REFERENCIA	NOMBRE DE AUDITORIA	FECHA DE REALIZACIÓN		FECHA DEL INFORME
		INICIO	CIERRE	
A-P-GTI-01-20	Auditoria al proceso de Gestión de Tecnologías de la Información	26/10/2020	30/11/2020	28/12/2020

PROCESO /AREA AUDITADA	AUDITOR LIDER / AUDITOR
Gestión de Tecnologías de la Información	LILIANA BARBOSA CARRILLO
EQUIPO DE AUDITORES	**AUDITORES ACOMPAÑANTES**
Ninguno	Ninguno

1. OBJETIVOS:

Evaluar el Proceso 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.

2. ALCANCE:

Comprende la evaluación del Proceso Gestión de Tecnologías de la Información sobre las acciones del proceso adelantadas durante el periodo 1 de octubre de 2019 y 30 de septiembre de 2020.

3. CRITERIOS:

- 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
- Decreto 1069 de 2015. Decreto Único Reglamentario del Sector Justicia y del Derecho - http://suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/30019870
- Decreto 1008 de 2018, el cual modificó el Decreto 1078 de 2015, en su artículo 2.2.9.1.1.3 definió la seguridad de la información como principio de la Política de Gobierno Digital. - http://suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/30019521
- Decreto 1499 de 2017 modificó el Decreto 1083 de 2015 (Decreto Único Reglamentario del Sector de Función Pública), y adoptó el Modelo Integrado de Planeación y Gestión - MIPG. Decreto 1083 de 2015 (Función Pública) ARTÍCULO 2.2.21.5.2 Libro 2, Parte 2, Titulo 21, Capítulo 5.- http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/30019891
- Decreto Ley 4085 de 2011. Por el cual se establecen los objetivos y la estructura de la Agencia Nacional de Defensa Jurídica del Estado. http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/1541296
- Decreto Reglamentario 1377 de 2013 - http://suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/1276081
- Resolución 338 del 24 de septiembre de 2020 que deroga la 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. https://www.defensajuridica.gov.co/normatividad/normas-internas/resoluciones_2019/Lists/resoluciones_2020/Attachments/9/res_338_24_septiembre_2020.pdf
- Marco de mejores prácticas en Tecnología alineados con COBIT 5, ITIL V3 2011 E ISO 27000:2013
- CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa https://www.mintic.gov.co/portal/inicio/3510:Conpes-3701-de-2011
- CONPES 3854 de 2016 Política Nacional de Seguridad Digital https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf
- CONPES 3995 2020 Política Nacional De Confianza y Seguridad Digital. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf
- CONPES N° 3920 - Política nacional de explotación de datos (Big Data) https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3920.pdf
- Modelo de Gestión de Riesgos de Seguridad Digital-MGRSD https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion

+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%C3%BAblicas+-+Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b

4. LIMITACIONES PARA EL DESARROLLO DE LA AUDITORIA:

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

5. DOCUMENTOS EXAMINADOS:

- Mapa de riesgos generales para proceso de Gestión de Tecnologías de la 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.
- GTI-P-01 Solicitud de servicios de TI Versión 2.
- GTI-P-02 GESTIÓN DE CAMBIOS DE TI Versión 0.
- GTI-P-03 SOLICITUD Y APROBACIÓN DE NUEVOS DESARROLLOS O MEJORAS DE SOFTWARE Versión 0.
- GTI-P-04 PROCEDIMIENTO PARA APROVISIONAMIENTO DE SERVIDORES Versión 0.
- GTI-P-05 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION Versión 0.
- Guía Administración de Riesgos Versión 3 fecha 21-09-2018
- Solicitud de información radicad No.

6. PLAN DE MUESTREO

- Se verifica la información suministrada por correo y a través de Orfeo, por parte del Proceso de Gestión de Tecnologías de la Información, en lo referente a procedimientos, contratos 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 Gestión de Tecnologías de la Información.
- Se hacen seguimientos a los avances en relación con evaluaciones anteriores.

7. INFORME

7.1 FORTALEZAS

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

Se resalta el interés por mejorar la estructuración y contenido de documentos relacionados con el Proceso.

7.2 CUMPLIMIENTO DE PRINCIPIOS

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

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

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

7.3 CONTENIDO

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

El proceso de Gestión de tecnologías de la Información hace parte de los procesos transversales de la Entidad, definido mediante Ley 4085 de 2011 y modificado por el Decreto 2269 de diciembre de 2019, 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 los 5 procedimientos que lo integran y que se encuentran documentados en el Sistema Integrado de Gestión Institucional – SIGI, la revisión está orientada a validar los puntos de control existentes.

7.3.1.1 GTI-P-01 Procedimiento Para Solicitud De Servicios De TI

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 con los siguientes usuarios:

Tabla N° 1 Muestra uncionarios

NOMBRES	DEPENDENCIA	CASOS
Luis Felipe Salamanca Cachay	Dirección de políticas y estrategias para la defensa	9508
Melco Javier Leuro	Oficina asesora de planeación	10048
Leonardo Juniors Martinez Joven	Dirección de defensa jurídica nacional	10497
Jhon Jairo Camargo Motta	Dirección de políticas y estrategias	10573
Luz Jhein Aguilar González	Secretaria general	10618
Sandra Garcia Martinez	Oficina asesora de planeación	10622
William Fabian Amaya Cardenas	Secretaria general	10691
Brayan Alexis Escalante Carvajal	Dirección de defensa jurídica nacional	10733
Alexandra Forero Forero	Dirección de defensa jurídica nacional	10831
Jonathan Alber Rondon Barbosa	Dirección de defensa jurídica nacional	10907
Jorge Mario Carrasco Ortiz	Dirección de gestión de información	10974
Fredy Fernando Niño Ochoa	Dirección de gestión de información	10997
Rosse Mary Villamil Cañas	Secretaria general	Traslado DGI a TI.
Carlos Lopez Narvaez	Dirección de gestión de información	11075
Juan Carlos Rozo Romero	Dirección de defensa jurídica nacional	13405
Lissette Cecilia Cervantes Martelo	Dirección de defensa jurídica nacional	14614
Carlos Alfonso Cotrino Guevara	Dirección de defensa jurídica nacional	14872
Maria Fernanda Suarez Celly	Dirección de políticas y estrategias	15243

Fuente: Elaboración propia

Pruebas de funcionalidad y monitoreo de IPv6 en los servicios de la Entidad. Análisis de información y pruebas de funcionalidad frente a las políticas de seguridad perimetral de la infraestructura de TI. Afinamiento de las configuraciones de hardware, software y servicios de la Entidad.

Tabla N° 2 Muestra Contratista

NOMBRE	OBSERVACIONES	CASO
Nicolas Eduardo Ramos Calderon	Fue una sumatoria de otros si, el cual solo se activaba el usuario hasta el mes de febrero.	7514
Hardy Deimont Niño Velasquez	Usuario del área de TI y por la antigüedad que tiene el usuario en la entidad y debido a que soporta la plataforma de Orfeo su usuario es activado por solicitud de Mauricio Galarza, cada vez que se renuevan los contratos.	
Andres Mauricio Briceño Chavez		11237
Alejandra Peláez Peñaranda		10695
Yair Morales Muñoz	Usuario del área de TI y por la antigüedad que tiene el usuario en la entidad y debido a que soporta los portales web de sharepoint su usuario es activado por solicitud de Mauricio Galarza, cada vez que se renuevan los contratos.	
Jorge Iván Rincón	Este usuario no tiene cuentas de acceso a ninguna plataforma tecnológica, nunca fue solicitada.	N/A

Fuente: Elaboración propia

De la muestra seleccionada se evidencia que para los funcionarios que ya venían vinculados con la Agencia, no se realizó la actividad de control establecida en el procedimiento, paso 4. Gestionar la Solicitud de Servicio de TI. ***Si solamente se realiza la actividad para las personas nuevas es necesario incluirlo en las Políticas de Operación. Adicional validar el tema por cuestión de permisos, si el funcionario cambia de área debe tener acceso a otras carpetas compartidas o repositorios de información que deben contar con niveles de autorizaciones diferentes. Para contratistas qué sucede si hay cambio de supervisor de contrato, dice la Política de Operación que debe ser con autorización expresa de Este.***

Se recomienda incluir el Diagrama de flujo del proceso en el documento publicado en el SGSI

GTI-P-02 GESTIÓN DE CAMBIOS DE TI

Se realiza la verificación de la funcionalidad y puntos de control del Procedimiento con los ingenieros delegados por el Líder del Proceso. Se revisan los activos de información para validar que se encuentran los activos relacionados con el procedimiento, así mismo se validó la existencia de ANS dentro de la herramienta.

Se solicita un reporte de la totalidad de las solicitudes realizadas entre el 15 de febrero y el 15 de abril de 2020 estas solicitudes se atienden a través de la mesa de ayuda https://soportetic.defensajuridica.gov.co/, un reporte gráfico de la atención de solicitudes el mes de octubre de 2020 y estadística gráfica.

Se recomienda crear un Indicador de atención de gestión de cambios que mida cuantos tienen calificación de emergencia, estándar y normal.
Se recomienda crear un indicador de cumplimiento de ANS para la atención de solicitudes.

GTI-P-03 SOLICITUD Y APROBACIÓN DE NUEVOS DESARROLLOS O MEJORAS DE SOFTWARE

Se revisa el procedimiento para validar puntos de control, activos de información y se requiere un listado de los casos radicados de desarrollo. validando el caso N° 11410 y N°11041.

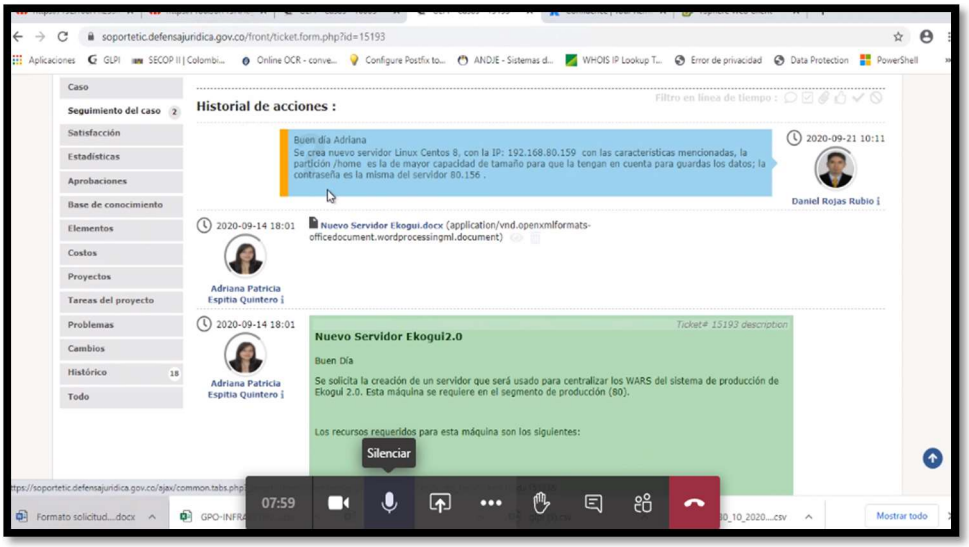
No se evidencia documento tipo parámetro o registro que contenga la metodología para el desarrollo de software, que se alineé a lo requerido en la Guía del dominio de Sistemas de Información del Modelo de Arquitectura

Política de Gobierno Digital Habilitador 1 Arquitectura SIS.01 Guía del dominio de Sistemas de Información. https://www.mintic.gov.co/arquitecturati/630/articles-9262_recurso_pdf.pdf Pag 48. 2.6.1 Metodología de referencia para desarrollo de sistemas de información

GTI-P-04 PROCEDIMIENTO PARA APROVISIONAMIENTO DE SERVIDORES

Se realiza la verificación de la funcionalidad y puntos de control del Procedimiento con los ingenieros delegados por el Líder del Proceso.

