REFERENCIA	NOMBRE DE AUDITORIA	FECHA DE REALIZACIÓN		FECHA DEL INFORME
		INICIO	CIERRE	
A-P-GTI-01	Auditoria al Proceso de Gestión de Tecnologías de la Información	01/08/2018	31/08/2018	31/08/2018

PROCESO /ÁREA AUDITADA	AUDITOR LÍDER / AUDITOR
Gestión de Tecnologías de la Información	Manuel Humberto Sierra López
EQUIPO DE AUDITORES	**AUDITORES ACOMPAÑANTES**
No Aplica	No Aplica

1. OBJETIVOS:

- Evaluar la gestión del proceso de TI en la ANDJE.
- Verificar el cumplimiento de normas y políticas asociadas.
- Establecer los avances en la implementación del Sistema de Gestión de Seguridad de la Información – SGSI y lo relacionado con evaluaciones anteriores.

2. ALCANCE:

Para la Evaluación al Proceso de Gestión Tecnologías de la Información se tomó como base las acciones del proceso adelantadas durante el periodo 01 de julio de 2017 al 31 de julio de 2018.

3. CRITERIOS:

- Ley de Transparencia Ley 1712 de 2014.
- Decreto Ley 4085 de 2011. Por el cual se establecen los objetivos y la estructura de la Agencia Nacional de Defensa Jurídica del Estado.
- Decreto 1069 de 2015. Sistema de Información Litigiosa del Estado.
- Decreto 1008 de junio 14 de 2018 del Ministerio de Tecnologías de la Información y las Comunicaciones
- Ley 1341 de 2012. Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Telecomunicaciones TIC´S.
- Decreto 1078 de 2015. Sector de Tecnologías de la Información y las Comunicaciones.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Decreto Reglamentario 1377 de 2013
- Marco de mejores prácticas en Tecnología alineados con Cobit 4.1, Itil V3 E ISO 27000/x
- Guías de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones
- Resolución 095 de febrero de 2018, por el cual se adopta el Nuevo Sistema Integrado de Gestión Institucional – SIGI – en la Agencia Nacional de Defensa Jurídica del Estado. SGS – SGSPI.
- Decreto 1083 de 2015 (Función Pública) Artículo 2.2.21.5.2 (Libro 2, Parte 2, Titulo 21, Capítulo 5).
- Modelo Integrado de Planeación y Gestión – MIPG
- Proceso, Procedimientos, políticas, guías, informes de Auditorias anteriores, Planes de Mejoramiento, Plan de Acción Institucional (PAI), Plan Operativo Anual (POA), Mapas de Riesgos e Indicadores.

4. LIMITACIONES PARA EL DESARROLLO DE LA AUDITORIA:

No se presentaron.

5. DOCUMENTOS EXAMINADOS:

- Mapa de riesgos generales para proceso de Gestión de Tecnologías de Información.

- Mapa de riesgos de Corrupción
- Mapa de riesgos de Seguridad de la Información.
- Documento de caracterización GTI-C-01 V1 Gestión de Tecnologías de la Información.
- Procedimiento GTI-P-01 Procedimiento para solicitud de servicios de TI
- Procedimiento GTI-P-02 Gestión de Cambios de TI
- Procedimiento GTI-P-03 Solicitud y aprobación de nuevos desarrollos o mejoras de Software
- Procedimiento GTI-P-04 Aprovisionamiento de Servidores
- Procedimiento GTI-P-05 Gestión de Incidentes de Seguridad
- Modelo de Seguridad y Privacidad de la Información
- Modelo OSI
- Manual de Políticas de seguridad del Subsistema de Seguridad y privacidad de la información.
- Documentación generada por la mesa de ayuda del proceso de Gestión de tecnologías de información.
- Documentos carpeta auditoria 2018 Remitida por el líder del proceso de Gestión de Tecnologías de información.
- Listado de contratistas que desarrollan funciones de apoyo en la mesa de ayuda.
- Formato de solicitud de cambio para revisión, análisis y aceptación de la actualización del firmware para el servidor SRVANDJE05 y su respectiva acta de reunión
- Formato de solicitud de cambio para aprobación de cambio en red wifi y traslado de Acces Point y su respectiva acta de reunión.
- Documento de los Modelos de Contingencia de Tecnologías de información para la infraestructura misional de la ANDJE.
- Diagrama del esquema de arquitectura de alta disponibilidad para el Sistema único de información litigiosa del Estado. (eKOGUI)
- Presentación de charlas de información de Gestión de Tecnologías de la Información y el Sistema de Gestión de Seguridad de la Información para funcionarios y contratistas de la ANDJE.
- Documentación allegada por parte del proceso de Gestión de Tecnologías de Información referente a la solicitud de información hecha por la Oficina de Control Interno sobre uso de activos tecnológicos por parte de exfuncionarios de proceso de Gestión Financiera.
- Documentación de soporte de los incidentes de seguridad presentados en el primer semestre de 2018.

