades TI realizado
PA220-008	125-PAI 100% Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información implementado
PA220-008	126-PAI Incrementar en 2 pp la calificación del Modelo de Seguridad y Privacidad de la Información
PA220-008	127-PAI 100% del PETI 2022 implementado
PA220-008	128-PAI 96% de las vulnerabilidades identificadas en 2021, subsanadas
PA220-008	130-PAI Modelo de Arquitectura Empresarial implementado
PA220-008	129-PAI Arquitectura de interoperabilidad diseñada e implementada
01-GTI-22	Atención de solicitudes de servicios tic
02-GTI-22	Nivel de disponibilidad de los servicios tecnológicos por tipo
03-GTI-22	Incidentes de seguridad de la información atendidos oportunamente
04-GTI-22	Activos de Información Identificados
05-GTI-22	Controles de Riesgo
06-GTI-22	Nivel de apropiación del SGSI
07-GTI-22	Brechas del SGSI

Fuente: Elaboración propia

Se hace seguimiento y se evidencia que los indicadores están en los tiempos de ejecución.

8. Protección de datos personales

Se verifica que, si bien a través de la Resolución 430 de 10 de octubre de 2017 en la cual se adopta la Política de Protección de datos personales se establece que "*la Oficina Asesora Jurídica será el área responsable de atender las peticiones, consultas y reclamos que presenten los titulares de los datos y en consecuencia a es el área de la ANDJE ante la cual estos podrán ejercer sus derechos de conformidad a lo establecido por la normatividad legal vigente*". Se evidencia que en la Política de Protección de datos Personales, no se encuentran la designación y la asignación de tareas del rol de Oficial de Protección de Datos Personales.

Responsabilidades establecidas en el Decreto 1377 de 2013 (junio 27) *"por el cual se reglamenta parcialmente la Ley 1581 de 2012. Artículo 23. Medios para el ejercicio de los derechos. Todo responsable y Encargado deberá designar a una persona o área que asuma la función de protección de datos personales, que dará trámite a las solicitudes de los Titulares"*, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012 y el presente decreto y así mismo el Anexo A controles de seguridad en su numeral A.18.1.4, el cual cita:

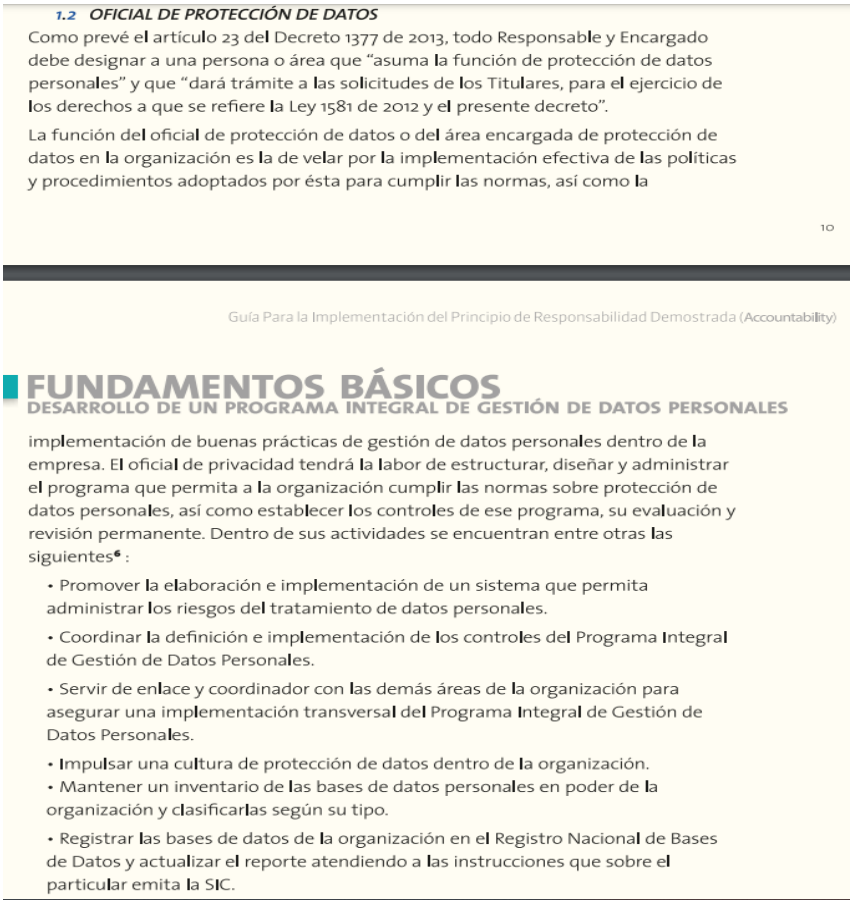
Imagen N° 14 - Anexo A

A.18.1.4	Privacidad y protección de datos personales		Control: Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.