Gráfica N° 1



Fuente: Evidencias aportadas por el Proceso

Se revisan los activos de información, la realización de back up y la realización de restauración de información.

Se revisa el procedimiento GTI-P-04 y es una actividad más dentro de las opciones de la mesa de servicio, se recomienda eliminar este procedimiento e integrarlo en el GTI-P-01 Procedimiento Para Solicitud De Servicios De TI

GTI-P-05 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

Se revisa el procedimiento, no es posible validar los puntos de control registrados dado que no hay reporte de incidentes de seguridad durante el periodo evaluado.

No se evidencia la inclusión de aspectos que estén alineados con el ciclo de vida de gestión y respuesta a un incidente de seguridad, el Procedimiento tiene en cuenta hasta la fase de Detección y análisis, faltando incluir las fases de contención, erradicación y recuperación y las actividades Post- incidentes

MSPI - 5. Definición formal de la guía propuesta para la gestión de incidentes *5.1 preparación Esta etapa dentro del ciclo de vida de respuesta a incidentes suele hacerse pensando no sólo en crear un modelo que permita a la entidad estar en capacidad de responder ante estos, sino también en la forma como pueden ser detectados, evaluados y*

gestionar las vulnerabilidades para prevenirse, asegurando que los sistemas, redes, y aplicaciones son lo suficientemente seguros. Guía No. 21 guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información

Política De Gobierno Digital *El objetivo general del Documento CONPES 3701 fue fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra la defensa y seguridad nacional en el ámbito cibernético (ciberseguridad y ciberdefensa)10, creando un ambiente y unas condiciones para brindar protección en el ciberespacio. Para cumplir este objetivo general, se formularon tres objetivos específicos: (i) implementar instancias apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias cibernéticas para afrontar las amenazas y los riesgos que atentan contra la ciberseguridad y ciberdefensa nacional.*

Gráfica N° 2 Fases Proceso Gestión de Incidentes

Fuente: Guía N° 21 MSPI

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

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

7.3.2.1 Riesgos de Proceso:

- Inadecuada conceptualización de los requerimientos para el desarrollo o mejoras de los sistemas de información.

- CONTROL GTI P 03 Solicitud y aprobación de nuevos desarrollos o mejoras de software – Adquisición, arrendamiento y/o construcción de soluciones informáticas que no se encuentran alineadas con los objetivos estratégicos de la Entidad.

- CONTROL . 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 Debilidad de control, la 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. No menciona al Líder de TI o quien haga sus veces, alguna obligatoriedad de autorización del área de TI, no se evidencian lineamientos sobre requisitos de alineación de contratación con objetivos

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.

DECRETO 415 DE 2016 A RTÍCULO 2.2.35.3. Objetivos del fortalecimiento institucional. Para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones las entidades y organismos a que se refiere el presente decreto, deberán: 1. Liderar la gestión estratégica con tecnologías de la información y las comunicaciones mediante la definición, implementación, ejecución, seguimiento y divulgación de un Plan Estratégico de Tecnología y Sistemas de Información (PETI) que esté alineado a la estrategia y modelo integrado de gestión de la entidad y el cual, con un enfoque de generación de valor público, habilite las capacidades y servicios de tecnología necesarios para impulsar las transformaciones en el desarrollo de su sector y la eficiencia y transparencia del Estado

- Memorando para todas las direcciones y oficinas sobre los lineamientos de sistemas de información.

- Aprobación a través del Comité Gestión y Desempeño institucional. *Se recomienda que la Adquisición, arrendamiento y/o construcción de soluciones informáticas se encuentren alineadas con los objetivos estratégicos de la Entidad. PETI*

- Inoportunidad en la atención de incidentes o requerimientos de TI.

  CONTROL Acuerdos de niveles de servicio, Atención de Mesa de ayuda de los servicios que apoyan al proceso de Gestión de tecnologías de Información – Portafolio y catálogo de servicios –

7.3.2.2 Riesgos de CORRUPCIÓN

- Fuga de información para favorecer a un tercero

CONTROLES
*Sistema de SIEM Gestor de eventos e información de Seguridad - Reporte cuatrimestral
*GTII01 Instructivo de control de accesos a centro de datos - Seguimiento
*Sistema de control de acceso de directorio activo para usuarios de la red - Seguimiento
*Sistema NAGIOS monitoreo a la infraestructura - Seguimiento
*Separación de ambientes informáticos para los sistemas misionales ekogui y orfeo - Seguimiento evidencia documentado
*Política de seguridad y privacidad de la información contenidas en el Manual de políticas de gestión y desempeño institucional de la agencia DEM02 – Evidencia de los controles en los procedimientos de seguridad

No se evidencia reporte al líder del proceso de los controles del riesgo de corrupción con la periodicidad que pide la guía, con el objetivo de monitorear la no materialización.

GUÍA ADMINISTRACIÓN DE RIESGOS ANDJE 9. MONITOREO Y REVISIÓN
Los líderes de los procesos en conjunto con sus equipos deben monitorear y revisar mensualmente el Mapa de Riesgos incluidos los de Corrupción y si es del caso ajustarlo.
Su importancia radica en la necesidad de monitorear permanentemente la gestión del riesgo y la efectividad de los controles establecidos. En esta fase se debe:
1. *Garantizar que los controles son eficaces y eficientes.*
2. *Obtener información adicional que permita mejorar la valoración del riesgo.*
3. *Analizar y aprender lecciones a partir de los eventos, los cambios, las tendencias, los éxitos y los fracasos.*
4. *Detectar cambios en el contexto interno y externo.*
5. *Identificar riesgos emergentes.*

Nota: El Monitoreo y Revisión permite determinar la necesidad de modificar, actualizar o mantener en las mismas condiciones los factores de riesgo, así como su identificación, análisis y valoración.
Para los riesgos de corrupción se deberá identificar la presencia de hechos significativos como:
- *Riesgos materializados de corrupción.*
- *Observaciones, investigaciones disciplinarias, penales, fiscales, o de entes reguladores, o hallazgos por parte de la Oficina de Control Interno.*
- *Cambios importantes en el entorno que den lugar a nuevos riesgos.*

7.3.2.3 Riesgos de seguridad de la Información

No se evidencia seguimiento trimestral al riesgo de Seguridad de la información y presentación del resultado de este seguimiento al Comité de Gestión y Desempeño Institucional.

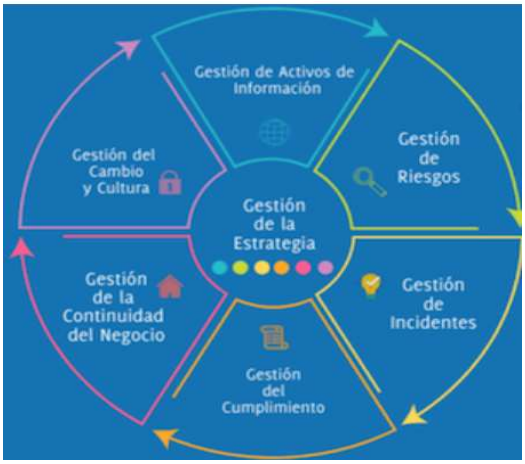
GUÍA ADMINISTRACIÓN DE RIESGOS - 13.5.4 Responsabilidades SEGUIMIENTO AL TRATAMIENTO DEL RIESGO El responsable del Sistema de Gestión de Seguridad de la Información con el apoyo del profesional del SGSI, solicitara trimestralmente al líder del proceso (dueño del riesgo) los avances y evidencias de los tratamientos de los riesgos a cargo de su gestión. ACEPTACIÓN DE LOS RIESGOS Y RIESGOS RESIDUALES El líder del proceso (dueño del riesgo) será el responsable de aceptar o rechazar los riesgos y riesgos residuales, posteriormente el responsable del Sistema de Gestión de Seguridad de la Información con el apoyo del profesional del SGSI deben presentar los riesgos y riesgos residuales al comité institucional de desarrollo administrativo CIDA también para su aprobación o rechazo.

Se recomienda actualizar el nombre del Comité en el documento GUÍA ADMINISTRACIÓN DE RIESGOS - 13.5.4 Responsabilidades (…) el responsable del Sistema de Gestión de Seguridad de la Información con el apoyo del profesional del SGSI deben presentar los riesgos y riesgos residuales al comité institucional de desarrollo administrativo CIDA también para su aprobación o rechazo.

7.3.3 Activos de información

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

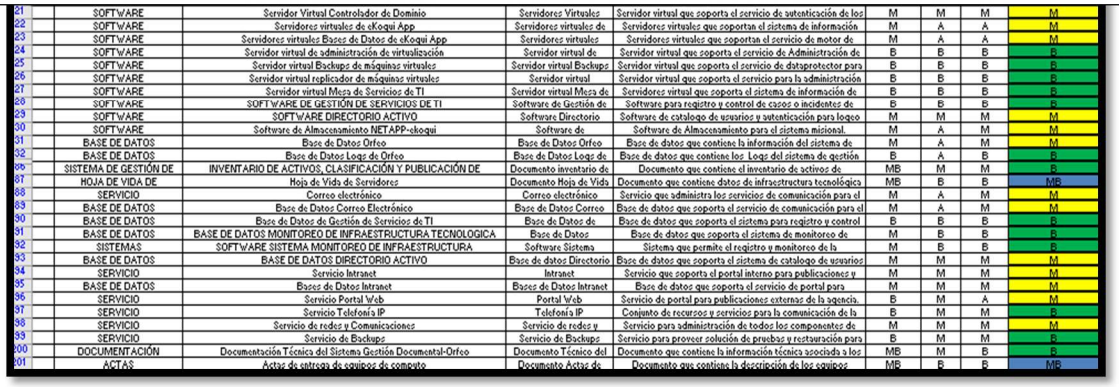
Gráfica No 3 : Gestión integral de la seguridad de la información