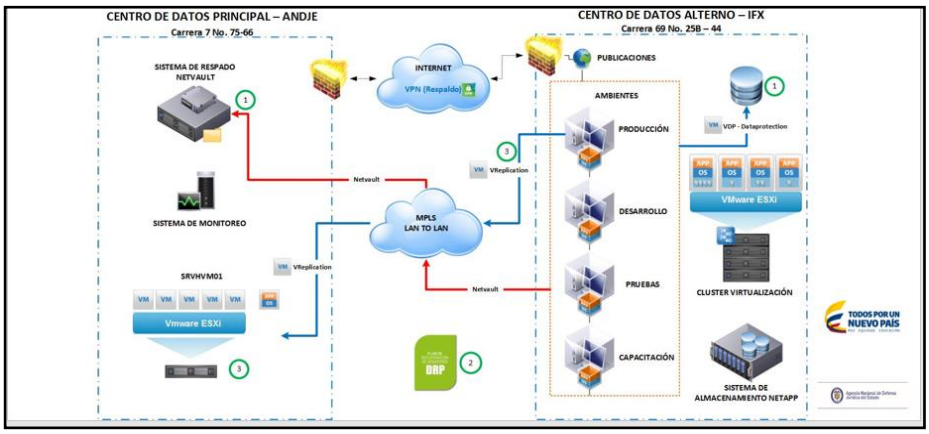
6. PLAN DE MUESTREO

Se verificó la información de los repositorios de la ANDJE como carpetas compartidas, pagina web, Sistema SIGI , Sistema ORFEO y la diferente información proporcionada por el líder del proceso a través de correo electrónico.

7. INFORME

7.1 FORTALEZAS

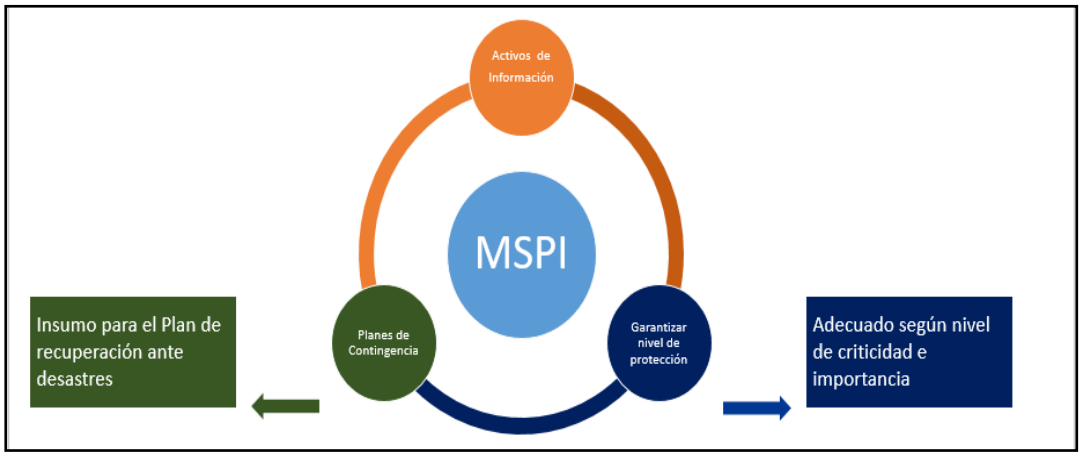
7.1.1. En la evaluación de la plataforma tecnológica que soporta toda la infraestructura de la Entidad y de acuerdo a la documentación allegada por el líder del proceso y la entrevista realizada en el marco de la auditoria al proceso de Gestión de Información Jurídica responsable del sistema EKOGUI, se evidencia la diligencia del proceso de Gestión de Tecnologías de Información para realizar tareas y actividades encaminadas a que la infraestructura tecnológica cuente con un esquema de alta disponibilidad de servicios misionales , adoptando arquitecturas redundantes en data center y políticas de copias de seguridad de la información sensible.