Fuente: ISO 27001

Las tareas designadas al rol de Oficial de Protección de Datos Personales, las enmarca la Super Intendencia de Industria y Comercio SIC en la Guía para la implementación del principio de responsabilidad demostrada (Accountability) y son las siguientes:

Imagen N° 15 - Funciones Oficial de Protección de Datos Personales



1.2 *OFICIAL DE PROTECCIÓN DE DATOS*

Como prevé el artículo 23 del Decreto 1377 de 2013, todo Responsable y Encargado debe designar a una persona o área que "asuma la función de protección de datos personales" y que "dará trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012 y el presente decreto".

La función del oficial de protección de datos o del área encargada de protección de datos en la organización es la de velar por la implementación efectiva de las políticas y procedimientos adoptados por ésta para cumplir las normas, así como la

10

Guía Para la Implementación del Principio de Responsabilidad Demostrada (Accountability)

FUNDAMENTOS BÁSICOS

DESARROLLO DE UN PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES

implementación de buenas prácticas de gestión de datos personales dentro de la empresa. El oficial de privacidad tendrá la labor de estructurar, diseñar y administrar el programa que permita a la organización cumplir las normas sobre protección de datos personales, así como establecer los controles de ese programa, su evaluación y revisión permanente. Dentro de sus actividades se encuentran entre otras las siguientes[6]:

- Promover la elaboración e implementación de un sistema que permita administrar los riesgos del tratamiento de datos personales.
- Coordinar la definición e implementación de los controles del Programa Integral de Gestión de Datos Personales.
- Servir de enlace y coordinador con las demás áreas de la organización para asegurar una implementación transversal del Programa Integral de Gestión de Datos Personales.
- Impulsar una cultura de protección de datos dentro de la organización.
- Mantener un inventario de las bases de datos personales en poder de la organización y clasificarlas según su tipo.
- Registrar las bases de datos de la organización en el Registro Nacional de Bases de Datos y actualizar el reporte atendiendo a las instrucciones que sobre el particular emita la SIC.

Fuente: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

9. Cumplimiento recomendaciones FURAG

Tabla N° 4 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	Documentar e implementar un plan de continuidad de los servicios tecnológicos mediante pruebas y verificaciones acordes a las necesidades de la entidad.
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 un documento de pruebas de funcionalidad para la implementación del Protocolo de Internet versión 6 (IPV6) en la entidad.
8	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).
9	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.
10	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.
11	Gobierno Digital	Utilizar tecnologías emergentes de cuarta revolución industrial como la robótica para mejorar la prestación de los servicios de la entidad.
12	Gobierno Digital	Ejecutar al 100% los proyectos de TI que se definen en cada vigencia.
13	Gobierno Digital	Publicar todos los conjuntos de datos abiertos estratégicos de la entidad en el catálogo de datos del Estado Colombiano www.datos.gov.co.
14	Gobierno Digital	Utilizar medios digitales en los ejercicios de rendición de cuentas realizados por la entidad.
15	Gobierno Digital	Publicar, en la sección "transparencia y acceso a la información pública" de su sitio web o sede electrónica información actualizada sobre la información sobre los grupos étnicos en el territorio.
16	Seguridad Digital	Fortalecer las capacidades en seguridad digital de la entidad a través de ejercicios de simulación de incidentes de seguridad digital al interior de la entidad.
17	Seguridad Digital	Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como participar en la construcción de los planes sectoriales de protección de la infraestructura crítica cibernética.
18	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.