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

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

Gráfica No 4. Activos de información Proceso Gestión de Información



21	SOFTWARE	Servidor Virtual Controlador de Dominio	Servidores Virtuales	Servidor virtual que soporta el servicio de autenticación de los	M	M	M	M
22	SOFTWARE	Servidores virtuales de eKoqui App	Servidores virtuales de	Servidores virtuales que soportan el sistema de información	M	A	A	M
23	SOFTWARE	Servidores virtuales Bases de Datos de eKoqui App	Servidores virtuales	Servidores virtuales que soportan el servicio de motor de	M	A	A	M
24	SOFTWARE	Servidor virtual de administración de virtualización	Servidor virtual de	Servidor virtual que soporta el servicio de Administración de	B	B	B	B
25	SOFTWARE	Servidor virtual Backups de máquinas virtuales	Servidor virtual Backups	Servidor virtual que soporta el servicio de dataprotector para	B	B	B	B
26	SOFTWARE	Servidor virtual replicador de máquinas virtuales	Servidor virtual	Servidor virtual que soporta el servicio para la administración	B	B	B	B
27	SOFTWARE	Servidor virtual Mega de Servicios de TI	Servidor virtual Mega de	Servidores virtual que soporta el sistema de información de	B	B	B	B
28	SOFTWARE	SOFTWARE DE GESTIÓN DE SERVICIOS DE TI	Software de Gestión de	Software para registro y control de casos o incidentes de	B	B	B	B
29	SOFTWARE	SOFTWARE DIRECTORIO ACTIVO	Software Directorio	Software de catalogo de usuarios y autenticación para logeo	M	M	M	M
30	SOFTWARE	Software de Almacenamiento NETAPP-ekoqui	Software de	Software de Almacenamiento para el sistema misional.	M	A	M	M
31	BASE DE DATOS	Base de Datos Orfeo	Base de Datos Orfeo	Base de datos que contiene la información del sistema de	M	A	M	M
32	BASE DE DATOS	Base de Datos Logs de Orfeo	Base de Datos Logs de	Base de datos que contiene los Logs del sistema de gestión	B	A	B	B
86	SISTEMA DE GESTIÓN DE	INVENTARIO DE ACTIVOS, CLASIFICACIÓN Y PUBLICACIÓN DE	Documento inventario de	Documento que contiene el inventario de activos de	MB	M	M	B
87	HOJA DE VIDA DE	Hoja de Vida de Servidores	Documento Hoja de Vida	Documento que contiene datos de infraestructura tecnológica	MB	B	B	MB
88	SERVICIO	Correo electrónico	Correo electrónico	Servicio que administra los servicios de comunicación para el	M	A	M	M
89	BASE DE DATOS	Base de Datos Correo Electrónico	Base de Datos Correo	Base de datos que soporta el servicio de comunicación para el	M	A	M	M
90	BASE DE DATOS	Base de Datos de Gestión de Servicios de TI	Base de Datos de	Base de datos que soporta el sistema para registro y control	B	B	B	B
91	BASE DE DATOS	BASE DE DATOS MONITOREO DE INFRAESTRUCTURA TECNOLOGICA	Base de Datos	Base de datos que soporta el sistema de monitoreo de	M	B	B	B
92	SISTEMAS	SOFTWARE SISTEMA MONITOREO DE INFRAESTRUCTURA	Software Sistema	Sistema que permite el registro y monitoreo de la	M	B	B	B
93	BASE DE DATOS	BASE DE DATOS DIRECTORIO ACTIVO	Base de datos Directorio	Base de datos que soporta el sistema de catalogo de usuarios	M	M	M	M
94	SERVICIO	Servicio Intranet	Intranet	Servicio que soporta el portal interno para publicaciones y	M	M	M	M
95	BASE DE DATOS	Bases de Datos Intranet	Bases de Datos Intranet	Base de datos que soporta el servicio de portal para	M	M	M	M
96	SERVICIO	Servicio Portal Web	Portal Web	Servicio de portal para publicaciones externas de la agencia.	B	M	A	M
97	SERVICIO	Servicio Telefonía IP	Telefonía IP	Conjunto de recursos y servicios para la comunicación de la	B	M	M	B
98	SERVICIO	Servicio de redes y Comunicaciones	Servicio de redes y	Servicio para administración de todos los componentes de	M	M	M	M
99	SERVICIO	Servicio de Backups	Servicio de Backups	Servicio para proveer solución de pruebas y restauración para	B	M	M	B
200	DOCUMENTACIÓN	Documentación Técnica del Sistema Gestión Documental-Orfeo	Documento Técnico del	Documento que contiene la información técnica asociada a los	MB	M	B	B
201	ACTAS	Actas de entrega de equipos de computo	Documento Actas de	Documento que contiene la descripción de los equipos	MB	B	B	MB

Fuente Pagina Web - Intranet

Grafica N° 5 Criterios de evaluación de activos de información

A (ALTA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
M (MEDIA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.
B (BAJA)	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA.

Tabla4. Esquema de clasificación por Integridad

INFORMACION PUBLICA RESERVADA	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.
INFORMACION PUBLICA CLASIFICADA	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
INFORMACION PÚBLICA	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PUBLICA RESERVADA.

Tabla3. Esquema de clasificación por confidencialidad

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Tabla 1: Criterios de Clasificación

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Tabla 2: Niveles de Clasificación

Fuente: Guía N° 21 MSPI

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

POLÍTICA NACIONAL DE SEGURIDAD DIGITAL - https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf (...) Adicionalmente, el mencionado ministerio diseñará e implementará esquemas tecnológicos y procedimentales para garantizar la identificación, autenticación y autorización de funcionarios, ciudadanos, activos de información y recursos (38) que acceden a la infraestructura del Estado colombiano (38) Activos de información y recursos se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.

POLITICA DE GOBIERNO DIGITAL Guía No. 5 - Guía para la Gestión y Clasificación de Activos de Información. La cual da lineamiento expreso para l a clasificación.7.1. Clasificación De Acuerdo Con La Confidencialidad, 7.2. Clasificación De Acuerdo Con La Integridad, 7.3. Clasificación De Acuerdo Con La Disponibilidad, .4. Etiquetado De Activos De Información

La responsabilidad sobre los activos Según establece la norma ISO 27002 es necesario justificar los activos y que cuenten con un propietario que debe estar correctamente identificado. Los propietarios de los activos tendrán la responsabilidad de mantener los controles necesarios. La implantación de los controles específicos se puede delegar por parte del propietario de forma conveniente. No obstante, el propietario será el responsable de la adecuada protección de todos los activos. La persona o entidad que será la responsable de un activo, debe contar con la aprobación del órgano de dirección, para establecer el control de la producción, el desarrollo, el mantenimiento, la utilización y la seguridad de todos los activos El término propietario no significa que la persona responsable disponga de los derechos de propiedad reales del activo, simplemente se dedica a proteger que no le suceda nada.

7.3.4 Planes de Mejoramiento

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

Tabla 3. Planes de mejoramiento Proceso Gestión de Tecnologías de la Información

Hallazgo	Validación de la acción propuesta por TI
N° 278 Fuga de información para favorecer a un tercero - Extracción de información almacenada en los diferentes sistemas misionales o de apoyo que reposan en la infraestructura de la ANDJE	Fecha registro 2019-10-31 es la materialización de un riesgo?
N° 300 Durante el proceso auditor no se evidenció herramienta o instrumento que permita medir y evaluar el porcentaje de avance consolidado del Plan Estratégico de Tecnología - PETI en concordancia con lo establecido en el Manual Operativo de Gobierno Digital. Lo anterior, no permite establecer aspectos como Ahorro en términos de tiempos y recursos. Disminución de costos. Desviaciones de cumplimiento.	Continúa presentándose la situación
N° 301 Durante la verificación se evidenció la planeación estratégica documento de PETI para la vigencia 2019-2022, sin embargo, en este documento no se confirma la alineación con la estrategia y modelo integrado de gestión de la entidad.	Continúa presentándose la situación
N° 302 Determinar acciones encaminadas a llegar al 100% de implementación de la política de Gobierno Digital y MSPI teniendo en cuenta las herramientas de diagnóstico suministradas por la auditoria.	No se evidencia un porcentaje de logro frente al autodiagnóstico realizado
N° 303 Fortalecer el sistema de riesgos del proceso GTI y Seguridad de la información, con el fin de cubrir todos los temas relevantes que este soporta y revisar los controles a la luz de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4.	Se está implementando un plan
N° 304 Como resultado de las pruebas funcionales realizadas en la intranet a los diferentes canales de reporte de incidentes de seguridad, como se evidencia en el anexo 1, no se está facilitando el cumplimiento la actividad 1 del procedimiento; situación que no permite en caso ocurrencia el correspondiente reporte por parte de los colaboradores de la Entidad.	Se valida el cumplimiento del plan de mejoramiento

Fuente: Guía N° 21 MSPI

Se evidencia debilidad en el plan de mejoramiento suscrito correspondiente a las acciones No. 300, 302, 302 y 303, dado que con el análisis de causas realizado no se logró su eliminación, por lo que se debe cerrar el plan de mejoramiento como ineficaz. Es necesario reformular el plan de mejoramiento, incluyendo las acciones necesarias para cumplir con la Política de Gobierno Digital y de Seguridad Digital.

Esta situación denota una desalineación con el 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 institucionales, según corresponda. ***La formulación de planes de mejoramiento, su aplicación y seguimiento para resolver los hallazgos presentados.***

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

7.3.5. 1 Cumplimiento a indicadores de gestión

- Indicador:01-GTI-20 Atención de solicitudes de servicios TIC
- Indicador:02-GTI-20 Nivel de disponibilidad de los servicios tecnológicos por tipo
- Indicador: 03-GTI-20 Incidentes de seguridad de la información atendidos oportunamente

Se recomienda evaluar la medición realizada porque no se tiene componente de calidad para medir el servicio en atención de solicitudes puede ser % atendido por debajo del ANS, Para incidentes de seguridad orientarlo a otros factores como capacitación, canales, pruebas de vulnerabilidad)

7.3.5.2 Cumplimiento a indicadores de MIPG

- Indicador:48-MIPG-20 Repositorio de conocimiento hecho y socializado
- Indicador:49-MIPG-20 Informe de activación de políticas de seguridad en IPv6 (Fase implementación) realizado

No se evidencia un plan que contenga las tres fases de transición de IPV4 a IPV6. Fase I. Planeación de IPv6 – Diagnóstico. Fase II. Implementación del protocolo IPv6 -Desarrollo del Plan de implementación. Fase III. Pruebas de funcionalidad de IPv6, aprobado por la Alta Dirección

Guía de Transición de IPv4 a IPv6 para Colombia - 7. FASES DE TRANSICIÓN
7.1 Fase I. Planeación de IPv6 - Diagnóstico

- *Construcción del plan de Diagnóstico*
- *Inventario de TI (Hardware, Software)*
- *Análisis de la nueva topología de la infraestructura actual y su funcionamiento*
- *Protocolo de pruebas de validación de aplicativos, comunicaciones, plan de seguridad y coexistencia de los protocolos*
- *Planeación de la transición de los servicios tecnológicos de la Entidad*
- *Validación de estado actual de los sistemas de información, los sistemas de comunicaciones, las interfaces y revisión de los RFC correspondientes.*
- *Identificación de esquemas de seguridad de la información y las comunicaciones*

7.2 Fase II. Implementación del protocolo IPv6 -Desarrollo del Plan de implementación

- *Habilitación direccionamiento IPv6 para cada uno de los componentes de hardware y software de acuerdo al plan de diagnóstico de la Primera Fase.*
- *Configuración de servicios de DNS, DHCP, Seguridad, VPN, servicios WEB, entre otros.*
- *Configuración del protocolo IPv6 en aplicativos, sistemas de Comunicaciones, sistemas de almacenamiento en general de los equipos susceptibles a emplear direccionamiento IP.*
- *Activación de políticas de seguridad de IPv6 en los equipos de seguridad y comunicaciones que posea cada entidad de acuerdo con los RFC de seguridad en IPv6.*
- *Coordinación con el (los) proveedor (es) de servicios de Internet ISP, para establecer el enrutamiento y la conectividad integral en IPv6 hacia el exterior*

7.3 Fase III. Pruebas de funcionalidad de IPv6 - Pruebas de funcionalidad de IPv6

- *Pruebas de funcionalidad y monitoreo de IPv6 en los servicios de la Entidad.*
- *Análisis de información y pruebas de funcionalidad frente a las políticas de seguridad perimetral de la infraestructura de TI.*
- *Afinamiento de las configuraciones de hardware, software y servicios de la Entidad.*

- Indicador:50-MIPG-20 Plan de apertura, mejora y uso de datos abiertos formulado y presentado en el CIDG para aprobación Plan de apertura, mejora y uso de datos abiertos

7.3.5.3 Cumplimiento a indicadores de PAAC

- Indicador:5.6-PAAC-20 Set de datos abiertos actualizado

Se recomienda alinear el indicador al objetivo de grado de cumplimiento frente a la Guía para el uso y aprovechamiento de Datos Abiertos en Colombia, Guía de Datos Abiertos de Colombia.pdf

7.3.5.4 Cumplimiento a indicadores de PAI

- Indicador:77-PAI-20 Mejoras al Sistema Orfeo para mejorar su usabilidad- Se verifican evidencias enviadas validando el avance propuesto.