Fuente Proceso de Gestión de Tecnologías de Información

7.1.2. El proceso de Gestión de Tecnologías de Información durante el último año ha llevado a cabo importantes tareas en la mejora de temas sensibles como la Seguridad de la Información, en el caso específico y siguiendo buenas practicas dio cumplimiento a las directrices establecidas en la Norma Técnica Colombiana NTC ISO 27001:2013 numeral 5.2 en lo referente a la definición de una política del Sistema de Gestión de la Seguridad de la información.

De igual forma la inclusión del sistema como subsistema de Seguridad y privacidad de la información en la Resolución 095 del 26/02/2018 "Por el cual se adopta el Sistema Integrado de Gestión Institucional – SIGI" es un buen avance para alcanzar los objetivos de seguridad informática de la Entidad. Además, la implementación del Modelo de Seguridad y Privacidad de la información enmarcado en la política de Gobierno Digital liderada por el Ministerio de Tecnologías de la Información y las comunicaciones sirve para adelantar actividades en proyectos de Análisis de Impacto de Negocios (BIA su sigla en inglés), Plan de Continuidad de Negocio y Plan de Recuperación ante Desastres.



Fuente Proceso de Gestión de Tecnologías de Información

7.1.3. El Líder del Proceso de Gestión de Tecnología de la Información con el fin de prever el ataque o vulnerabilidad de los sistemas tecnológicos de la Agencia, se suscribió una consultoría de Ethical hacking por medio del Contrato No. 035- 2018 con la firma Alinatech cuyo objeto es contratar el servicio para realizar el diagnostico de vulnerabilidades y hacking ético de la infraestructura tecnológica y sistemas de información de la Agencia Nacional de Defensa Jurídica del Estado, y a su vez generar un plan de remediación como apoyo al cierre de vulnerabilidades encontradas.
Así mismo se evidenció acta de reunión de apertura del Proyecto hacking ético con fecha 23/08/2018.

7.2 CUMPLIMIENTO DE PRINCIPIOS

Se tomaron como referente los principios emitidos por el Ministerio de las tecnologías y Comunicaciones:

7.2.1 Excelencia del servicio al ciudadano

Se fortalece la relación con los ciudadanos a través de la mejora continua en la disponibilidad presentada en la plataforma tecnológica debido a que los usuarios tienen acceso de manera rápida y eficiente a toda la documentación presentada en el marco de la ley de transparencia y del derecho al acceso a la información pública.

7.2.2 Estandarización

A través de formatos, guías, políticas, evaluación de casos de uso, lineamientos, se permiten la estandarización de los procedimientos de atención al usuario, gestión de cambios, etc.

7.2.3 Seguridad de la Información

La adopción de las nuevas políticas de seguridad de la información, la evaluación de riesgos asociados a la seguridad, definición de políticas de seguridad y la atención a los incidentes de seguridad hacen que se cumpla con estándares y fortalezas que aseguran la disponibilidad, integridad y confidencialidad de la información litigiosa del Estado.

