RESOLUCIÓN 95 DE 2018

(febrero)

<Fuente: Archivo interno entidad emisora>

<Esta norma no incluye análisis de vigencia>

AGENCIA NACIONAL DE DEFENSA JURIDICA DEL ESTADO

Por la cual se adopta el Nuevo Sistema Integrado de Gestión Institucional SIGI - en la Agencia Nacional de Defensa Jurídica del Estado y se dictan otras disposiciones

EL DIRECTOR GENERAL

En ejercicio de sus facultades legales, y en especial las conferidas por el artículo 6o de la Ley 87 de 1993, y en los numerales 3, 17 y 21 del artículo 11o del Decreto Ley 4085 de 2011 y demás normas concordantes y,

CONSIDERANDO:

Que en aplicación de los principios constitucionales de la función administrativa consagrados en el artículo 209 de la Constitución Política, (...) Las autoridades administrativas deben coordinar sus actuaciones para el adecuado cumplimiento de los fines del Estado. La administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley."

Que el artículo 269 de la Constitución Política establece que: "En las entidades públicas, las autoridades correspondientes están obligadas a diseñar y aplicar según la naturaleza de sus funciones; métodos y procedimientos de Control Interno, de conformidad con lo que disponga la ley (...)".

Que el artículo 133 de la Ley 1753 del 9 de junio de 2015, "Por la cual se expide el Plan Nacional de Desarrollo 2014 – 2018 "Todos por un nuevo país", dispuso la integración en un solo Sistema de Gestión, de los Sistemas de Gestión de la Calidad de qué trata la Ley 872 de 2003 y de Desarrollo Administrativo de que trata la Ley 489 de 1998; así mismo señaló que el Sistema de Gestión deberá articularse con los Sistemas Nacional e Institucional de Control Interno consagrado en la Ley 87 de 1993 y en los artículos 27 al 29 de la Ley 489 de 1998. Finalmente, dicha disposición estableció, que una vez el Gobierno Nacional reglamente y entre en aplicación el nuevo Modelo de Gestión, los artículos 15 al 23 de la Ley 489 de 1998 y la Ley 872 de 2003 perderían vigencia.

Que el Gobierno Nacional expidió el Decreto 1499 del 11 de septiembre de 2017, "Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015" y en su artículo 1o sustituyó el Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015.

Que dentro del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015 sustituido mediante Decreto 1499 de 2017, se encuentra el artículo 2.2.22.1.1. que estableció que el Sistema de Gestión "que integra los Sistemas de Desarrollo Administrativo y de Gestión de la Calidad, es el conjunto de entidades y organismos del Estado, políticas, normas, recursos e información, cuyo

objeto es dirigir la gestión pública al mejor desempeño institucional y a la consecución de resultados para la satisfacción de las necesidades y el goce efectivo de los derechos de los ciudadanos, en el marco de la legalidad y la integridad"; así mismo el artículo 2.2.22.1.5., señaló que: "El Sistema de Gestión se complementa y articula, entre otros, con los Sistemas Nacional de Servicio al Ciudadano, de Gestión de la Seguridad y Salud en el Trabajo de Gestión Ambiental y de Seguridad de la Información", los cuales cuentan' respectivamente, con normatividad que los regula y reglamenta.

Que, así mismo, dentro de Titulo 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015 sustituido mediante Decreto 1499 de 2017, en el artículo 2.2.22.3.1. se adopta la versión actualizada del Modelo Integrado de Planeación y Gestión - MIPG-, y en el artículo 2.2.22.3.4. se establece que éste se adoptará por los organismos y entidades de los órdenes nacional y territorial de la Rama Ejecutiva del Poder Público y su implementación y operación estará a cargo del Comité Institucional de Gestión y Desempeño que sustituye los demás comités que tengan relación con el Modelo y que no sean obligatorios por mandato legal, tal como lo dispone el artículo 2.2.22.3.8.

Que el Decreto 1499 de 2017, en su artículo 2o sustituyó el Título 23 de la Parte 2 del Libro 2 del Decreto 1083 de 2015 y en el artículo 2.2.23.1., señaló que en el marco del Modelo Integrado de Planeación y Gestión - MIPG, el Sistema de Control Interno previsto en la Ley 87 de 1993 y en la Ley 489 de 1998 se articula al Sistema de Gestión, "(...) a través de los mecanismos de control y verificación que permiten el cumplimiento de los objetivos y el logro de resultados de las entidades (...)" y que se implementa a través del Modelo Estándar de Control Interno -MECI-. En consonancia, el artículo 2.2.21.1.5. del Decreto 648 de 2017 establece que las entidades que hacen parte del ámbito de aplicación de la Ley 87 de 1993, deberán establecer un Comité Institucional de Coordinación de Control Interno como órgano asesor e instancia decisoria en los asuntos del control interno.

Que como consecuencia de lo anteriormente expuesto, la Agencia Nacional de Defensa Jurídica del Estado considera necesario tener en cuenta los desarrollos normativos expuestos, tomando como punto de partida los avances logrados en materia de gestión y desempeño de la Entidad, y así adoptar un Nuevo Sistema Integrado de Gestión Institucional -SIGI- articulado con el Sistema de Control Interno, el cual estará compuesto por los Subsistemas de Gestión de Calidad - SGC-, Gestión de la Seguridad y Salud en el Trabajo - SG-SST y Gestión de Seguridad y Privacidad de la información - SGSPI.

Que así mismo, se adopta para la Agencia el nuevo Modelo Integrado de Planeación y Gestión - MIPG-, las Políticas de Gestión y Desempeño Institucional, así como las políticas de los Subsistemas citados, contenidos en el Manual de Políticas de Gestión y Desempeño Institucional de la Agencia (DE-M-02) que las complementan y que sirven de marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión en la Entidad.

Que en virtud de lo expuesto,

RESUELVE:

TITULO I.

EL NUEVO SISTEMA INTEGRADO DE GESTIÓN INSTITUCIONAL.