- Indicador:88-PAI-20 Porcentaje de implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

No se tiene un cronograma aprobado por la alta dirección a la cual se pueda asociar el indicador

No se evidencia un objetivo frente al tratamiento de los riesgos de seguridad alineado con la política de riesgos

- Indicador: :94-PAI-20 Porcentaje de implementación del Plan de Seguridad y Privacidad de la Información
- Indicador:97-PAI-20 Porcentaje de implementación del Plan Estratégico de Tecnologías y las Comunicaciones -PETI 2020

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.

Formular los planes de acción anual: Para la formulación de los planes de acción institucional, las entidades deben tomar en cuenta lo previsto en la Ley 152 de 1994, y en el artículo 74 de la Ley 1474 de 2011, en el que se establece que debe especificar en él: (los objetivos, las estrategias, los proyectos, las metas, los responsables, los planes generales de compras y la distribución presupuestal de sus proyectos de inversión) así mismo, deber incluir tanto los aspectos relacionados con el componente misional como con los relacionados con los planes de que trata el Decreto 612 de 2018. (…) Debe incluirse además en el Plan de Acción, las acciones y estrategias a través de las cuales las entidades facilitarán y promoverán la participación de las personas en los asuntos de su competencia, en los términos señalados en el artículo 2 de la Ley 1757 de 2015.

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 a comité y aprobado.

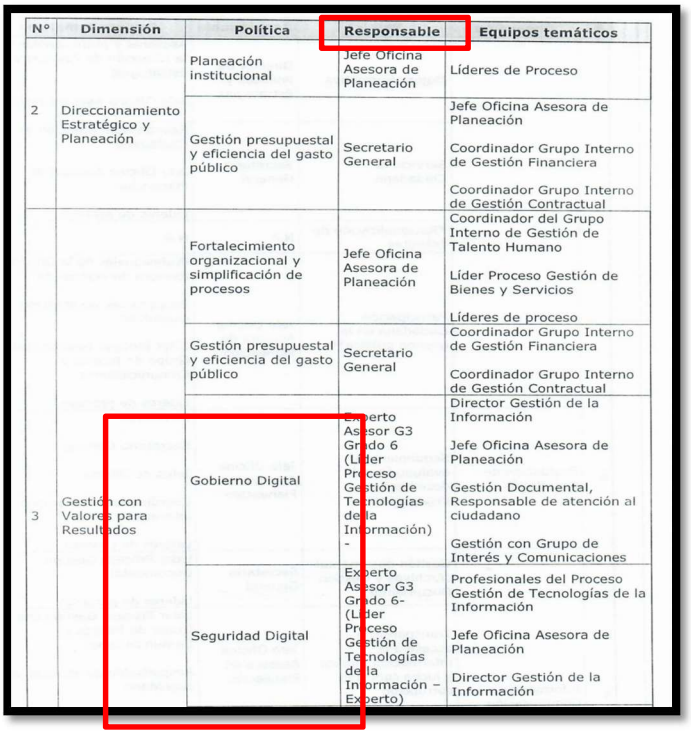
Manual Operativo de MIPG - Manual Operativo de MIPG que cita: "Desde el ejercicio de planeación se deben definir los mecanismos a través de los cuales se hará el seguimiento y evaluación a su cumplimiento (ver 4a Dimensión Evaluación de Resultados). Esto permitirá, verificar el logro de objetivos y metas, así como el alcance de los resultados propuestos e introducir ajustes a los planes de acción. Por ello, es recomendable contar con un grupo de indicadores que permita conocer el estado real de la ejecución de las actividades, el logro de metas, objetivos o resultados y sus efectos en la ciudadanía. Para su construcción es útil: · Tener claro los objetivos, planes, programas y proyectos para identificar los aspectos prioritarios a ser susceptibles de medición. · Determinar puntos o factores críticos de éxito, es decir, aquellas acciones o actividades de cuyo desarrollo depende la consecución de los objetivos. · Establecer qué se debe medir y qué información se quiere obtener de esa medición, para saber qué tipo de indicador se necesita. Establecer la frecuencia adecuada para la medición de los indicadores, para tomar decisiones en el momento justo. (…)

7.3.6 Cumplimiento MIPG

En la Resolución 338 del 24 de septiembre de 2020 se define como Responsable de la Política de Gobierno Digital y de Seguridad Digital al Líder del Proceso Gestión de TI el Manual de Gobierno digital define que el Responsable de estas políticas hará parte del Comité Institucional de Gestión y Desempeño y responderá directamente al representante legal de la entidad. Si bien hace parte del Comité de Gestión y Desempeño no se evidencia la respuesta directa ante la Dirección.

El director, Jefe de Oficina o Coordinador de Tecnologías y Sistemas de la Información y las Comunicaciones, o quien haga sus veces, hará parte del Comité Institucional de Gestión y Desempeño y responderá directamente al representante legal de la entidad, de acuerdo con lo establecido en el artículo 2.2.35.4. del Decreto Único Reglamentario de Función Pública 1083 de 2015. Teniendo en cuenta que el nuevo enfoque de Gobierno Digital es el uso de la tecnología como una herramienta que habilita la gestión de la entidad para la generación de valor público, todas las áreas o dependencias son corresponsables en su implementación.

Grafica N° 6 Resolución 338 de 2020



N°	Dimensión	Política	Responsable	Equipos temáticos
2	Direccionamiento Estratégico y Planeación	Planeación institucional	Jefe Oficina Asesora de Planeación	Líderes de Proceso
		Gestión presupuestal y eficiencia del gasto público	Secretario General	Jefe Oficina Asesora de Planeación Coordinador Grupo Interno de Gestión Financiera Coordinador Grupo Interno de Gestión Contractual
3	Gestión con Valores para Resultados	Fortalecimiento organizacional y simplificación de procesos	Jefe Oficina Asesora de Planeación	Coordinador del Grupo Interno de Gestión de Talento Humano Líder Proceso Gestión de Bienes y Servicios Líderes de proceso
		Gestión presupuestal y eficiencia del gasto público	Secretario General	Coordinador Grupo Interno de Gestión Financiera Coordinador Grupo Interno de Gestión Contractual
		Gobierno Digital	Experto Asesor G3 Grado 6 (Líder Proceso Gestión de Tecnologías de la Información) -	Director Gestión de la Información Jefe Oficina Asesora de Planeación Gestión Documental, Responsable de atención al ciudadano Gestión con Grupo de Interés y Comunicaciones
		Seguridad Digital	Experto Asesor G3 Grado 6- (Líder Proceso Gestión de Tecnologías de la Información – Experto)	Profesionales del Proceso Gestión de Tecnologías de la Información Jefe Oficina Asesora de Planeación Director Gestión de la Información

Fuente: Pagina Web Intranet

7.3.6.1 Política de Gobierno Digital

Grafica N° 7 Estructura Política de Gobierno Digital

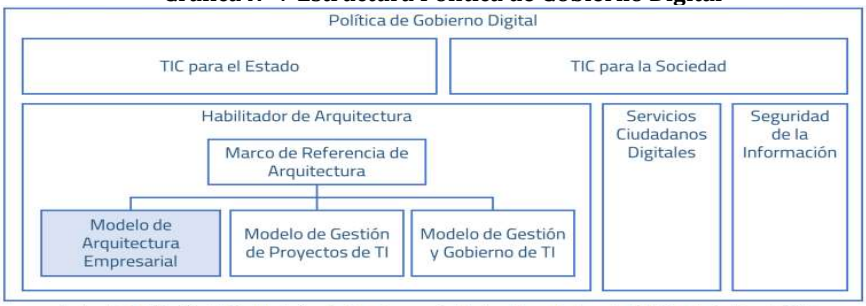


Ilustración 1 Ubicación del Modelo de Arquitectura Empresarial dentro de la estructura de la Política de Gobierno Digital

Fuente: Manual Operativo -MSPI

7.3.6.1.1 Habilitador 1 Arquitectura

7.3.6.1.1. 1Modelo de Arquitectura Empresarial

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)

Grafica N° 8 Modelo de Arquitectura

Ilustración 3 Dominios del Modelo de Arquitectura Empresarial

Fuente: Modelo de Arquitectura Empresarial -MSPI

7.3.6.1.1.2 Modelo de Gestión de Proyectos de TI - Documento Maestro de Gestión de Proyectos de TI (mintic.gov.co)
MGPTI.G.GEN.01 – Documento Maestro del Modelo de Gestión de Proyectos TI - Contratación de proyectos de TI

Grafica N° 9 Modelo de Arquitectura

Ilustración 3 Dominios del Modelo de Gestión y Gobierno de TI

Fuente: Modelo de Arquitectura Empresarial -MSPI

No se evidencia un Plan Estratégico de Tecnología y Sistemas de Información (PETI) que este alineado con el Modelo de Arquitectura Empresarial
Política de Gobierno Digital Habilitador 1 Arquitectura Guia Modelo de Gestión de Proyectos de TI DECRETO 415 DE 2016 ARTÍCULO 2.2.35.3. Objetivos del fortalecimiento institucional (..) deberá. Liderar la gestión estratégica con tecnologías de la información y las comunicaciones mediante la definición, implementación, ejecución, seguimiento y divulgación de un Plan Estratégico de Tecnología y Sistemas de Información (PETI) que esté alineado a la estrategia y modelo integrado de gestión de la entidad y el cual, con un enfoque de generación de valor público, habilite las capacidades y servicios de tecnología necesarios para impulsar las transformaciones en el desarrollo de su sector y la eficiencia y transparencia del Estado.
Debe existir relación entre:
PND - Plan Nacional de Desarrollo
PETI – Plan Estratégico de tecnologías de la Información Metodología alineado al plan estratégico cuatrienal
PETI – Plan Estratégico de tecnologías de la Información Operativo, alineado con el estratégico, vigencia anual
PAA – Plan Anual De Adquisiciones
PAI – Plan De Acción Institucional

7.3.6.1.1.3 **Modelo Óptimo De Gobierno De Información** Documento Maestro del Modelo de Gestión y Gobierno de TI (mintic.gov.co)

Grafica N° 10 Modelo de Gobierno De Información

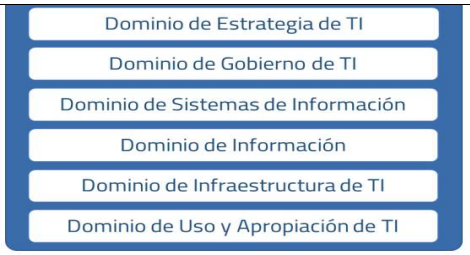


Ilustración 3 Dominios del Modelo de Gestión y Gobierno de TI

Fuente: Modelo de Arquitectura Empresarial -MSPI

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 DE-MO-01 Modelo Óptimo De Gobierno De Información.