7.2.4 Socialización

El proceso de Gestión de Tecnologías de información ha realizado tareas muy importantes en términos de seguridad de la información y fortalecimiento de la plataforma tecnológica, a través de campañas de socialización sobre todo en el tema de políticas de seguridad de la información establecidas en el subsistema como se evidenció en los expedientes de Orfeo 20182007801000001E, 20182007802000001E y 20182007803000001E

7.3 CONTENIDO

7.3.1 Descripción de la Evaluación del Proceso

Para dar inicio a la auditoria interna se realizó un análisis de la información que se encuentra en el sistema SIGI y más específicamente en el Mapa de Procesos de la Entidad en Gestión de Tecnologías de la información:

- GTI-C-01 v.1 Caracterización Proceso de Gestión de Tecnologías de información.
- GTI-P-01 v1. Procedimiento de Solicitud de servicios de Tecnología
- GTI-P-02 Procedimiento de Gestión de Cambios de TI
- GTI-P-03 Procedimiento Solicitud y aprobación de nuevos desarrollos o mejoras de Software.
- GTI-P-04 Procedimiento para aprovisionamiento de servidores.
- GTI-P-05 Procedimiento de Gestión de Incidentes de Seguridad de la Información.

- De acuerdo a la información recolectada tanto en los diferentes repositorios, a los hechos ocurridos recientemente y a la información suministrada por el líder del proceso, se determinó verificar de manera detallada los procedimientos GTI-P-01 v1. Procedimiento de Solicitud de Servicios de Tecnología, GTI-P-02 Procedimiento de Gestión de Cambios de TI y GTI-P-05 Procedimiento de Gestión de Incidentes de Seguridad de la Información.

De otra parte, en el marco de la auditoria se evaluaron los siguientes temas:

- Esquema de alta disponibilidad de la infraestructura que tiene la Agencia Nacional de Defensa Jurídica del Estado y en general la arquitectura de la Entidad.

- Respecto a mesa de ayuda se solicitó información de los casos atendidos por la misma, además de información referente a los niveles de atención de los incidentes y los ingenieros encargados de esta tarea.
- Se revisaron actividades del procedimiento GTI-P-02 Procedimiento de Gestión de Cambios de TI específicamente en dos casos específicos realizados durante el periodo.
- Se llevó a cabo análisis de la matriz de riesgos del proceso, matriz de riesgos de corrupción y matriz de riesgos de seguridad de la información.
- Se hizo revisión a la aplicabilidad de las políticas de seguridad de la información establecidas en la resolución 095 de 26 de febrero de 2018 en el que el subsistema de gestión de seguridad y privacidad de la información forma parte del Sistema Integrado de Gestión Institucional.

7.3.1.1 De los cinco procedimientos se verificaron de manera detallada los siguientes:

7.3.1.1.1 El procedimiento GTI-P-01 v1. Procedimiento de Solicitud de servicios de Tecnología, fue evaluado para el periodo, en el primer semestre del año se evidencia que el 100% de los incidentes registrados en la herramienta de mesa de ayuda fueron atendidos en su totalidad en los diferentes niveles de atención que existen en el proceso de Gestión de Tecnologías de información.

Enero	Febrero	Marzo	Abril	Mayo	Junio
21	15	12	19	23	14
44	14	11	8	0	0
				15	19
12	38	20	26	42	22
39	56	43	49	45	27
81	77	36	24	61	37
49	37	23	34	45	21
246	237	145	160	231	140
	0	2	0	0	0
246	237	143	160	231	140
90%	90%	90%	90%	90%	90%
100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

7.3.1.1.2 Se evalúo el GTI-P-02 Procedimiento de Gestión de Cambios de TI en cambios específicos realizados:

- Cambio realizado el día 11/05/2018 se llevó a cabo la actualización de políticas de la red wifi de la ANDJE.
- Cambio realizado el día 23/06/2018 en el que modificó el firmware de un servidor de la plataforma tecnológica de la Entidad.

En los dos casos, se evidenció el cumplimiento de las actividades del procedimiento incluyendo el uso del formato GTI-F-09 Formato de Solicitud de Cambios RFC.