ARTÍCULO 1. ADOPCIÓN DEL NUEVO SISTEMA INTEGRADO DE GESTIÓN

INSTITUCIONAL. Adóptese el Nuevo Sistema Integrado de Gestión Institucional de la Agencia Nacional de Defensa Jurídica del Estado, articulado con el Sistema de Control Interno, y entendido como un conjunto de subsistemas de gestión que tiene como propósito orientar y fortalecer la gestión institucional, estableciendo responsabilidades e instancias decisorias orientadas a la planificación, implementación, articulación y sostenibilidad del sistema, de conformidad con la normatividad vigente, las características y desarrollo institucional de la Entidad.

ARTÍCULO 2. CONFORMACIÓN DEL NUEVO SISTEMA INTEGRADO DE GESTIÓN INSTITUCIONAL. El Sistema Integrado de Gestión Institucional lo conforman los siguientes subsistemas de gestión:

1. SUBSISTEMA DE GESTIÓN DE CALIDAD -SGC-. Este subsistema se estructura de acuerdo con lo establecido en la norma NTC ISO 9001:2015 que es la base del Sistema de Gestión de la Calidad y demás normas concordantes y vigentes que le sean aplicables. Esta norma internacional se centra en todos los elementos de la gestión de la calidad para tener un sistema efectivo que permita administrar y mejorar la calidad de los productos o servicios en la Entidad.

2. SUBSISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO - SG-SST-. Las directrices frente al Subsistema están contenidas en el Decreto 1072 de 2015, "Por medio del cual se expide el Decreto Único Reglamentario del Sector Trabajo", e incluye la política, la organización, la planificación, la aplicación, la evaluación, la auditoría y las acciones de mejora para anticipar, reconocer, evaluar y controlar los riesgos que puedan afectar la seguridad y la salud en el trabajo, y se sustenta en dicha normatividad y demás normas que la complementen, modifiquen o adicionen.

3. SUBSISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - SGSPI-. Este subsistema se basa en la norma internacional ISO 27001 de 2013 y en el Decreto 1078 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones", que define los 4 componentes de la Estrategia de Gobierno en Línea GEL, entre estos el de seguridad y privacidad de la información, respecto del cual se diseñó un documento de lineamientos denominado Modelo de Seguridad y Privacidad de la Información (MSPI), que soporta transversalmente los componentes de la Estrategia de Gobierno en Línea y se sustenta en la legislación aplicable y las normas que la complementen, modifiquen o adicionen.

TITULO II.

RESPONSABLES Y RESPONSABILIDADES PARA EL DESARROLLO DEL SISTEMA INTEGRADO DE GESTIÓN INSTITUCIONAL.

ARTÍCULO 3. RESPONSABLES DEL NUEVO SISTEMA INTEGRADO DE GESTIÓN INSTITUCIONAL. Los responsables de la implementación, sostenimiento y mejora del nuevo Sistema Integrado de Gestión Institucional de la Entidad son los siguientes:

1. El Director General.

2. El Representante de la Alta Dirección para el Sistema.

3. Los líderes de procesos.

4. Los colaboradores de la Entidad.

5. Los enlaces del Sistema - Equipo SIGI.

6. El Jefe de la Oficina Asesora de Planeación, responsable del Subsistema de Gestión de la Calidad -SGC-.

7. El Coordinador del Grupo Interno de Gestión de Talento Humano, responsable del Subsistema de Gestión de Seguridad y Salud en el Trabajo - SG-SST-.

8. El Líder del Proceso de Gestión de Tecnologías de la Información, responsable del Subsistema de Gestión de Seguridad y Privacidad de la Información - SGSPI-.

CAPÍTULO I.

RESPONSABILIDADES DEL DIRECTOR GENERAL, REPRESENTANTE DE LA ALTA DIRECCIÓN, LÍDERES DE PROCESOS, COLOBORADORES DE LA ENTIDAD Y DEL EQUIPO SIGI.

ARTÍCULO 4. RESPONSABILIDADES DEL DIRECTOR GENERAL. El Director General será el responsable de liderar y asegurar la implementación, cumplimiento y sostenibilidad del Sistema Integrado de Gestión Institucional en la Agencia Nacional de Defensa Jurídica del Estado, y tendrá las siguientes responsabilidades:

1. Designar los responsables y sus responsabilidades frente al Sistema.

2. Asignar los recursos para su implementación y sostenibilidad.

3. Revisar el cumplimiento de las políticas y objetivos del Sistema.

4. Evaluar la mejora continua y desempeño de la Entidad.

Adicionalmente, respecto de cada uno de los Subsistemas que lo componen, Gestión de Calidad -SGC-, de Seguridad y Salud en el Trabajo - SG-SST-, y de Seguridad y Privacidad de la Información - SGSPI-, el Director General asumirá su liderazgo y compromiso y atenderá las responsabilidades que le señale la normatividad vigente.

ARTÍCULO 5. DESIGNACIÓN DEL REPRESENTANTE DE LA ALTA DIRECCIÓN PARA EL SISTEMA INTEGRADO DE GESTIÓN INSTITUCIONAL. Se designa como representante de la Alta Dirección para el Sistema Integrado de Gestión Institucional, al Jefe de la Oficina Asesora de Planeación de la Agencia Nacional de Defensa Jurídica del Estado, quien asegurará que se establezcan, implementen y mantengan los procesos necesarios para el adecuado desarrollo, sostenibilidad y mejora continua del Sistema Integrado de Gestión Institucional en la Agencia Nacional de Defensa Jurídica del Estado y de los Subsistemas que lo componen.

ARTÍCULO 6. RESPONSABILIDADES DEL REPRESENTANTE DE LA ALTA DIRECCIÓN PARA EL SISTEMA INTEGRADO DE GESTIÓN INSTITUCIONAL. En el marco del Sistema Integrado de Gestión Institucional de la Agencia Nacional de Defensa Jurídica del Estado, el representante de la Alta Dirección tendrá a su cargo las siguientes funciones:

1. Someter a aprobación del Comité Institucional de Gestión y Desempeño, las políticas, objetivos y el mapa de procesos para la implementación, mantenimiento y mejora del Sistema Integrado de Gestión Institucional.

2. Promover la divulgación y apropiación de las políticas y objetivos aprobados por el Comité Institucional de Gestión y Desempeño.