Asignación específica de responsabilidades 2.5.2.1 Proceso de Gestión de Tecnologías de la Información: "Proponer el Modelo de Gobierno de Tecnologías de la Información.

MODELO ÓPTIMO DE GOBIERNO DE INFORMACIÓN 2.5.2 Asignaciones específicas de responsabilidad en la Agencia-2.5.2.4 Oficina Asesora de Planeación La Oficina Asesora de Planeación se encarga de la creación y actualización permanente del Modelo de Gobierno de Información - MOGI. Y 2.5.2.6 Proceso de Gestión de Tecnologías de la Información - Proponer el Modelo de Gobierno de Tecnologías de la Información.

Tomando como base el Modelo Óptimo de Gobierno de Información definido en el marco del contrato de consultoría BID N°. 008 de 2014, suscrito entre la Agencia Nacional de Defensa Jurídica del Estado y la firma Ernst & Young, se crea el Modelo Óptimo de Gobierno de Información (ANDJE; 2014, 2016a) ALINEADO CON MINTIC (2016). Arquitectura TI de Colombia. Recuperado en junio de 2016 de http://www.mintic.gov.co/arquitecturati/

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, que asegura los esfuerzos para que los recursos requeridos se encuentren disponibles en el momento adecuado, garantizando la alineación con los objetivos estratégicos y el cumplimiento de la misión de la ANDJE y manteniendo la efectividad y relevancia del Gobierno de Información, antes, durante y después de su implementación.
- Gerencia del programa y proyectos de Gobierno de Información, que se asegura de la implementación de los proyectos transversales para concretar los lineamientos de Gobierno de Información, incorporándolos en la gestión de la ANDJE y en su actuar misional, estratégico y de apoyo.
- Especialistas de Tecnologías de Información, integrando las tecnologías de información como herramientas para facilitar la implementación del Gobierno de Información en la ANDJE.
- Especialistas en gestión de riesgos, para lograr la adecuada identificación y gestión de riesgos relacionados con la información, los cuales deben administrarse para mitigar su efecto a través de los lineamientos de Gobierno de Información.
- Especialistas de las unidades de negocio, incorporando el conocimiento del negocio en los niveles misional, estratégico y de apoyo para identificar los activos de información de mayor valor estratégico según la misión de la ANDJE.
- Especialistas en Seguridad de la Información, para establecer los lineamientos específicos en aseguramiento de la disponibilidad, integridad y confidencialidad de los activos de información y proponer las acciones preventivas y correctivas necesarias para que estas características de la información sean afianzadas para los activos de información de la ANDJE.
- Especialistas en Gestión Documental, para asegurar que los activos de información de carácter documental son administrados correctamente y, a su vez, la especificación e implementación de lineamientos sobre retención, preservación y disposición según estándares, requerimientos legales y necesidades misionales de la ANDJE.
- Especialistas en Gestión de Procesos, para lograr a integración de los procesos de la ANDJE desde el punto de vista del Gobierno de Información y la implementación de los procedimientos o ajustes a los existentes con el

fin de evaluar, dirigir y monitorear en relación con los componentes de modelo óptimo de gobierno de información
- Especialistas en regulaciones, de las que están definidas para la ANDJE, de tal forma que se asegure el cumplimiento de los requerimientos generados con base en dichas regulaciones.

Modelo Óptimo De Gobierno De Información Código: De-Mo-01 2.5 Estructura Organizacional Para El Gobierno De Información 2.5.1Consideraciones generales sobre estructura organizacional

7.3.6.1.2 Habilitador 2 Seguridad y privacidad de la Información se validará todo el MSPI

Se evidencia que en la Agencia no existe 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,

RESPONSABLES DE LA POLÍTICA - Responsable Institucional de la Política de Gobierno Digital: es el *representante* legal de cada sujeto obligado y es el **responsable de coordinar, hacer seguimiento y verificación de la implementación de la Política de Gobierno Digital**. Como responsables de la política de Gobierno Digital, los representantes legales (ministros, directores, gobernadores y alcaldes, entre otros), deben garantizar el desarrollo integral de la política como una herramienta transversal que apoya la gestión de la entidad y el desarrollo de las políticas de gestión y desempeño institucional del Modelo Integrado de Planeación y gestión.

Responsable de liderar la implementación la Política de Gobierno Digital: es el director, jefe de oficina o coordinador de tecnologías y sistemas de la información y las comunicaciones o G-CIO (sigla en inglés de Government Chief Information Officer), o quien haga sus veces en la entidad, de acuerdo con el artículo 2.2.35.5. del Decreto 1083 de 2015. Las demás áreas de la respectiva entidad serán corresponsables de la implementación de la Política de Gobierno Digital en los temas de su competencia.

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

Documentos externos

- Ley 1341 de 2009 numeral 8 del artículo 2, principio de "masificación del gobierno en línea" hoy Gobierno Digital las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de sus funciones.

- Decreto 1078 de 2015 Sector de Tecnologías de la Información y las Comunicaciones -La política de Gobierno Digital establecida mediante el Decreto 1008 de 2018 (cuyas disposiciones se compilan en el Decreto 1078 de 2015, "Decreto Único Reglamentario del sector TIC", específicamente en el capítulo 1, título 9, parte 2, libro 2), forma parte del Modelo Integrado de planeación y Gestión (MIPG) ARTÍCULO 2.2.9.1.3.4. *Responsable de liderar la implementación la Política de Gobierno Digital.* El Director, Jefe de Oficina o Coordinador de Tecnologías y Sistemas de la Información y las Comunicaciones, o quien haga sus veces, de la respectiva entidad, tendrá la responsabilidad de liderar la implementación de la Política de Gobierno Digital. Las demás áreas de la respectiva entidad serán corresponsables de la implementación de la Política de Gobierno Digital en los temas de su competencia.

- Decreto No. 1083 de 2015 ARTÍCULO 1°. Adiciónese el Título 35 a la parte 2 del libro 2, Decreto Único Reglamentario del sector de la Función Pública, en los siguientes términos:, Jefe de Oficina o Coordinador de Tecnologías y Sistemas de la Información y las Comunicaciones, o quien haga sus veces, hará parte del Comité Institucional de Gestión y Desempeño y responderá directamente al representante legal de la entidad, de acuerdo a lo establecido en el artículo 2.2.3.5.4.

- Decreto 415 de 2016 – Titulo 35 ARTÍCULO 2.2.35.4. Nivel Organizacional. Cuando la entidad cuente en su estructura con una dependencia encargada del accionar estratégico de las Tecnologías y Sistemas de la Información y las Comunicaciones, hará parte del comité directivo y dependerán del nominador o representante legal de la misma.

- Modelo de Seguridad y Privacidad de la Información - ANEXO 4 LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PÚBLICAS - Este documento complementa y profundiza lo expuesto en la Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas. "Responsable de Seguridad Digital Cada entidad pública debe designar un responsable de Seguridad Digital que también es el responsable de la Seguridad de la Información, el cual debe pertenecer a un área que haga parte de la Alta Dirección o Línea Estratégica (…)

7.3.6.1.2.1 Políticas de seguridad y Privacidad. Se valida la existencia de los productos relacionados en el Modelo de Seguridad y Privacidad de la Información.

Tabla 4. Productos Modelo de Seguridad y Privacidad de la Información

No.	Producto MSPI-MGRSD	Aprobación y socialización	Guía de Mintic - https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/
1	Política de Riesgos	Director	
2	Informe diagnóstico con recomendaciones	CGD	Instrumento de evaluación-MSTI- Guía No. 1 Pruebas de efectividad
3	Plan de seguridad y privacidad de la información	Director	Alineado con el objetivo misional de la entidad - Enfoque por procesos
4	Socializacion de la Política de Seguridad y Privacidad	Comunicaciones	
5	Política control de acceso	CGD- Comunicaciones	Guía No. 3 Procedimientos de seguridad de la información
6	Política criptografía	CGD- Comunicaciones	Guía No. 3 Procedimientos de seguridad de la información
7	Política seguridad física y del entorno	CGD- Comunicaciones	Guía No. 3 Procedimientos de seguridad de la información
8	Política seguridad de las operaciones	CGD- Comunicaciones	Guía No. 3 Procedimientos de seguridad de la información
9	Política seguridad de las comunicaciones	CGD- Comunicaciones	Guía No. 3 Procedimientos de seguridad de la información
10	Política adquisición, desarrollo y mantenimiento de sistemas de información	CGD- Comunicaciones	Guía No. 3 Procedimientos de seguridad de la información
11	Política relaciones con los proveedores	CGD- Comunicaciones	Guía No. 3 Procedimientos de seguridad de la información
12	Política gestión de incidentes de seguridad de la información	CGD- Comunicaciones	Guía No. 3 Procedimientos de seguridad de la información
13	Lineamientos terminales de áreas financieras de entidades públicas	CGD- Comunicaciones	Guía No. 18 - Lineamientos: Terminales de áreas financieras
14	Seguridad en la nube	CGD- Comunicaciones	Guía No. 12 - Seguridad en la nube
15	Roles y responsabilidades-Resolución Comité de Seguridad de la Información	Director	Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información.
16	Metodología para identificación, clasificación y valoración de activos de información	Director	Guía No 5 - Gestión De Activos - Guía GRSD numeral 4.2.1 Identificación de activos de información
17	Inventario de activos IPV6	CGD	Guía No 20 - Transición Ipv4 a Ipv6
18	Integración del MSPI con el Sistema de Gestión documental	CGD	Guía No 6 - gestión Documental
19	Metodología de gestión de riesgos	Director	Guía No 7 - gestión de Riesgos Guía No 8 - Controles de Seguridad Guía GRSD numeral 4.1.2., 4.1.3., 4.1.5. , 4.1.7., 4.1.8.
20	Plan de comunicación, sensibilización y capacitación para la entidad	Director-asignación de recursos	Guía No 14 - Plan de comunicación, sensibilización y capacitación Guía GRSD numeral 4.4.
21	Plan de diagnóstico para la transición de IPv4 a IPv6	CGD	Estrategias del plan de implementación de IPv6 en la entidad Guía No 19 y 20 - Transición IPv4 a IPv6
22	Informe de la ejecución del plan de tratamiento de riesgos.	CGD	Documento con la declaración de aplicabilidad. Documento con el plan de tratamiento de riesgos. Guía GRSD numeral 4.2.5. Tratamiento de los riesgos de seguridad digital
23	Indicadores de gestión de seguridad y privacidad de la información	CGD	Guía No 9 - Indicadores de Gestión SI.
24	Plan de revisión y seguimiento, a la implementación del MSPI y del MGRSD.	Director	Guía No 16 – Evaluación del desempeño. - Guía GRSD numeral 4.3. Fase 3. Monitoreo y Revisión.
25	Plan de Ejecución de Auditorias.	Director	Guía No 15 – Guía de Auditoría. Guía GRSD numeral 4.3. Fase 3. Monitoreo y Revisión.
26	Informe diagnóstico activos de información	CGD	Metodología para identificación, clasificación y valoración de activos de información
27	Registro de las Bases de datos	CGD	Procedimiento Superintendencia de Industria y Comercio-Herramienta de Diagnóstico. Guía No 7 – gestión de Riesgos

28	Índice de información clasificada, reservada, revisada y sus procedimientos ajustados	CGD	Procedimiento Secretaría de Transparencia de la Presidencia- Ley 1712 de 2014.-Herramienta de Diagnóstico.
29	Informe de la implementación del plan y la estrategia de transición de IPv4 a IPv6	Director	Guía No 20 – Guía Transición de IPv4 a IPv6 para Colombia -Guía No 19 - Guía de Aseguramiento del Protocolo IPv6.
30	Continuidad de negocio	Director - Comunicaciones	Plan de trabajo y documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección. Guía 10 Continuidad de negocio, Guia 11 Impacto de negocio

Fuente: Elaboración propia

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

Decreto 1008 de 2018 ARTíCULO 2.2.9.1.2.2. Manual de Gobierno Digital. 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, el cual será elaborado y publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones, en coordinación con el Departamento Nacional de Planeación.