7.3.1.1.3 Se evalúo el GTI-P-05 Procedimiento de Gestión de Incidentes de Seguridad de la Información para los incidentes de seguridad presentados en el primer semestre de 2018, y fueron los siguientes:

- Incidente Número 1374 Falla en la Infraestructura Física: "*Se presenta falla en el electroimán que controla el acceso al centro de datos principal de la Agencia, se notifica verbalmente al proceso de gestión administrativa acerca del incidente.*"

- Incidente Número 2256 Falla en la Infraestructura Tecnológica: "*Falla en la infraestructura del Switch Core de la Agencia, lo que provoco indisponibilidad de los canales de comunicación internos, de los sistemas eKOGUI, Orfeo y portales por 3 horas aproximadamente.*"

- Incidente Número 2606 Perdida de Información: "*Por lo anterior dando cumplimiento a la solución del ticket 2574 solicitado por la funcionaria (Nombre de Funcionaría), se evidencia por parte del equipo de infraestructura tecnológica que este Backup fuel mal generado por parte del equipo de soporte técnico de primer nivel, esto debido a que el archivo (pst) no corresponde al usuario (Nombre de Funcionaria).*"

En los tres (03) casos se evidenció que se llevaron a cabo las actividades y la documentación pertinente para cumplir con el procedimiento.

7.3.2 Solicitud Información de la Oficina de Control para caso especifico

El pasado 19 de julio, el jefe (e) de la Oficina de Control Interno en el marco del Decreto 1083 de 2015 (Función Pública) articulo 2.2.21.5.3 (Libro 2, Parte 2, Titulo 21, Capítulo 5) mediante correo electrónico solicitó información al encargado del Proceso de Gestión de Tecnologías en lo referente a el uso de la infraestructura tecnológica por parte de exfuncionarios del Proceso de Gestión Financiera que ya no laboraban en la Entidad.

El 27/07/2018 el líder del proceso de Gestión de Tecnologías mediante correo electrónico respondió las inquietudes de la oficina de Control Interno. Dentro de las respuestas se anexaron documentos como el pantallazo del ticket No. 5641 y correo de funcionaria de Financiera, ambos posteriores a la solicitud de información de la OCI.

En el marco de la Auditoria el líder del Proceso realizó las siguientes aclaraciones:

- En el Procedimiento GTI-P-01 "Solicitar incidente o requerimiento de servicios TI.", se enuncia en la salida de la actividad No. 1 el formato Solicitud de servicio de tecnología y formato GTI-F04. En donde indicaron que este no se diligencia para los casos de los visitantes; el anterior tiene como objetivo registrar la creación, modificación, des habilitación o eliminación de cuentas de usuario para gestión del proceso Gestión de Tecnologías de la Información.

- Los usuarios genéricos tienen privilegios de navegación limitada, ya que son usuarios visitantes que en cualquier lugar como puede ser: cafeterías, aeropuertos, estaciones de bus etc. Por lo anterior no se consideran como riesgo para la entidad. Además, el usuario entregado no es de tipo "usuario local estándar" como se menciona en la observación y se puede evidenciar en la mesa de ayuda de TI, el cual corresponde a un usuario dentro del Directorio Activo y esta con las políticas de seguridad perimetral correspondiente a un usuario de bajos privilegios en la red de la entidad.

- Desde el año 2016 y a la fecha, Gestión de Tecnologías de la Información no solo ha divulgado las políticas de seguridad para todos los colaboradores de la Agencia, sino también se ha encargado de gestionar visitas externas con la participación de la Policía Nacional, Superintendencia de Industria y Comercio, Ministerio de las Tecnologías, en pro de las buenas prácticas en lo que respecta el cuidado de la información.

- El respectivo acceso y buen uso de los sistemas externos de la entidad no hace parte de la vigilancia o auditoria por parte del proceso de tecnología de la entidad y en ningún caso es potestad de autorización, tockens y/o contraseñas, estas son directamente del usuario y del coordinador de Financiera, además del encargado del sistema en este caso el ministerio de hacienda.
  Además de lo anterior, los colaboradores que hacen parte del Grupo de Gestión Financiera deberán ser responsables con el uso de la información contenida en el SIIF Nación y con la información que se produce al interior del proceso.

También es importante indicar que como política es importante utilizar el sistema desde el computador de la entidad, no debe realizar transacciones desde computadores o lugares públicos, como cafés Internet, equipos o conexiones a internet desconocidos.