3. Informar a la Alta Dirección sobre el desempeño del Sistema Integrado de Gestión Institucional.

4. Informar a la Alta Dirección los cambios del Sistema Integrado de Gestión Institucional que se planifiquen e implementen garantizando que se mantenga la integridad del mismo.

5. Promover la toma de conciencia al interior de la Agencia respecto a la identificación y cumplimiento de los requisitos del cliente.

6. Promover la generación de acciones de mejora, en la implementación, sostenibilidad del Sistema Integrado de Gestión Institucional.

7. Gestionar los recursos requeridos para garantizar la implementación, sostenibilidad y mejora del Sistema Integrado de Gestión Institucional.

8. Adoptar con autonomía las decisiones que correspondan al desarrollo, implementación y mejora continua de los sistemas, sin contravenir las competencias y atribuciones que en el mismo sentido le hayan sido asignadas a otras instancias o dependencias de la Agencia.

9. Determinar la conveniencia de las solicitudes de cambio de documentos que se tramitan ante el sistema para asegurar que se conserve la consistencia y sustentabilidad.

10. Las demás que se encuentren definidas en la normatividad vigente o las que sean definidas por el Departamento Administrativo de la Función Pública-DAFP.

ARTÍCULO 7. RESPONSABILIDADES DE LOS LÍDERES DE PROCESO. Son responsabilidades de los líderes de los procesos:

1. Implementar el plan de sostenibilidad del Sistema Integrado de Gestión Institucional de acuerdo con las directrices emitidas por los responsables de cada uno de los subsistemas de gestión que lo conforman.

2. Proponer ajustes al diseño de los procesos con el fin de lograr las metas y objetivos del mismo.

3. Gestionar y aprobar los riesgos identificados en el Sistema Integrado de Gestión Institucional.

4. Aprobar y gestionar los activos de información de su proceso.

5. Administrar la documentación de su proceso.

6. Identificar y garantizar el cumplimiento de los requisitos legales asociados a su proceso.

7. Realizar el seguimiento y monitoreo al desempeño del proceso.

8. Identificar las no conformidades e implementar las respectivas acciones de mejora.

9. Promover la apropiación del Sistema Integrado de Gestión Institucional en su proceso.

ARTÍCULO 8. RESPONSABILIDADES DE LOS COLABORADORES DE LA ENTIDAD. Los colaboradores de la Entidad tendrán la responsabilidad de atender los lineamientos, metodologías y directrices establecidas en la presente resolución, así como las demás que sean definidas para la implementación, desarrollo y mejora del Sistema Integrado de Gestión Institucional, para alcanzar los resultados planificados y la mejora continua de los procesos.

PARÁGRAFO: Adicionalmente, respecto de los Subsistemas de Gestión de Calidad - SGC, de Seguridad y Salud en el Trabajo - SG-SST y de Seguridad y Privacidad de la Información - SGSPI asumirán las responsabilidades que les señale la normatividad vigente y la presente resolución.

ARTÍCULO 9. RESPONSABILIDADES DE LOS ENLACES DEL SISTEMA INTEGRADO DE GESTIÓN INSTITUCIONAL (EQUIPO SIGI). En el marco del Sistema Integrado de Gestión Institucional se conformará un equipo con integrantes de todas las dependencias de la Agencia, designados por el jefe inmediato mediante comunicación escrita dirigida al representante de la Alta Dirección, que serán los enlaces del equipo SIGI para el Sistema Integrado de Gestión Institucional, los cuales tendrán a su cargo las siguientes responsabilidades:

1. Ejercer el rol de facilitadores y actuar como enlace directo entre el Representante de Ja Alta Dirección para el Sistema Integrado de Gestión Institucional, los líderes de proceso y colaboradores de la dependencia.

2. Difundir al interior de sus dependencias toda la información relacionada con el Sistema Integrado de Gestión Institucional - SIGI.

3. Apoyar a los jefes de las dependencias en las actividades de documentación, actualización y mejora de los documentos del Sistema Integrado de Gestión Institucional-SIGI que tengan a su cargo.

4. Apoyar a los jefes de las dependencias en la aplicación de las metodologías desde su formulación, documentación, seguimiento y reporte de: análisis de indicadores, administración de riesgos, acciones de mejora y activos de información.

5. Apoyar las labores de sensibilización y socialización de los procesos que lidera su dependencia.

6. Fomentar al interior de sus dependencias la cultura de autocontrol, autogestión y autorregulación como mecanismo para promover la mejora continua.

7. Apoyar a los jefes de dependencia en la formulación, seguimiento, reporte y solicitud de ajustes del Plan Operativo Anual correspondiente.

8. Asistir y participar activamente en las reuniones y capacitaciones programadas para el Equipo SIGI.

CAPÍTULO II.

RESPONSABILIDADES FRENTE A LOS SUBSISTEMAS DE GESTIÓN DE CALIDAD - SGC-, DE SEGURIDAD Y SALUD EN EL TRABAJO - SG-SST- Y DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - SGSPI-.

ARTÍCULO 10. RESPONSABILIDADES FRENTE AL SUBSISTEMA DE GESTIÓN DE CALIDAD-SGC-. Este Subsistema tiene como objetivo dirigir y evaluar el desempeño institucional en términos de calidad, satisfacción de los usuarios y partes interesadas en la prestación de los servicios y productos de la Agencia, y busca mejorar la gestión por procesos con un enfoque orientado a resultados.

El Jefe de la Oficina Asesora de Planeación será el responsable del Subsistema de Gestión de la Calidad, y tendrá las siguientes responsabilidades:

1. Proponer al Representante de la Alta Dirección, el mapa de procesos, política y objetivos del Subsistema de Gestión de Calidad que serán sometidos a aprobación del Comité Institucional de Gestión y Desempeño.

2. Planear, implementar, hacer seguimiento y evaluar los planes de sostenibilidad y mejora del Subsistema de Gestión de Calidad.

3. Establecer las metodologías y herramientas necesarias para la mejora del Subsistema de Gestión de Calidad de manera articulada con los líderes de los otros subsistemas de gestión.