MANUAL DE GOBIERNO DIGITAL Implementación de la Política de Gobierno Digital - Seguridad de la información: 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. Este habilitador se soporta en el Modelo de Seguridad y Privacidad de la Información -MSPI, que contempla 6 niveles de madurez.

Modelo de Seguridad y Privacidad de la Información -MSPI A nivel metodológico es importante tener presente que el (MSPI) cuenta con una serie de guías anexas que ayudarán a las entidades a cumplir lo solicitado permitiendo abordar de manera detallada cada una de las fases del modelo, buscando a su vez comprender cuáles son los resultados a obtener y como desarrollarlos, incluyendo los nuevos lineamientos que permiten la adopción del protocolo IPv6 en el Estado Colombiano.

7.3.6.3 BCP

No se evidenció 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.

El desarrollo del plan de continuidad de negocio se fundamenta en la necesidad de preservar la disponibilidad continuidad de los servicios que presta la entidad, dentro del **marco de la implementación de la política de gobierno digital y los lineamientos generales en el uso de servicios digitales ciudadanos**. Igualmente, la estrategia de continuidad de negocio institucional está articulado con el modelo integrado de planeación y gestión a través de la 3ª. Dimensión: Gestión con valores para resultados.

Ley 1955 de 2018, por el cual se expide el Plan Nacional de Desarrollo 2018 -2022. "Pacto por Colombia, Pacto por la Equidad".
Artículo 147. Transformación Digital Pública. Las entidades estatales del orden nacional deberán (…) 2. **Aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales**. 11. Inclusión y actualización permanente de políticas de seguridad y confianza digital.

Decreto 1078 de 2015. por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. (…) ARTÍCULO 2.2.17.5.6. Seguridad de la información y Seguridad Digital. **Los actores que traten información en el marco del presente título deberán contar con una estrategia de seguridad y privacidad de la información, seguridad digital y continuidad de la prestación del servicio. en la cual, deberán hacer periódicamente una evaluación del riesgo de seguridad digital.** (…) Modelo Integrado de planeación y gestión, 3ª. Dimensión: Gestión con valores para resultados.

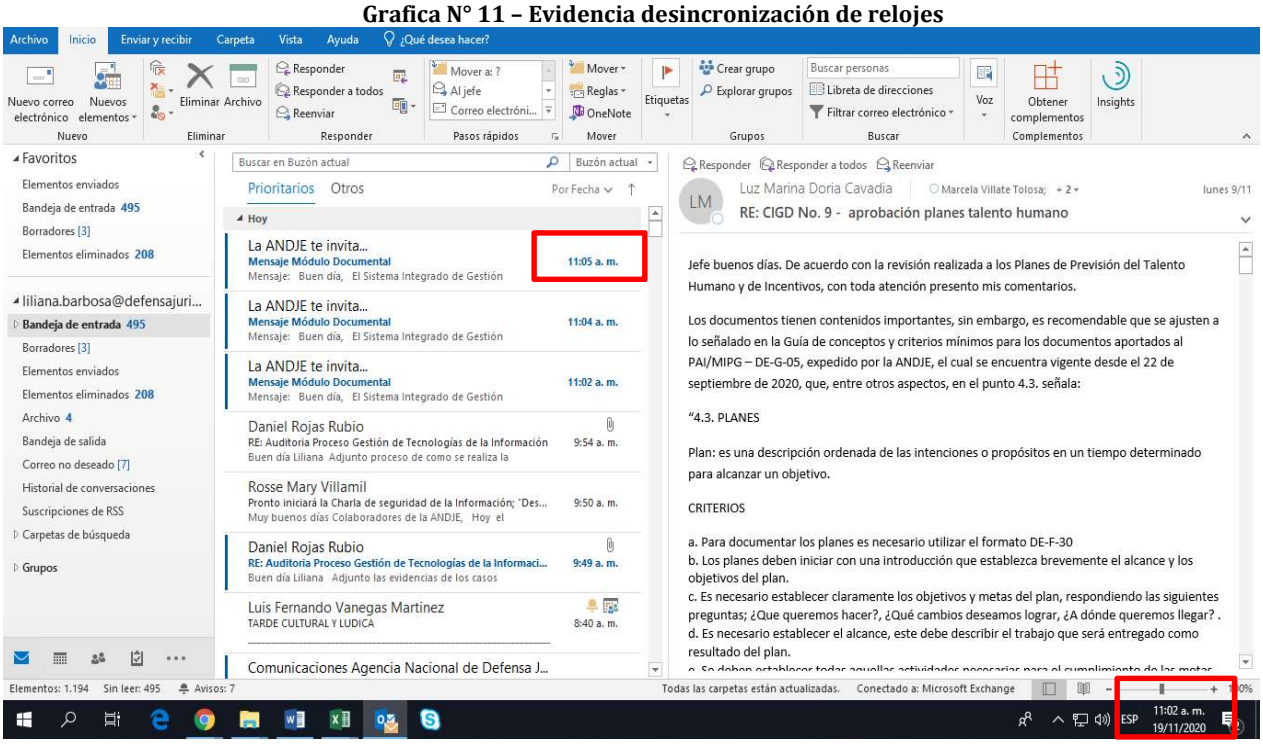
3.2.1.4 Política de Seguridad Digital

En materia de Seguridad Digital, el Documento CONPES 3854 de 2016 incorpora la Política Nacional de Seguridad Digital coordinada por la Presidencia de la República, para orientar y dar los lineamientos respectivos a las entidades. Con la política se fortalecen las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, ***así como en la creación e implementación de instrumentos de resiliencia, recuperación y respuesta nacional en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital*** *nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país.*

7.3.6.4 Política seguridad de las operaciones

Se evidencia un desincronización de 3 minutos en los relojes de lo s sistemas de la Agencia desatendiendo la Política seguridad de las operaciones Modelo de Seguridad y Privacidad de la Información Guía No. 8 - Controles de Seguridad y Privacidad de la Información https://www.mintic.gov.co/gestionti/615/articles-482_G8_Controles_Seguridad.pdf A.12 Seguridad de las operaciones: A.12.4.4 sincronización de relojes Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo. TI debe sincronizar los relojes de los servidores con una única fuente de referencia de tiempo (http://horalegal.inm.gov.co/), con el fin de garantizar la exactitud de los registros de auditoría.

Grafica N° 11 – Evidencia desincronización de relojes



Fuente: Intranet - Correo institucional

La desincronización de relojes se corrige en el desarrollo de la auditoria. Se recomienda implementar un control para evitar se vuelva a presentar.

Habilitador 3 Servicios ciudadanos digitales

Por lo cual, el articulador señalado en el numeral 3 del artículo 2.2.17.1.5. del Decreto 1078 de 2015, deberá cumplir las condiciones y estándares establecidos en la Guía de lineamientos de los servicios ciudadanos digitales que se encuentran señaladas, con el fin de garantizar la correcta prestación de los servicios ofertados, y, las autoridades señaladas en el artículo 2.2.17.1.2. del Decreto 1078 de 2015, deberán cumplir las condiciones y estándares establecidos en la Guía para vinculación y uso de los servicios ciudadanos digitales que se encuentran señaladas para la preparación, adecuación, integración, uso y apropiación de los servicios ciudadanos digitales, a través de los cuales podrán integrar a sus sistemas de información los mecanismos de autenticación digital, interoperabilidad,

carpeta ciudadana digital y vincularlos al Portal Único del Estado colombiano.

Guía de integración de los prestadores de servicio a los Servicios Ciudadanos Digitales, que expida el Ministerio de Tecnologías de la Información y las Comunicaciones. articles-152267_recurso_4.pdf (mintic.gov.co)

a. Servicio de Interoperabilidad Microsoft Word - Marco de interoperabilidad - Agosto2019.docx (mintic.gov.co)

b. Autenticación Digital Servicio de autenticación digital: Es el procedimiento que, utilizando mecanismos de autenticación, permite verificar los atributos digitales de una persona cuando adelanten trámites y servicios a través de medios digitales. Además, en caso de requerirse, permite tener certeza sobre la persona que ha firmado un mensaje de datos, o la persona a la que se atribuya el mismo en los términos de la Ley 527 de 1999 y sus normas reglamentarias, o las normas que la modifiquen, deroguen o subroguen, y sin perjuicio de la autenticación notarial.

c. Carpeta Ciudadana Digital Es el servicio que le permite a los usuarios de servicios ciudadanos digitales acceder digitalmente de manera segura, confiable y actualizada al conjunto de sus datos, que tienen o custodian las entidades señaladas en el artículo 2.2.17.1.2 del Decreto 1078 de 2015. Adicionalmente, este servicio podrá entregar las comunicaciones o alertas que las entidades señaladas tienen para los usuarios, previa autorización de estos.

7.3.6.2 Política de Seguridad Digital

Modelo Nacional de Gestión de Riesgos de Seguridad Digital Modelo de Gestión de Riesgos de Seguridad Digital - MinTIC www.mintic.gov.co › portal › articles-61854_documento (google.com)

Grafica N° 11 Fases Política de Seguridad Digital

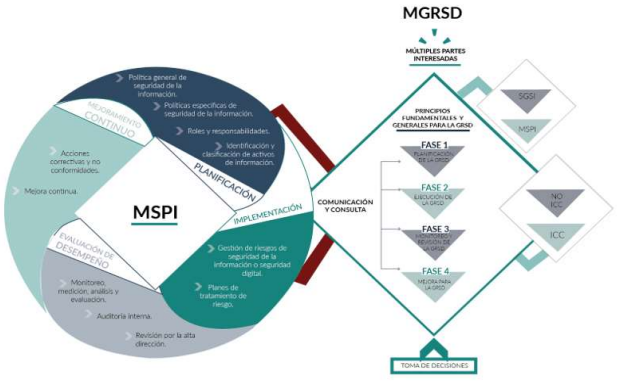


Imagen 3. Interacción entre el MSPI y el MGRSD. Fuente: MinTIC.

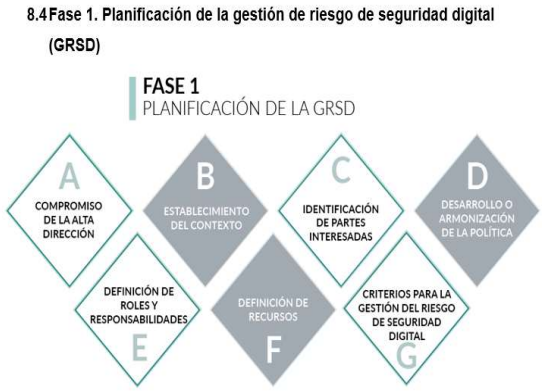


Imagen 6. Descripción de la fase 1. Planificación de la GRSD. Fuente: elaborado por el autor.