- Tecnología de la Información no es responsable de la administración del aplicativo SIIF, ni mucho menos de sus usuarios, tal y como lo establece las Políticas de Seguridad de la Agencia, DE-M-02 Manual de Políticas Institucionales y de Desarrollo Administrativo, numeral 3.4.14 POLÍTICA GESTIÓN FINANCIERA. La responsabilidad de Gestión de Tecnologías de la Información, es concienciar a los procesos y a los colaboradores de no prestar sus usuarios y más aún si son de aplicativos externos, tarea que se ha venido realizando desde el 2016 y como se evidencia en los controles de asistencia de las charlas realizadas

7.3.3 Seguimiento a las No Conformidades anteriores (Planes de Mejoramiento)

REQUISITO DE LA NORMA	HALLAZGOS	SEGUIMIENTO DE LA OCI
No aplica	No se presentaron	No aplica

Fuente Informe de Auditoria de agosto 10 de 2017 de la OCI

7.3.4 Seguimiento a los Mapas de Riesgos

7.3.4.1 En relación al Mapa de Riesgos de Proceso Operativos

El proceso de Gestión de Tecnologías de información definió tres (03) riesgos de proceso operativos, donde se evidenció:

1. El Riesgo “Inadecuada conceptualización de los requerimientos para el desarrollo o mejoras de los sistemas de información”, ubicado en nivel moderado y el control para su mitigación es la aplicación del procedimiento “GTI P 03 Solicitud y aprobación de nuevos desarrollos o mejoras de software”; no tiene un plan de acción establecido, ya que este se asume a través de la revisión en conjunto con el colaborador que solicita la mejora o el desarrollo de la aplicación a mejorar o desarrollar.

2. El Riesgo “Adquisición, arrendamiento y/o construcción de soluciones informáticas que no se encuentran alineadas con los objetivos estratégicos de la Entidad”, definido con un nivel moderado, tiene plan de acción con dos (02) actividades:

   - Divulgar a los líderes misionales sobre adquisición yo desarrollo de nuevos sistemas de información.
   - Generar memorando para todas las direcciones y oficinas sobre los lineamientos de sistemas de información.

   En el marco de la auditoria se indicó que se desarrollaron reuniones de grupo primario directivo y de secretaria general, donde consta en Acta de Reunión GPSG – 63.

   Es de anotar que estas actividades se tienen previstas desarrollar entre el 01/07/2018 al 30/09/2018 y al 30/11/2018 respectivamente.

3. El Riesgo “Inoportunidad en la atención de incidentes o requerimientos de TI” definido con un nivel moderado, tiene plan de acción con tres (03) actividades:

   - Desarrollar el portafolio de servicios y establecer los diferentes Acuerdos de Niveles de Servicio - ANS e incorporar en los documentos del proceso.
   - Caracterizar los usuarios solicitantes e incorporar en los documentos del proceso.
   - Socializar los documentos (portafolio y ANS) a los colaboradores involucrados.

A la fecha de la auditoria se evidenció que el encargado del proceso de tecnología cuenta con los respectivos documentos borrador sobre los que se han venido trabajando en conjunto con los diferentes niveles de soporte de TI; como soporte de lo anterior se presentó los avances en las siguientes acciones:

- Documento Portafolio y Catálogo de Servicios Tecnología
- Actividades del Catálogo de Servicios
- Documento Actividades del Catálogo de Servicio en donde se establece los diferentes ANS.
- Formato Caracterización de usuarios solicitantes e incorporar en los documentos del proceso.