4. Brindar asistencia técnica a todos los procesos en temas relacionados con el Subsistema de Gestión de Calidad.

5. Gestionar los cambios que puedan afectar el Subsistema de Gestión de Calidad.

6. Administrar los riesgos de gestión y corrupción.

7. Establecer la metodología para la identificación y seguimiento al cumplimiento de los requisitos legales asociados a los procesos.

8. Diseñar estrategias y emitir directrices a los Enlaces SIGI, para la implementación de acciones dirigidas a la sostenibilidad del Subsistema de Gestión de Calidad.

9. Las demás que se encuentren definidas en la normatividad vigente.

ARTÍCULO 11. RESPONSABILIDADES FRENTE AL SUBSISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO -SG-SST-. La gestión de seguridad y salud en el trabajo se basa en un conjunto de actividades planificadas y controladas enfocadas a la prevención de las lesiones y enfermedades causadas por las condiciones de trabajo, y a la protección y promoción de la salud de los trabajadores, como también de los clientes y demás partes interesadas, que puedan estar expuestas a peligros asociados.

El Coordinador del Grupo Interno de Gestión de Talento Humano será el responsable del Subsistema de Gestión de Seguridad y Salud en el Trabajo -SG-SST- y tendrá las siguientes responsabilidades:

1. Proponer al Representante de la Alta Dirección la política y objetivos del Subsistema de Gestión de Seguridad y Salud en el Trabajo, que serán sometidos a aprobación del Comité Institucional de Gestión y Desempeño, para su posterior adopción por parte del Director General.

2. Planear, implementar, hacer seguimiento a los planes de sostenibilidad y mejora del Subsistema y realizar su evaluación como mínimo una (1) vez al año.

3. Rendir cuentas a la alta Dirección, sobre el funcionamiento y los resultados del Sistema de

Gestión de Seguridad y Salud en el Trabajo, conforme a los estándares mínimos del sistema SG-SST.

4. Promover medidas de divulgación y conocimiento de la Política en Seguridad y Salud en el Trabajo.

5. Promover la participación de todos los colaboradores de la Agencia en la implementación del Sistema de Gestión de Seguridad y Salud en el Trabajo.

6. Promover actividades para el cuidado integral de la salud de los colaboradores de la Agencia y adoptar las medidas de prevención que se requieran.

7. Informar oportunamente al Secretario General, acerca de los peligros y riesgos latentes en las instalaciones de la Agencia, así como los actos y condiciones inseguras que puedan generar un incidente o accidente de trabajo.

8. Coordinar las actividades y seguimiento al plan de trabajo con la Administradora de riesgos laborales - ARL.

9. Diseñar actividades de capacitación, inducción y reinducción en seguridad y salud en el trabajo, definidas en el plan de capacitación del Sistema de Gestión de Seguridad y Salud en el Trabajo.

10. Reportar a la ARL los accidentes laborales que se puedan presentar y llevar estadísticas de los mismos, así como los incidentes y efectuar actividades de prevención frente a ellos.

11. Las demás que se encuentren definidas en la normatividad vigente.

PARÁGRAFO 1o. De conformidad con el Decreto 1072 de 2015, el Sistema de Gestión de la Seguridad y Salud en el Trabajo -SG-SST debe ser liderado e implementado por el empleador o contratante, con la participación de los trabajadores y/o contratistas, garantizando a través de dicho sistema, la aplicación de las medidas de Seguridad y Salud en el Trabajo, el mejoramiento del comportamiento de los trabajadores, las condiciones y el medio ambiente laboral, y el control eficaz de los peligros y riesgos en el lugar de trabajo. En consecuencia, el Sistema -SG-SST establece obligaciones específicas para el empleador o representante legal, para los servidores públicos de distintos niveles, así como para contratistas de la Agencia, y se regirán por el Decreto 1072 de 2015 y la normatividad vigente que la complemente, modifique o adicione.

PARÁGRAFO 2o. Para el cumplimiento de las responsabilidades asignadas, el Coordinador el Grupo Interno de Gestión de Talento Humano contará con el apoyo de un profesional de seguridad y salud en el trabajo con licencia en Salud Ocupacional y demás requisitos legales.

ARTÍCULO 12. RESPONSABILIDADES FRENTE AL SUBSISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Este tiene como objetivo principal proteger la información y los sistemas de información, así como asegurar la confidencialidad, integridad y disponibilidad de la información de la Agencia.

El Líder del Proceso de Gestión de Tecnologías de la Información, será el responsable frente al Subsistema de Gestión de Seguridad y Privacidad de Ja Información y tendrá las siguientes responsabilidades:

1. Proponer al Representante de la Alta Dirección las políticas y objetivos del Subsistema de

Gestión de Seguridad y Privacidad de la Información que serán sometidas a aprobación del Comité Institucional de Gestión y Desempeño.

2. Planear, implementar, hacer seguimiento y evaluar los planes de sostenibilidad y mejora del Subsistema de Gestión de Seguridad y Privacidad de la Información- SGSPI.

3. Precisar los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) que deban ser implementados en la Agencia de acuerdo con las necesidades de la Entidad.

4. Revisar y mantener actualizada la Política de Seguridad de la Información que debe ser aplicada por los funcionarios, contratistas, proveedores, visitantes y partes interesadas.

5. Brindar asistencia técnica a los líderes de otros procesos en temas relacionados con confidencialidad, integridad y disponibilidad de la información de la Agencia.

6. Participar como representante de la Agencia, en las reuniones sectoriales que lidera el Ministerio de Justicia y del Derecho ante el Ministerio de Tecnologías de la Información y las Comunicaciones.

7. Establecer las acciones de divulgación y comunicación de la implementación y mantenimiento del Subsistema de Gestión de Seguridad y Privacidad de la Información.

8. Determinar las acciones para la implementación y/o mantenimiento de los controles de seguridad de la información para la Agencia.

9. Participar en los comités de cambios y gestionar aquellos cambios que puedan afectar el Subsistema de Gestión de Seguridad y Privacidad de la Información.