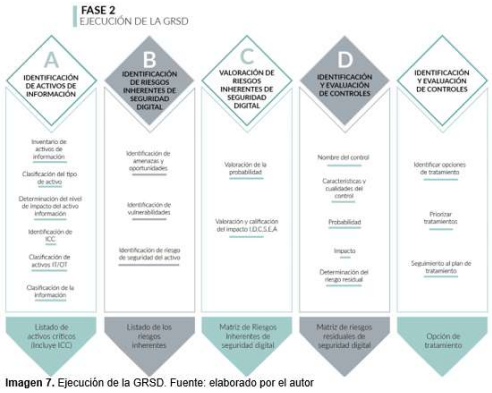


Imagen 7. Ejecución de la GRSD. Fuente: elaborado por el autor

Imagen 8. Descripción de la fase 3. Monitoreo y revisión de la GRSD. Fuente: elaborado por autor

Fuente: Modelo Nacional de Gestión de Riesgos de Seguridad Digital

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

Política de Seguridad Digita. Decreto 1078 de 2015. por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. (…) ARTÍCULO 2.2.17.5.6. Seguridad de la información y Seguridad Digital. Los actores que traten información en el marco del presente título deberán contar con una estrategia de seguridad y privacidad de la información, seguridad digital y continuidad de la prestación del servicio. en la cual, deberán hacer periódicamente una evaluación del riesgo de seguridad digital. (…) Modelo Integrado de planeación y gestión, 3ª. Dimensión: Gestión con valores para resultados.

3.**2.1.4 Política de Seguridad Digital** En materia de Seguridad Digital, el Documento CONPES 3854 de 2016 incorpora la Política Nacional de Seguridad Digital coordinada por la Presidencia de la República, para orientar y dar los lineamientos respectivos a las entidades. Con la política se fortalecen las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, así como en la creación e implementación de instrumentos de resiliencia, recuperación y respuesta nacional en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país

Modelo Nacional de Gestión de Riesgos de Seguridad Digital - MinTIC www.mintic.gov.co › portal › articles-61854_documento (google.com) Modelo de Gestión de Riesgos de Seguridad Digital - MinTIC www.mintic.gov.co › portal › articles-61854_documento (google.com)

7.3.7 Seguimiento Contractual (Asociado al EKOGUI)

Se hace la validación y se recomienda incluir lo correspondiente a compras de operación en el PETI

G.E.S.06 Guía para la Construcción del PETI – Planeación de la Tecnología para a Transformación Digital - julio de 2019

Grafica N° 12 Requisitos en la Construcción del PETI

9 sesiones de la fase 3		
Cuarta fase: Presentar	Sesión 20: Definir el seguimiento y control del PETI	Definir el tablero de indicadores para medir el avance en la estrategia de TI.
	Sesión 21: Aprobar y publicar el PETI	Aprobar el PETI por el grupo institucional de gestión y desempeño y la alta dirección de la entidad.
	Sesión 22: Presentar el PETI	Presentar el PETI a los interesados.
	Sesión 23: Validar equivalencias y relación de evidencias	Revisar las equivalencias del PETI con otros modelos de medición.
4 sesiones de la fase 4		

Tabla 7 Modelo operativo

Modelo Operativo									
Capacidades				Modelo Operativo					
Capacidades		Subcapacidades		Proceso o Procedimiento		Recursos		Roles	
ID	Nombre	ID	Nombre	ID	Nombre	ID	Nombre	ID	Nombre
C01	Ej. Gestionar la estrategia institucional	C01.01	Ej. Definir la estrategia institucional	PR001	Ej. Definición de la estrategia institucional	RE001	Ej. Herramienta de seguimiento estratégico	RO001	Ej. Líder estratégico
		C01.02	Ej. Gestionar el plan de acción institucional		Ej. No hay definido un procedimiento	RE016	Ej. Plan de acción institucional		
		C01.03	Ej. Gestionar la arquitectura empresarial	PR002	Ej. Ejecución de ejercicios de arquitectura empresarial	RE002	Ej. Herramienta de Arquitectura empresarial	RO002	Ej. Arquitecto Empresarial
						RE003	Ej. Repositorio de arquitectura empresarial		
C02	Ej. Gestionar las comunicaciones	C02.01	Ej. Definir el plan de comunicaciones		Ej. No hay definido un procedimiento				
		C02.02	Ej. Gestionar los comunicados externos	PR004	Ej. Gestión de comunicaciones externas				
		C02.03	Ej. Gestionar los comunicados internos		Ej. No hay definido un procedimiento				

5 Identificar las áreas involucradas en cada uno de los gastos. Ej. Conectividad es para todas las áreas y el licenciamiento de las licencias del software x es para una sola área.

Fuente: G.E.S.06 Guía para la Construcción del PETI

Requisitos de arquitectura para que se tenga responsabilidad de TI en la contratación ver los comentarios del riesgo de Gestión Adquisición, arrendamiento y/o construcción de soluciones informáticas que no se encuentran alineadas con los objetivos estratégicos de la Entidad

DECRETO 415 DE 2016 "Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones." ARTÍCULO 2.2.35.3. Objetivos del fortalecimiento institucional. Para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones las entidades y organismos a que se refiere el presente decreto, deberán:
Liderar la gestión estratégica con tecnologías de la información y las comunicaciones mediante la definición, implementación, ejecución, seguimiento y divulgación de un Plan Estratégico de Tecnología y Sistemas de Información (PETI) que esté alineado a la estrategia y modelo integrado de gestión de la entidad y el cual, con un enfoque de generación de valor público, habilite las capacidades y servicios de tecnología necesarios para impulsar las transformaciones en el desarrollo de su sector y la eficiencia y transparencia del Estado. Política de Gobierno Digital Habilitador 1 Arquitectura Guia Modelo de Gestión de Proyectos de TI .

7.3.8 Gestión de TI

Se realiza verificación de las medidas tomadas por la contingencia del Covid 19

A través del Decreto No. 491 del 28 de marzo de 2020, el Gobierno Nacional adoptó medidas de urgencia para garantizar la atención y prestación de los servicios por parte de las autoridades públicas, estableciendo en su artículo 11 lo siguiente: "(...) De las firmas de los actos, providencias y decisiones. Durante el período de aislamiento preventivo obligatorio las autoridades a que se refiere el artículo 1 del presente Decreto, cuando no cuenten con firma digital, podrán válidamente suscribir los actos, providencias y decisiones que adopten mediante firma autógrafa mecánica, digitalizadas o escaneadas, según la disponibilidad de dichos medios. Cada autoridad será responsable de adoptar las medidas internas necesarias para garantizar la seguridad de los documentos que se firmen por este medio".

Se revisa documentación enviada por el Proceso y se evidencia gestión en temas de sensibilización en cuanto a Seguridad con la campaña "lunes seguro", en lo correspondiente al Decreto 491 de 2020 nos informan que es responsabilidad del Proceso de Gestión Documental, por lo cual se recomienda hacer un trabajo en conjunto "*para garantizar la seguridad de los documentos que se firmen por este medio".* Lo anterior teniendo en cuenta que el Líder de TI es responsable de Seguridad y Privacidad de la Información, en todos los sistemas de información de la Agencia

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

Para la elaboración del informe final se tienen en cuenta los comentarios y observaciones brindadas por los diferentes responsables en las mesas de trabajo realizadas con cada uno de ellos durante el 16 y 17 de diciembre de 2020.

REQUISITO	NO CONFORMIDAD	OBSERVACIONES
GTI - P 01 Solicitud De Servicios de TI paso 4. Gestionar la Solicitud de Servicio de TI y Política de Operación Detalle numeral **7.3.1.1 GTI-P-01**	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 *Esta no conformidad es de responsabilidad compartida entre el Proceso Gestión de TI, Talento Humano y/o Supervisores de los contratos.*	
POLITICA DE SEGURIDAD DIGITAL El objetivo general del Documento CONPES 3701 fue fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra la defensa y seguridad nacional en el ámbito cibernético (ciberseguridad y ciberdefensa)10, creando un ambiente y unas condiciones para brindar protección en el ciberespacio. Para cumplir este objetivo general, se	En el Procedimiento Gestión de incidentes no se evidencia la inclusión de niveles de escalamiento para un manejo Post-incidente.	

formularon tres objetivos específicos: (i) implementar instancias apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias cibernéticas para afrontar las amenazas y los riesgos que atentan contra la ciberseguridad y ciberdefensa nacional ; Guía No. 21 Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información - MSPI		
Guía administración de riesgos ANDJE seguimiento. Los líderes de los procesos en conjunto con sus equipos deben monitorear y revisar mensualmente el Mapa de Riesgos incluidos los de Corrupción y si es del caso ajustarlo. (…)		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.
DECRETO 415 DE 2016 A RTÍCULO 2.2.35.3. Objetivos del fortalecimiento institucional. Para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones las entidades y organismos a que se refiere el presente decreto, deberán: 1. Liderar la gestión estratégica con tecnologías de la información y las comunicaciones mediante la definición, implementación, ejecución, seguimiento y divulgación de un Plan Estratégico de Tecnología y Sistemas de Información (PETI) que esté alineado a la estrategia y modelo integrado de gestión de la entidad **y el cual, con un enfoque de generación de valor público, habilite las capacidades y servicios de tecnología necesarios para impulsar las transformaciones en el desarrollo de su sector y la**	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.	

eficiencia y transparencia del Estado		
GUÍA ADMINISTRACIÓN DE RIESGOS ANDJE - Seguridad Digital 13.5.4 Responsabilidades ACEPTACIÓN DE LOS RIESGOS Y RIESGOS RESIDUALES. El líder del proceso (dueño del riesgo) será el responsable de aceptar o rechazar los riesgos y riesgos residuales, posteriormente el responsable del Sistema de Gestión de Seguridad de la Información con el apoyo del profesional del SGSI deben presentar los riesgos y riesgos residuales al comité institucional de desarrollo administrativo CIDA también para su aprobación o rechazo.	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	
POLÍTICA NACIONAL DE SEGURIDAD DIGITAL - Guía No. 5 - Guía para la Gestión y Clasificación de Activos de Información		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,
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 institucionales, según corresponda. La formulación de planes de mejoramiento, su aplicación y seguimiento para resolver los hallazgos presentados.	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 refor 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 establecidas. mular el plan de mejoramiento, incluyendo las acciones necesarias para cumplir con la Política de Gobierno Digital y de Seguridad Digital	

Manual Operativo de MIPG - Manual Operativo de MIPG que cita: "Desde el ejercicio de planeación se deben definir los mecanismos a través de los cuales se hará el seguimiento y evaluación a su cumplimiento (ver 4a Dimensión Evaluación de Resultados). Esto permitirá, verificar el logro de objetivos y metas, así como el alcance de los resultados propuestos e introducir ajustes a los planes de acción. Por ello, es recomendable contar con un grupo de indicadores que permita conocer el estado real de la ejecución de las actividades, el logro de metas, objetivos o resultados y sus efectos en la ciudadanía. Para su construcción es útil: · Tener claro los objetivos, planes, programas y proyectos para identificar los aspectos prioritarios a ser susceptibles de medición. · Determinar puntos o factores críticos de éxito, es decir, aquellas acciones o actividades de cuyo desarrollo depende la consecución de los objetivos. · Establecer qué se debe medir y qué información se quiere obtener de esa medición, para saber qué tipo de indicador se necesita. Establecer la frecuencia adecuada para la medición de los indicadores, para tomar decisiones en el momento justo. (…)		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 establecidas. *Esta observación es de responsabilidad compartida entre el Proceso Gestión de TI, y el Proceso Control de la Gestión*
Manual Operativo de MIPG la Ley 152 de 1994, y en el artículo 74 de la Ley 1474 de 2011, en el que se establece que debe especificar en él: · los objetivos, · las estrategias, · los proyectos, · las metas, · los responsables, · los planes generales de	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.	