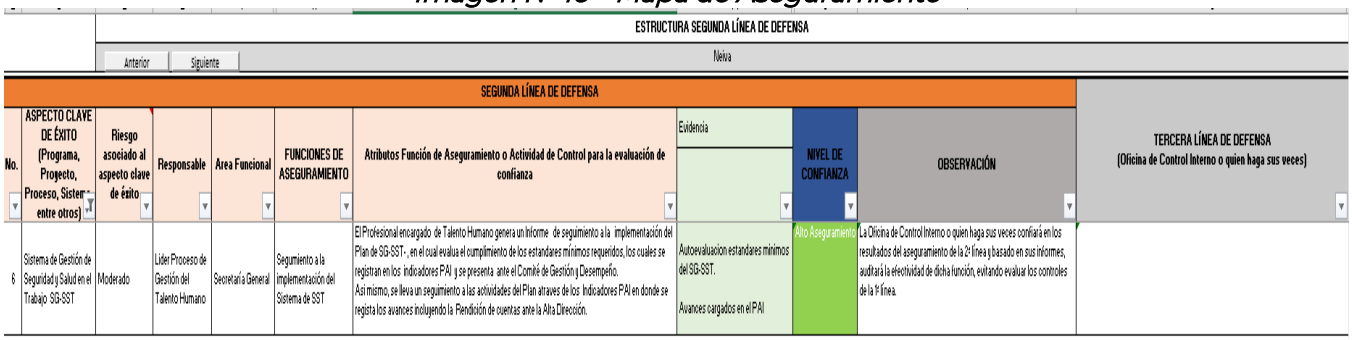
Fuente: Elaboración Propia

Dado 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, se recomienda atender las observaciones hechas en relación con Datos abiertos, uso de tecnologías emergentes y la información sobre grupos étnicos en territorio.

10. Mapa de Aseguramiento tareas como segunda línea de defensa

Validación cumplimiento de actividades:

Imagen N° 16 – Mapa de Aseguramiento



ESTRUCTURA SEGUNDA LÍNEA DE DEFENSA

Anterior | Siguiente | Nelva

SEGUNDA LÍNEA DE DEFENSA											TERCERA LÍNEA DE DEFENSA (Oficina de Control Interno o quien haga sus veces)
No.	ASPECTO CLAVE DE ÉXITO (Programa, Proyecto, Proceso, Sister... entre otros)	Riesgo asociado al aspecto clave de éxito	Responsable	Area Funcional	FUNCIONES DE ASEGURAMIENTO	Atributos Función de Aseguramiento o Actividad de Control para la evaluación de confianza	Evidencia	NIVEL DE CONFIANZA	OBSERVACIÓN	
6	Sistema de Gestión de Seguridad y Salud en el Trabajo SG-SST	Moderado	Líder Proceso de Gestión del Talento Humano	Secretaría General	Seguimiento a la implementación del Sistema de SST	El Profesional encargado de Talento Humano genera un Informe de seguimiento a la implementación del Plan de SG-SST-, en el cual evalúa el cumplimiento de los estandares mínimos requeridos, los cuales se registran en los Indicadores PAI y se presenta ante el Comité de Gestión y Desempeño. Así mismo, se lleva un seguimiento a las actividades del Plan atraves de los Indicadores PAI en donde se registra los avances incluyendo la Rendición de cuentas ante la Alta Dirección.	Autoevaluacion estandares minimos del SG-SST. Avances cargados en el PAI	Alto Aseguramiento	La Oficina de Control Interno o quien haga sus veces confiará en los resultados del aseguramiento de la 2ª línea y basado en sus informes, auditará la efectividad de dicha función, evitando evaluar los controles de la 1ª línea.	

Fuente: Elaboración Propia

Se verifico el diligenciamiento del Formato DE-F-26 Formato para el registro de la información para la revisión por la dirección a través de correo enviado al a Oficina Asesora de Planeación.