10. Las demás que se encuentren definidas en la normatividad vigente.

PARÁGRAFO. De conformidad con el Decreto 1078 de 2015, el representante legal de la Entidad es el responsable de coordinar, hacer seguimiento y verificación de la implementación y desarrollo de la Estrategia de Gobierno en línea, que se regirá por dicha normatividad y aquella que la complemente, modifique o adicione.

TITULO III.

INSTANCIAS DE PARTICIPACIÓN, COORDINACIÓN Y ARTICULACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN INSTITUCIONAL.

CAPÍTULO I.

COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO.

ARTÍCULO 13. COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO. Este Comité funcionará como un órgano de decisión, coordinación y asesoría para la definición de estrategias, políticas y lineamientos del Sistema Integrado de Gestión Institucional y de los Subsistemas que lo componen, así como para la implementación, desarrollo y mejoramiento Modelo Integrado de Planeación y Gestión- MIPG.

PARÁGRAFO 1o. El Comité Institucional de Gestión y Desempeño sustituirá los demás comités

que tengan relación con el Modelo y que no sean obligatorios por mandato legal, tal como lo dispone el art. 2.2.22.6. literal b. del Decreto 1083 de 2015.

ARTÍCULO 14. INTEGRANTES DEL COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO. El Comité Institucional de Gestión y Desempeño de la Agencia Nacional de Defensa Jurídica del estado estará integrado de la siguiente manera:

1. Integrantes con voz y voto:

1.1. El Director General o su delegado.

1.2. El Secretario General, quien lo presidirá.

1.3. Los Directores Técnicos.

1.4. El Subdirector Técnico.

1.5. El Jefe de la Oficina Asesora Jurídica.

1.6. El Jefe de la Oficina Asesora de Planeación.

2. Invitado permanente con derecho a voz, sin voto:

2.1. El Jefe de la Oficina de Control Interno.

PARÁGRAFO 1o. La asistencia al Comité es obligatoria para los integrantes con voz y voto, sin embargo, cuando por motivo de fuerza mayor algún miembro del Comité no pueda asistir, deberá comunicarlo a la Secretaría Técnica del Comité y, en todo caso, deberá consultar las actas, especialmente en lo relacionado con los resultados y los compromisos adquiridos durante la respectiva sesión.

PARÁGRAFO 2o. A las reuniones del Comité podrán asistir en calidad de invitados ocasionales, con voz, pero sin voto, los funcionarios, contratistas o cualquier tercero que por su conocimiento técnico o del asunto a tratar deban asistir. Estos serán invitados a la sesión del Comité por intermedio de su Secretario Técnico.

ARTÍCULO 15. FUNCIONES DEL COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO. Son funciones del Comité Institucional de Gestión y Desempeño las siguientes:

1. Respecto del Sistema Integrado de Gestión Institucional

a) Definir y aprobar políticas, objetivos y lineamientos y/o cualquier modificación o adición que se proponga y que contribuya a la implementación, mantenimiento y mejora del Nuevo Sistema Integrado de Gestión Institucional - SIGI y de los Subsistemas que lo componen.

b) Servir de instancia de coordinación de las políticas, objetivos, lineamientos de los Subsistemas de Gestión.

c) Aprobar el Código de Integridad de la Entidad y servir de instancia de interpretación de los acuerdos y compromisos éticos asumidos por la Entidad y definir los lineamientos de divulgación y socialización del mismo.

d) Revisar el desempeño del Sistema Integrado de Gestión Institucional de la Agencia Nacional de Defensa Jurídica del Estado y de cada uno de los Subsistemas que lo componen.

e) Efectuar recomendaciones al Director para la adopción de decisiones y revisión de políticas internas a que haya lugar, con el propósito de lograr un desempeño institucional integral.

g) Las demás responsabilidades asociadas que propendan por el buen funcionamiento del Sistema Integrado de Gestión Institucional.

2. Respecto del Modelo Integrado de Planeación y Gestión - MIPG.

a. Aprobar y hacer seguimiento, por lo menos una vez cada tres meses, a las acciones y estrategias adoptadas para la operación del Modelo Integrado de Planeación y Gestión - MIPG.

b. Articular los esfuerzos institucionales, recursos, metodologías y estrategias para asegurar la implementación, sostenibilidad y mejora del Modelo Integrado de Planeación y Gestión - MIPG.

c. Proponer al Comité Sectorial de Gestión y el Desempeño Institucional, iniciativas que contribuyan al mejoramiento en la implementación y operación del Modelo Integrado de Planeación y Gestión - MIPG.

d. Presentar los informes que el Comité Sectorial de Gestión y el Desempeño Institucional y los organismos de control requieran sobre la gestión y el desempeño de la entidad.

e. Adelantar y promover acciones permanentes de autodiagnóstico para facilitar la valoración interna de la gestión.

f. Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.

g. Las demás que tengan relación directa con la implementación, desarrollo y evaluación del Modelo.

3. Respecto a la Gestión Documental y Archivo

Cumplir las funciones del Comité Interno de Archivo definidas en el artículo 2.8.2.1.16 del Decreto 1080 de 2015, el cual reglamentó el Sistema Nacional de Archivos.

4. Respecto de los Inventarios y Bienes de la Agencia

a) Analizar la necesidad y conveniencia para dar de baja los bienes que se encuentran en buenas condiciones pero que no se requieren para el desarrollo de las actividades de la Agencia, o que sean inservibles u obsoletos y recomendar la baja de los mismos.

b) Aprobar la destinación de los bienes muebles objeto de baja.

ARTÍCULO 16. SECRETARÍA TÉCNICA. El Jefe de la Oficina Asesora de Planeación de la Agencia Nacional de Defensa Jurídica del Estado actuará como Secretario Técnico del Comité Institucional de Gestión y Desempeño y tendrá a su cargo las siguientes funciones:

1. Coordinar las reuniones del Comité Institucional de Gestión y Desempeño, citar a los integrantes e invitados al Comité, elaborar el orden del día de la reunión, dar lectura al acta anterior y realizar seguimiento a los compromisos.

2. Elaborar las actas de cada sesión del Comité.

3. Preparar o consolidar y presentar los documentos, informes o material que se requiera para el normal desarrollo de las sesiones del Comité.