Estas actividades se tienen previstas desarrollar entre el 01/07/2018 al 31/10/2018 y al 31/11/2018

7.3.4.2 En relación con Mapa de Riesgos de Corrupción

El proceso de Gestión de Tecnologías de Información identificó el riesgo de corrupción "Fuga de Información" para el cual se realizaron las actividades previstas en el plan de tratamiento, no se identifican nuevos riesgos de corrupción. Las actividades se realizaron con corte a abril 30 de 2018 así:

Apoyo en la proyección y elaboración de la Resolución 095 del 26 de febrero de 2018, "Por la cual se adopta el Nuevo Sistema Integrado de Gestión Institucional –SIGI – en la Agencia Nacional de Defensa Jurídica del Estado y se dictan otras disposiciones", en lo que respecta Seguridad de la información en los siguientes aspectos:

- Conformación del nuevo sistema integrado de gestión institucional, conformación del Subsistema de Seguridad y Privacidad de la Información.
- Definición de los Roles y Responsabilidades de los colaboradores de la ANDJE frente al Subsistema de Seguridad y Privacidad de la Información.
- Creación y funciones del comité institucional, apoyo para la gestión del Subsistema de Seguridad y Privacidad de la Información.

7.3.4.3 En relación con el Mapa de riesgos de la Seguridad de la Información

El proceso de Gestión de Tecnologías de información definió cuatro (04) riesgos, de los cuales se evidenció:

1. Riesgo "Posible falla total o parcial de los servicios tecnológicos de la ANDJE, debido a exposición a vulnerabilidades informáticas por desactualización en: Servidores y/o Sistemas Operativos, afectando Confidencialidad, Integridad y Disponibilidad de la información"

2. Riesgo "Posibles Fallas en las copias de seguridad que se generan, debido a que no se realizan pruebas periódicas de las mismas afectando Integridad y Disponibilidad de la información."

3. Riesgo "Posibles accesos no autorizados a los servidores y sistemas de información de la ANDJE, debido a la ausencia de lineamientos para la gestión de usuarios afectando Confidencialidad, Integridad y Disponibilidad de la información."

4. Riesgo "Posible Fuga y/o modificación 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."

Todos los riesgos anteriores tuvieron acciones de tratamiento durante el 2016 y algunos hasta diciembre de 2017 con todas las tareas o actividades terminadas de acuerdo al plan de tratamiento que se estableció.

En lo corrido del 2018 se han venido realizando seguimientos a los riesgos de seguridad de la información como costa en el Acta AG-1051, dónde se evidencia seguimiento a los riesgos en mayo de 2018 y donde queda en evidencia que los riesgos si se asocian con procedimiento propios de Gestión de Tecnologías de la información.

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

REQUISITO	NO CONFORMIDAD	OBSERVACIONES
No se presentaron	No se presentaron	No se presentaron

9. RECOMENDACIONES:

9.1 Matriz de Riesgos

De acuerdo a la evaluación de los riesgos establecidos en la Matriz de riesgos de seguridad, operativos y de corrupción y dado que frecuentemente se realizan cambios en la infraestructura tecnológica, se realizan nuevos desarrollos, se prestan nuevos servicios, se adoptaron nuevos prácticas de mesa de ayuda, se establecieron nuevas políticas de seguridad informática; se recomienda evaluar las diferentes matrices de riesgos y evaluar si se hace necesario detectar nuevos riesgos con el propósito de aumentar el nivel de madurez de la plataforma tecnológica de la Entidad.

9.2 Seguridad de la Información

Como continuidad a los procesos de aseguramiento de la plataforma tecnológica y a las políticas establecidas a través del subsistema de Seguridad y Privacidad de la información se recomienda continuar con la concientización y aplicación de dichas políticas por parte de todos los usuarios de la Agencia.

9.3 Mesa de ayuda

En el marco de las políticas de Gobierno Digital y los compromisos adquiridos con el Ministerio de Tecnologías de Información y comunicaciones sobre la iniciativa/proyecto Mesa de Servicios, se recomienda continuar fortaleciendo los protocolos y actividades de la mesa de ayuda ya que se ha hecho un gran avance implementado los primeros procedimientos. Y mantener las campañas de concientización de uso de la mesa de ayuda a los usuarios de la Entidad.

Firma Auditor Designado y Equipo Auditor	Firma Jefe de Control Interno ANDJE
Informe realizado Electrónicamente por: Manuel Humberto Sierra López Técnico Oficina de Control Interno No. Radicado: 20181020011743.	Informe Firmado Electrónicamente por: Luis Eberto Hernández León Jefe Oficina de Control Interno No. Radicado: 20181020011743.