PRINCIPALES SITUACIONES DETECTADAS/ RESULTADOS DE LA AUDITORÍA / RECOMENDACIONES:

N°	REQUISITO	NO CONFORMIDAD	OBSERVACIONES
1	Procedimiento GTI-P-03 Solicitud y Aprobación De Nuevos Desarrollos o Mejoras De Software.	Se evidencia que no se sigue el lineamiento dado en los numerales del 6 al 18 del procedimiento, en la fase de planeación y desarrollo de los aplicativos revisados TI.	
2	Guía Para Desarrollo De Software Seguro Numeral 4. Desarrollo Técnico. A continuación, se describen los lineamientos a tener presente para el desarrollo, mantenimiento o adquisición de software para la Agencia Nacional de Defensa Jurídica del Estado - ANDJE, para establecer requisitos de seguridad. Pruebas de Seguridad y Aceptación. Cuando se realizan cambios al sistema hacer pruebas.	No se evidencia la aplicación de las pruebas citadas en las fases previas a la publicación en el portal web de la Agencia.	
3	GTI-P-01 Procedimiento Para Solicitud de Servicios de TI el Numeral 3. Asignar la Solicitud (Profesional de Infraestructura y Profesional de Soporte Técnico); El sistema de gestión de servicios de tecnología asignará automáticamente la solicitud al área encargada dependiendo la categoría de la solicitud.	Se evidencia que, para la atención de solicitudes de cliente externo, usuarios de los servicios de la Agencia evaluados, no se cuenta con un protocolo de atención de solicitudes en el cual se pueda centralizar, revisar cuantos casos radican, tiempo de solución y satisfacción de usuarios. Respuesta de TI	

		Aunque entendemos la necesidad, desde T.I apoyaremos la necesidad técnica que se requiera y que surja del protocolo que establezca el proceso responsable de realizar dicho documento. Por lo anterior solicitamos que se eleve el hallazgo al proceso responsable y que ellos nos involucren cuando así lo requieran. **Respuesta OCI** La herramienta de gestión de solicitudes es un componente de TI, por lo cual la solución debe ser trabajada, desde su Planeación en conjunto con el Proceso que la requieran. **Respuesta Proceso Comunicaciones** La Agencia cuenta con una sección llamada Buzones Electrónicos que está ubicada en la página principal en la sección de Destacados y también se encuentra en la sección de atención y servicios a la ciudadanía, estos buzones reciben gran parte de las peticiones realizadas a través de la Wb por usuarios externos, desconocemos hasta donde es posible hacer el seguimiento pertinente a la información recibida y contenida en las bases de datos de estos formularios. **Respuesta OCI** Dado que las herramientas de gestión de solicitudes tienen componente de TI, la solución debe ser trabajada, desde su Planeación en conjunto con el Proceso de TI. ***Esta No conformidad es de responsabilidad compartida entre: El Proceso Gestión de TI, Gestión de grupos de interés y Comunicaciones y la Dirección de Políticas y Estrategias***	
4	Decreto 1008 de 2018 Modelo de Seguridad y Privacidad de la Información 11.3.2 Clasificación de Activos de Información La clasificación de activos de información tiene como objetivo asegurar que la información recibe los niveles de protección adecuados, de acuerdo con sus características particulares.	Se evidencia vulnerabilidad frente al manejo de los datos personales recolectados al momento del registro. ***Esta No conformidad es de responsabilidad compartida entre: El Proceso Gestión de TI y la Dirección de Políticas y Estrategias***	
5	Resolución 1519 de 2021. Anexo 1 1.5 Criterios generales de accesibilidad web para contenidos audiovisuales web. Los sujetos obligados tendrán que adecuar los contenidos audiovisuales de sus sitios web bajo los siguientes requerimientos: ▪ Subtítulos o Closed Caption. A partir del 1 de enero del 2022, todos los sujetos obligados deberán incluir en el 100% de los contenidos audiovisuales (vídeos) nuevos la opción de subtítulos incorporados o texto escondido (closed caption) auto activable por los	Se evidenció que la publicación de los contenidos no atiende lo establecido en el Anexo Técnico 1. Accesibilidad web: 1.1. Directrices de Accesibilidad Web **Respuesta Proceso Comunicaciones** De acuerdo a esta evidencia creemos que se pueden revisar los videos para ver la posibilidad de activar el Closed Caption,	