4. Verificar el cumplimiento de las decisiones adoptadas por el Comité.

5. Custodiar, conservar y coordinar el archivo y control de las actas del Comité.

6. Consolidar y reportar la información de seguimiento requerida por el Comité Sectorial de Desarrollo Administrativo del Sector Justicia.

7. Proyectar y someter a consideración del Comité, la información que este requiera para la formulación y diseño de las políticas de desarrollo administrativo de la Entidad.

8. Las demás que le sean asignadas por el Comité y por la normatividad vigente.

ARTÍCULO 17. REUNIONES Y CONVOCATORIA DEL COMITÉ. De manera ordinaria, el Comité Institucional de Gestión y Desempeño se reunirá por lo menos cuatro (4) veces al año, y de manera extraordinaria cuando las circunstancias lo ameriten o su Presidente lo convoque. El Secretario Técnico del Comité procederá a convocar a los integrantes del mismo, indicando día, hora y lugar de la reunión y el respectivo Orden del día. No obstante, lo anterior, el Comité se podrá reunir de manera extraordinaria por solicitud de dos (2) de los integrantes con derecho a voz y voto y previa citación efectuada por el Secretario Técnico.

ARTÍCULO 18. QUORUM DELIBERATORIO Y ADOPCIÓN DE LAS DECISIONES. El Comité Institucional de Gestión y Desempeño deliberará y decidirá como mínimo con la mitad más uno de sus integrantes con voz y voto. Las proposiciones serán aprobadas por la mayoría simple de los miembros asistentes a la sesión.

Las disposiciones generales adoptadas por el Comité serán registradas en el acta correspondiente.

CAPÍTULO II.

COMITÉ INSTITUCIONAL DE COORDINACIÓN DE CONTROL INTERNO.

ARTÍCULO 19. COMITÉ INSTITUCIONAL DE COORDINACIÓN DE CONTROL INTERNO. Funcionará como un órgano asesor e instancia decisoria en los asuntos del control interno.

ARTÍCULO 20. INTEGRANTES DEL COMITÉ INSTITUCIONAL DE COORDINACIÓN DE CONTROL INTERNO. El Comité estará integrado de la siguiente manera:

1. El Director General, quien lo presidirá.

2. El Secretario General.

3. Los Directores Técnicos.

4. El Subdirector Técnico.

5. El Jefe de la Oficina Asesora de Planeación, quien es a su vez el representante de la Alta Dirección para la implementación del Modelo Estándar de Control Interno y del Sistema Integrado de Gestión Institucional.

PARÁGRAFO 1o. El Jefe de Control Interno o quien haga sus veces, participará con voz, pero sin voto en el mismo.

PARÁGRAFO 2o. El Presidente del comité, podrá invitar a otros funcionarios de la Agencia, quienes participarán con voz, pero sin voto. El Jefe de la Oficina Asesora Jurídica será invitado permanente a las sesiones del comité, con voz, pero sin voto.

PARÁGRAFO 3o. La asistencia al Comité es obligatoria para los integrantes con voz y voto.

ARTÍCULO 21. FUNCIONES DEL COMITÉ INSTITUCIONAL DE COORDINACIÓN DE CONTROL INTERNO. EL Comité Institucional de Coordinación de Control Interno ejercerá las funciones dispuestas en el artículo 2.2.21.1.6. del Capítulo 1 del Título 21 del Decreto 1083 de 2015 adicionado por el artículo 4 del Decreto 648 de 2017, que se señalan a continuación:

1. Evaluar el estado del Sistema de Control Interno de acuerdo con las características propias de cada organismo o entidad y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento del sistema a partir de la normatividad vigente, los informes presentados por el jefe de control interno o quien haga sus veces, organismos de control y las recomendaciones del equipo MECI.

2. Aprobar el Plan Anual de Auditoría de la entidad presentado por el Jefe de Control Interno o quien haga sus veces, hacer sugerencias y seguimiento a las recomendaciones producto de la ejecución del plan, de acuerdo con lo dispuesto en el estatuto de auditoría, basado en la priorización de los temas críticos según la gestión de riesgos de la Administración.,

3. Aprobar el Estatuto de Auditoría Interna y el Código de Ética del Auditor y sus modificaciones, así como verificar su cumplimiento.

4. Revisar la información contenida en los estados financieros de la entidad y hacer las recomendaciones a que haya lugar.

5. Servir de instancia para resolver las diferencias que surjan en desarrollo del ejercicio de auditoría interna.

6. Conocer y resolver los conflictos de interés que afecten la independencia de la auditoría.

7. Someter a aprobación del representante legal, la política de administración del riesgo y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta.

8. Las demás asignadas por la normatividad vigente y el Representante Legal de la entidad.

PARÁGRAFO 1o. Entiéndase como Equipo MECI en la Agencia Nacional de Defensa Jurídica del Estado el Equipo SIGI.

ARTÍCULO 22. SECRETARÍA TÉCNICA. El Jefe de la Oficina de Control Interno de la Agencia Nacional de Defensa Jurídica del Estado, ejercerá la Secretaría Técnica del Comité Institucional de Coordinación de Control Interno y tendrá a su cargo las siguientes funciones:

1. Coordinar las reuniones del Comité, citar a los integrantes e invitados al Comité, elaborar el orden del día de la reunión, dar lectura al acta anterior y realizar seguimiento a los compromisos pendientes.

2. Elaborar las actas de cada sesión del Comité.

3. Preparar o consolidar los documentos, informes o material que se requiera para el normal desarrollo de las sesiones del Comité.

4. Verificar el cumplimiento de las decisiones adoptadas por el Comité.

5. Custodiar, conservar y coordinar el archivo y control de las actas del Comité.

6. Consolidar y reportar la información de seguimiento requerida por el Comité de Coordinación del Sistema de Control Interno.