compras y · la distribución presupuestal de sus proyectos de inversión; así mismo, deber incluir tanto los aspectos relacionados con el componente misional como con los relacionados con los planes de que trata el Decreto 612 de 2018. (…) Debe incluirse además en el Plan de Acción, las acciones y estrategias a través de las cuales las entidades facilitarán y promoverán la participación de las personas en los asuntos de su competencia, en los términos señalados en el artículo 2 de la Ley 1757 de 2015 Guía De Conceptos Y Criterios Mínimos Para Los Documentos Aportados Al PAI/MIPG DE - G-05		
Modelo de Seguridad y Privacidad de la Información - Plan de transición de IPv4 a IPv6Guía de Transición de IPv4 a IPv6 para Colombia - 7. FASES DE TRANSICIÓN	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 Detalle en 7.3.5.2	
Política de Gobierno Digital Habilitador 1 Arquitectura Guia Modelo de Arquitectura Empresarial	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)	
Política de Gobierno Digital Habilitador 1 Arquitectura Guía **Modelo de Gestión de Proyectos de TI** DECRETO 415 DE 2016 ARTÍCULO 2.2.35.3. Objetivos del fortalecimiento institucional (..) deberá. Liderar la gestión estratégica con tecnologías de la información y las comunicaciones **mediante la definición,**	No se evidencia un Plan Estratégico de Tecnología y Sistemas de Información (PETI) que este alineado con el Modelo de Arquitectura Empresarial	

implementación, ejecución, seguimiento y divulgación de un Plan Estratégico de Tecnología y Sistemas de Información (PETI) que esté alineado a la estrategia y modelo integrado de gestión de la entidad y el cual, con un enfoque de generación de valor público, habilite las capacidades y servicios de tecnología necesarios para impulsar las transformaciones en el desarrollo de su sector y la eficiencia y transparencia del Estado. Política de Gobierno Digital Habilitador 1 Arquitectura Guía Modelo de Gestión de Proyectos de TI		
Habilitador 1 Modelo de gestión y gobierno de TI MGGTI.LI.ES.03 Código: DE-MO-01 Modelo Óptimo De Gobierno De Información Asignación específica de responsabilidades 2.5.2.1 Proceso de Gestión de Tecnologías de la Información: "Proponer el Modelo de Gobierno de Tecnologías de la Información.	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. *Esta No conformidad es de responsabilidad del Proceso Gestión de Tecnologías de información y del Proceso Direccionamiento Estratégico*	
Modelo Óptimo De Gobierno De Información Código: De-Mo-01 2.5 Estructura Organizacional Para El Gobierno De Información 2.5.1Consideraciones generales sobre estructura organizacional	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 *Esta No Conformidad es de responsabilidad compartida entre el Proceso Gestión de TI, y el Proceso de Direccionamiento estratégicos*	
Decreto 1008 de 2018 Decreto No. 1083 de 2015 ARTÍCULO 1°. Decreto 415 de 2016 – Titulo 35 ARTÍCULO 2.2.35.4. Decreto 415 de 2016 – Titulo 35 ARTÍCULO 2.2.35.4. Nivel Organizacional. Cuando la entidad cuente en su estructura con una dependencia encargada del accionar estratégico de las Tecnologías y Sistemas de la Información y las Comunicaciones, hará parte del comité directivo y dependerán del nominador o representante legal de la misma. Nivel Organizacional. Política de Gobierno Digital Habilitador 2 Seguridad y Privacidad	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, *Esta No Conformidad es de responsabilidad compartida entre el Proceso Gestión de TI, y el Proceso de Direccionamiento estratégicos*	
Decreto 1078 de 2015 cita: Artículo 2.2.9.1.2.1. Estructura. La Política de Gobierno Digital será definida por (…) Propósitos de la Política de Gobierno Digital: Son los fines de la Política de Gobierno Digital, que se obtendrán a partir del desarrollo de los componentes y los habilitadores transversales, estos son: 4.1. Habilitar y mejorar la provisión de servicios digitales de confianza y calidad. 4.2.	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	

Lograr procesos internos, seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información. 4.3. Tomar decisiones basadas en datos a partir del aumento, el uso y aprovecha-miento de la información. 4.4. Empoderar a los ciudadanos a través de la consolidación de un Estado Abierto. 4.5. Impulsar el desarrollo de territorios y ciudades inteligentes para la solución de retos y problemáticas sociales a través del aprovechamiento de las TIC. Política de Gobierno Digital Habilitador 1 Arquitectura SIS.01 Guía del dominio de Sistemas de Información. https://www.mintic.gov.co/arquitecturati/630/articles-9262_recurso_pdf.pdf Pag 48. 2.6.1 Metodología de referencia para desarrollo de sistemas de información	de desarrollo de sistemas de Información. *Esta No Conformidad es de responsabilidad compartida entre el Proceso Gestión de TI, y el Proceso de Direccionamiento estratégicos*	
Política de Gobierno Digital Habilitador 2 Seguridad y Privacidad - Decreto 1008 de 2018 Artículo 2.2.9.1.2.2. Manual de Gobierno Digital. Para la implementación de la Política de Gobierno Digital,		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.
POLITICA DE SEGURIDAD DIGITAL: Preparación y continuidad: con el fin de reducir los efectos adversos de los incidentes de seguridad, y apoyar la continuidad y la capacidad de recuperación de las actividades económicas y sociales, deben adoptarse preparaciones y planes de continuidad. (…) Privacidad Guia 10 y 11 6.1.3. MGGTI.LI.ES.03 - Políticas de TI La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe identificar y definir las políticas y	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.	

estándares que faciliten la gestión y la gobernabilidad de TI, contemplando por lo menos los siguientes temas: seguridad, **continuidad del negocio**, (…). Política de Gobierno Digital Habilitador 2 Seguridad		
Política de Gobierno Digital Habilitador 3 Servicios Ciudadanos digitales - 2.2.17.1.5. del Decreto 1078 de 2015, deberá cumplir las condiciones y estándares establecidos en la Guía de lineamientos de los servicios ciudadanos digitales (…)l artículo 2.2.17.1.2. del Decreto 1078 de 2015, deberán cumplir las condiciones y estándares establecidos en la Guía para vinculación y uso de los servicios ciudadanos digitales que se encuentran señaladas (…) los mecanismos de autenticación digital, interoperabilidad, carpeta ciudadana digital y vincularlos al Portal Único del Estado colombiano.	Habilitador 3 No se evidencia un documento de diagnóstico y plan del **Marco de interoperabilidad**, que cumpla con lo estipulado en **- Marco de interoperabilidad - Agosto2019.docx (mintic.gov.co)**	
Política de Seguridad Digital Decreto 1078 de 2015. por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. (…) ARTÍCULO 2.2.17.5.6. Seguridad de la información y Seguridad Digital. Detalle en Numeral 7.3.6.2	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	

9. RECOMENDACIONES:

La Oficina de Control Interno en el marco de la auditoria recomienda:

- Actualizar el Normograma relacionado con el Proceso incluyendo la normatividad generada en relación con la Política de Gobierno digital y la Política de Seguridad Digital
  Rta. GTI (Esta actualización se hace de manera periódica y en conjunto con la Oficina Asesora Planeación, esta actividad ya se hizo para la vigencia 2020. Por lo anterior esta recomendación sobra)

Rta OCI El Procedimiento Código: Identificación Y Verificación De Requisitos Legales MC-P-07 "Los líderes de proceso realizaran la identificación de manera mensual para asegurar la actualización de la normatividad de su proceso" Ultima actualización e, 2029 de 2020 no hay registro

- Incluir el Diagrama de flujo del procedimiento en el documento publicado en el SGSI

  Rta. GTI (A qué proceso se refiere)
  Rta OCI Código: GTI-P-01 SOLICITUD DE SERVICIOS DE TI

- Crear un Indicador de atención de gestión de cambios que mida cuantos tienen calificación de emergencia, estándar y normal. (Más que un indicador se hará una categorización para poder sacar reportes)

- Crear un indicador de cumplimiento de ANS para la atención de solicitudes de TI.

  Rta. GTI (Ya se cuenta con el indicador 01-GTI-20 Atención de solicitudes de servicios TIC, Fórmula: (N° de Solicitudes atendidas/ Total solicitudes recibidas - N° Casos especiales) *100 Medir el porcentaje de solicitudes TIC atendidas en el período establecido. Por lo anterior esta recomendación sobra)
  Rta. OCI El indicador contiene todas las solicitudes, no puedo saber cuáles de ellas fueron de emergencia, estándar o normal

- Se recomienda evaluar si es pertinente eliminar el procedimiento GTI-P-04, dado que es una actividad más dentro de las opciones de la mesa de servicio, e integrarlo en el GTI-P-01 Procedimiento Para Solicitud De Servicios De TI (Se revisará)

- Se recomienda agregar un criterio de calidad a los indicadores. Por ejemplo, para medir el servicio en atención de solicitudes, puede ser % atendido por debajo del ANS y para incidentes de seguridad se puede orientar a otros factores como capacitación, canales, pruebas de vulnerabilidad. (Se revisará)

- Se recomienda alinear el indicador al objetivo de grado de cumplimiento frente a la Guía para el uso y aprovechamiento de Datos Abiertos en Colombia con la guía de Datos Abiertos de Colombia.pdf. (Se revisará)

- Se recomienda que la Adquisición, arrendamiento y/o construcción de soluciones informáticas se encuentran alineadas con los objetivos estratégicos de la Entidad.

  Rta. GTI (Esto siempre se ha tenido presente en el PAI y PAA, por lo anterior esta recomendación sobra).

  Rta. OCI no se evidencio la alineación con los objetivos estratégicos, no hay documentación es una de las funcionalidades del PETI

- Se recomienda incluir lo correspondiente a compras de operación en PETI (Se revisará con la consultoría EVERIS)

- Se recomienda implementar un control para evitar la desincronización de relojes

  Rta. GTI (Ya se realizó)
  Rta. OCI Se realizo la sincronización por observación realizada durante la auditoria, la recomendación va orientada a implementar el control

- Se recomienda actualizar el nombre del Comité en el documento Guía Administración De Riesgos - 13.5.4 Responsabilidades (…) el responsable del Sistema de Gestión de Seguridad de la Información con el apoyo del profesional del SGSI deben presentar los riesgos y riesgos residuales al comité institucional de desarrollo administrativo CIDA también para su aprobación o rechazo. (Se realizará)

- Se recomienda hacer un trabajo en conjunto con el Proceso Gestión documental "para garantizar la seguridad de los documentos que se firmen por este medio (Firma digital)". Lo anterior teniendo en cuenta que el Líder

de TI es responsable de Seguridad y Privacidad de la Información en todos los sistemas de información de la Agencia. (Se revisará)

- Se recomienda asignar la responsabilidad de liderar las políticas de gobierno digital y de seguridad digital a un rol de nivel directivo.

Firma Auditor Designado y Equipo Auditor	Firma Jefe de Control Interno ANDJE
Informe realizado Electrónicamente por: Liliana Barbosa Carrillo **Gestora Oficina de Control Interno** No. Radicado: 20201020015383	**Informe Firmado Electrónicamente por:** Luis Eberto Hernández León **Jefe Oficina de Control Interno** No. Radicado: 20201020015383