	usuarios. Esta disposición no aplica para transmisiones en vivo y en directo.	generalmente se puede hacer dependiendo de la aplicación utilizada para hacer el Streamig, de no ser posible la recomendación es hacer que el proveedor de dichos videos deje activada dicha propiedad para cumplir con la directiva **Respuesta OCI** Dado que el Anexo A tienen componente de TI, la solución debe ser trabajada, en conjunto con el Proceso de TI. ***Esta No conformidad es de responsabilidad compartida entre: El Proceso Gestión de TI, Gestión de grupos de interés y Comunicaciones y la Dirección de Políticas y Estrategias***	
6	Decreto 1008 de 2018 Modelo de Seguridad y Privacidad de la Información Anexo A 3.4.12 Política de copias de respaldo. · Deberá existir una bitácora de administración y control de copias de respaldos que permita conocer qué información está respaldada y almacenada en las bóvedas de seguridad del sitio externo	Se evidencia la ausencia de un plan o protocolo definido de traslado y restauración de back up en medio físico.	
7	Decreto 1008 de 2018 Modelo de Seguridad y Privacidad de la Información Decreto 767 del 16 de mayo de 2022 Política de Gobierno Digital Declaración de aplicabilidad	Se evidencia debilidad en la aplicación de los siguientes controles de seguridad: Control 9.4.2 Procedimientos seguros de inicio de sesión; 8.3 Manejo de los soportes de almacenamiento;9.2.4 Gestión De La Información De Autenticación Secreta De Los Usuarios. **Respuesta de TI** *Nos podrían indicar el nombre de la aplicación para revisar el hallazgo.* **Respuesta OCI** *No es una situación particular en el desarrollo de la Auditoria numeral 3.2 Riesgos de seguridad, se detallan*	
8	Ley 1581 de 2012 Decreto 767 del 16 de mayo de 2022 Política de Gobierno Digital Decreto 1377 de 2013 (junio 27) “por el cual se reglamenta parcialmente la Ley 1581 de 2012. Artículo 23.	Se evidencia que, en la Política de Protección de datos Personales, no se encuentran la designación del rol y la asignación de tareas del Oficial de Protección de Datos Personales. **Respuesta de TI** *Aunque se entiende la necesidad, consideramos que no debe tratar como una NO CONFORMIDAD y se debe tratar como una recomendación la cual debe ser elevada a la alta dirección para determinar la creación de este ROL y en apoyo con la OAJ.* **Respuesta OCI**	

		La situación genera un incumplimiento de Ley razón por la cual se debe tomar medida correctiva.	
9	Decreto 1008 de 2018 Política de Seguridad Digital Gestión de Incidentes de seguridad		Se reitera la recomendación dada frente a 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.

RECOMENDACIONES:

- Se recomienda definir controles que permitan ampliar el alcance de los lineamientos emitidos por la OASTI, involucrando las áreas que tienen a cargo la administración de los sistemas de información.
- Se recomienda complementar la Matriz de riesgos de seguridad de la Información con información faltante, para cumplir con el diseño de controles establecido en la Guía de diseño de controles del DAFP.
- Se recomienda la actualización del sitio del MSPI en relación con la Guía de riesgos publicada y la matriz de riesgos publicada.
- Se recomienda publicar la Matriz De Riesgos de Seguridad de la Información en la herramienta para gestión de riesgos de la Agencia DARUMA, situación que facilita realizar los seguimientos correspondientes.
- Se recomienda priorizar la formalización relación con el DRP y el BCP se observa que aún no se encuentra implementado y es una situación que vienen desde 2020, estos documentos deben ser aprobados por la alta dirección, socializados e implementados.
- Se recomienda Incluir en el listado de activos de información de la entidad los nuevos sistemas de información que se están implementando en la Agencia, Chat box, Gestor documental entre otros.
- Se recomienda actualizar el Procedimiento GTI-P-03 actividad 2, ampliando el alcance actualmente está solo para ORFEO.
- Se recomienda atender las recomendaciones realizadas en el Formulario Único Reporte de Avances de la Gestión (FURAG) en relación con Datos abiertos, uso de tecnologías emergentes y la información sobre grupos étnicos en territorio.
- Se recomienda identificar y registrar en algún lineamiento de la Agencia; los responsables directos de implementar los controles necesarios para el cumplimiento de la Resolución 1519 del 2020
- Se recomienda la implementación del catálogo de componentes de información siguiendo los lineamientos dados en la *Guía G.INF.07- Cómo construir el Catálogo de Componentes de Información MINTIC.*

Para constancia se firma en Bogotá D.C., a los 21 días del mes de diciembre de 2022.

_____

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