7. Las demás que le sean asignadas por el Comité y por la normatividad vigente.

ARTÍCULO 23. REUNIONES Y CONVOCATORIA. El Comité Institucional de Coordinación de Control Interno de la Agencia Nacional de Defensa Jurídica del Estado se reunirá de manera ordinaria dos (02) veces al año. De manera

extraordinaria cuando sea convocado por su Presidente, por el Jefe de la Oficina de Control Interno o por solicitud de la mitad más uno de los miembros del Comité. El Secretario Técnico del Comité convocará con al menos tres (03) días de anticipación, indicando día, hora y lugar de reunión y el respectivo orden del día.

ARTÍCULO 24. QUORUM DELIBERATORIO Y ADOPCIÓN DE LAS DECISIONES. El Comité Institucional de Coordinación de Control Interno deliberará y decidirá como mínimo con la mitad más uno de sus integrantes con voz y voto, y las proposiciones serán aprobadas por la mayoría simple de los miembros asistentes a la sesión.

TÍTULO IV.

CAPÍTULO I.

MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN -MIPG, POLÍTICAS, MANUALES DEL SISTEMA INTEGRADO DE GESTIÓN INSTITUCIONAL.

ARTÍCULO 25. ADOPCIÓN DEL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN -MIPG- Y DE LAS POLÍTICAS. Adóptese en la Agencia Nacional de Defensa Jurídica del Estado el Modelo Integrado de Planeación y Gestión -MIPG (versión 2), las Políticas de Gestión y Desempeño Institucional enunciadas en el Artículo 2.2.22.2.1. del Decreto 1499 de 2017, complementadas y articuladas son las Políticas de los Subsistemas de Gestión de Calidad -SGC, de Seguridad y Salud en el Trabajo - SG-SST y de Seguridad y Privacidad de la Información - SGSPI- desarrolladas por la Entidad, y el Manual Operativo del Departamento Administrativo de Función Pública, como un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión la Entidad para el cumplimiento de las metas institucionales y de Gobierno.

PARÁGRAFO: Las Políticas de los Subsistemas de Gestión de Calidad -SGC, de Seguridad y Salud en el Trabajo - SG-SST- y de Seguridad y Privacidad de la Información - SGSPI- están contenidas en Manual de Políticas de Gestión y Desempeño Institucional - DE-M-02, que hace parte integral de la presente Resolución y podrá ser actualizado con las políticas que se definan y las necesidades de la Entidad, de acuerdo con la elaboración y control de documentos previstos por el Sistema Integrado de Gestión Institucional.

ARTÍCULO 26. IMPLEMENTACIÓN Y SOSTENIBILIDAD DE LAS POLÍTICAS DE GESTIÓN Y DESEMPEÑO INSTITUCIONAL Y DE LOS SUBSISTEMAS DE GESTION DE LA ENTIDAD. Para la implementación y/o ejecución y/o sostenibilidad de las Políticas de Gestión y Desempeño Institucional enunciadas en el artículo anterior, se conforman los equipos temáticos que se señalan en los siguientes cuadros, que deberán presentar propuestas y estrategias de operación al Comité Institucional de Gestión y Desempeño para su aprobación y/o realizar los ajustes que éste considere necesarios, respecto de las correspondientes políticas:

Cuadro 1: Responsables y Equipos temáticos para la implementación y/o sostenibilidad de las Políticas de Gestión y Desempeño Institucional

No	Dimensión	Política	Responsable	Equipos temáticos
1	Talento Humano	Gestión Estratégica del Talento Humano	Secretario General	Coordinador del Grupo Interno de Gestión de Talento Humano
		Integridad		
No	Dimensión	Política	Responsable	Equipos temáticos
2	Direccionamiento Estratégico y Planeación	Planeación institucional	Jefe Oficina Asesora de Planeación	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 Resultado	Fortalecimiento organizacional y simplificación de procesos	Jefe Oficina Asesora de Planeación	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, antes Gobierno en Línea	Jefe Oficina Asesora de Planeación	Director Gestión de la Información Líderes de los Procesos: Gestión de Tecnologías de la Información, Gestión Documental, Gestión con Grupo de Interés y Comunicaciones
		Seguridad Digital	Líder Proceso Gestión de Tecnologías de la Información	Líder Proceso Gestión de Tecnologías de la Información Jefe Oficina Asesora de Planeación Director Gestión de la Información
		Defensa jurídica	Jefe Oficina Asesora Jurídica	Oficina Asesora Jurídica Líderes de proceso

		Servicio al Ciudadano	Secretario General	Jefe Oficina Asesora de Planeación Responsable Atención al Ciudadano Líderes de proceso
		Racionalización de Trámites	N.A	N.A
		Participación ciudadana en la gestión pública	Líder Proceso Gestión con Grupo de Interés y Comunicaciones	Jefe Oficina Asesora de Planeación Líder Proceso Gestión con Grupo de Interés y Comunicaciones Líderes de proceso
4	Evaluación de Resultados	Seguimiento y evaluación de) desempeño institucional	Jefe Oficina Asesora de Planeación	Directores Subdirector Secretario General Jefes de Oficina Líderes de proceso
5	Información y Comunicación	Gestión documental	Secretario General	Líder Proceso Gestión Documental Líderes de proceso
		Transparencia, acceso a la información pública y lucha contra la corrupción	Jefe Oficina Asesora de Planeación	Líder Proceso Gestión con Grupo de Interés y Comunicaciones Jefe Oficina Asesora de Planeación Líderes de proceso
6	Gestión del Conocimiento y la Innovación	Gestión de] Conocimiento y la Innovación	Jefe Oficina Asesora de Planeación	Director de Gestión de la Información Director de Políticas y Estrategias Jefe Oficina Asesora de Planeación Líderes de proceso
7	Control Interno	Control Interno	Jefe Oficina de Control Interno	Jefe Oficina de Control Interno

*De acuerdo con el objeto y funciones que desarrolla la Agencia Nacional de Defensa Jurídica del Estado, no ejerce funciones administrativas que conlleven a la realización de un trámite u otro procedimiento administrativo orientado a ningún tipo de usuario, por tanto, no se encuentra dentro del ámbito de aplicación de la política de racionalización de trámites (Concepto emitido por el Departamento Administrativo de la Función Pública).

Cuadro 2: Responsables y Equipos temáticos la implementación y/o ejecución y/o sostenibilidad de las Políticas de los Subsistemas del Sistema Integrado de Gestión Institucional

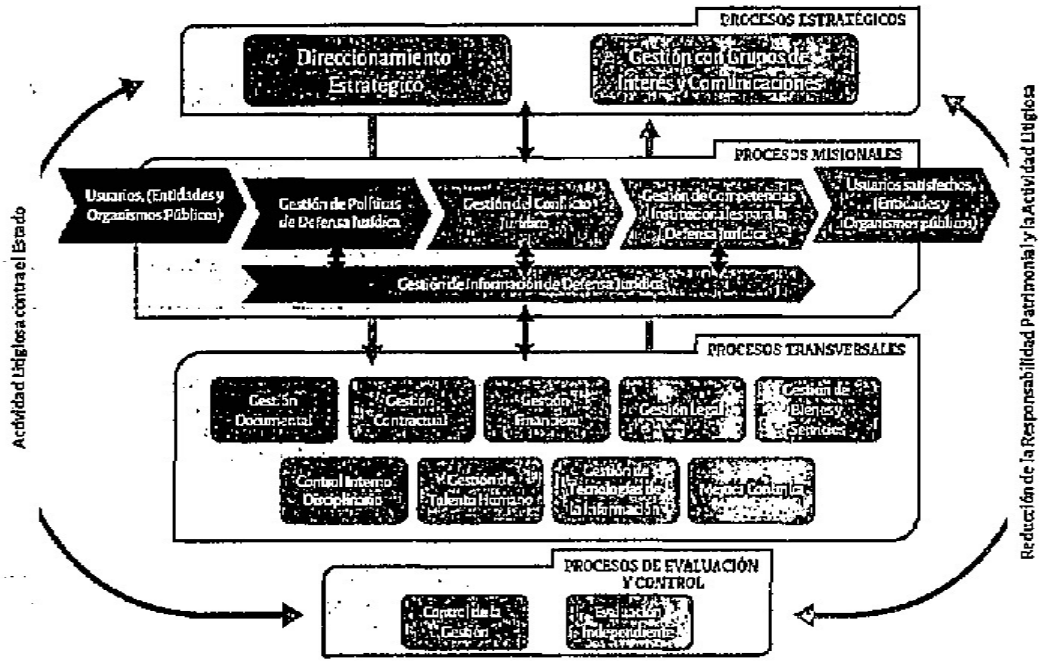
Política y objetivos	Responsable	Apoyan
Subsistema de Gestión de Calidad	Jefe Oficina Asesora de Planeación	Colaboradores de la Oficina Asesora de Planeación
Subsistema de Gestión de Seguridad y Salud en el Trabajo	Coordinador del Grupo Interno de Gestión de Talento Humano	Secretario General Colaboradores del Grupo Interno de Gestión de Talento Humano
Subsistema de Gestión de Seguridad y Privacidad de la Información	Líder del Proceso de Gestión de Tecnologías de la Información	Secretario General Colaboradores del proceso Gestión de Tecnologías de la Información Oficina Asesora de Planeación Oficina Asesora Jurídica Gestión Documental

CAPÍTULO II.

INSTRUMENTOS ADMINISTRATIVOS DEL SISTEMA INTEGRADO DE GESTIÓN INSTITUCIONAL.

ARTÍCULO 27. ADOPCIÓN DEL MAPA DE OPERACIÓN POR PROCESOS. Adóptese el mapa de operación por procesos de la Agencia Nacional de Defensa Jurídica del Estado, como herramienta administrativa que estandariza las interrelaciones de los procesos estratégicos, misionales, transversales y de evaluación y control.

Mapa de procesos de la Agencia Nacional de Defensa Jurídica del Estado.



ARTÍCULO 28. EVALUADOR DEL SISTEMA. La Oficina de Control Interno, será responsable de realizar la evaluación independiente y objetiva de la implementación, mantenimiento y mejora del Sistema Integrado de Planeación y Gestión y del Modelo Integrado de Planeación y Gestión - MIPG.

TÍTULO V.

DISPOSICIONES VARIAS.

ARTÍCULO 29. VIGENCIA Y DEROGATORIAS. La presente Resolución rige a partir de la fecha de su expedición y deroga las siguientes disposiciones:

- Resolución 362 de 9 de octubre de 2015, "Por medio de la cual se adopta el Sistema Integrado de Gestión Institucional y se dictan otras disposiciones."

- Numeral, 6.1. De los Comités para las Buenas Prácticas en la Agencia del Código Ética y Buen Gobierno de la Agencia Nacional de Defensa Jurídica del Estado, adoptado mediante la Resolución 178 de 7 de julio de 2014.

- Resolución 038 de 2015 "Por medio del cual se conforman los Comités de Buen Gobierno y Ética de la Agencia Nacional de Defensa Jurídica del Estado."

- Artículos 2 y 3 de la Resolución 021 de 2016 "Por medio de la cual se asignan unas obligaciones y responsabilidades frente al Sistema de Gestión de Seguridad y Salud en el Trabajo, y se dictan otras disposiciones."

- Artículo 5, 6, 7 y 8 de la Resolución 263 del 17 de julio de 2017, "Por medio de la cual se modifica la Resolución No. 105 del 12 de mayo de 2014, la Resolución No. 038 del 16 de febrero de 2015, la Resolución 362 del 09 de octubre de 2015, la Resolución No. 127 del 02 de mayo de 2016 y la Resolución No. 260 del 01 de septiembre de 2016. "

Dada en la Ciudad de Bogotá D.C, a los, 26 FEB 2018

COMUNIQUESE Y CÚMPLASE

LUIS GUILLERMO VÉLEZ CABRERA

Director General

ANEXO.

MANUAL DE POLITICAS DE GESTION Y DESEMPEÑO INSTITUCIONAL DE LA AGENCIA

UNIDAD ADMINISTRATIVA ESPECIAL AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO FEBRERO DE 2018

TABLA DE CONTENIDO

OBJETIVO

Proporcionar el compendio de las políticas definidas por la Agencia desde su creación, entre estas las que corresponden a las políticas del Sistema Integrado de Gestión Institucional - SIGI-, que complementan las Políticas de Gestión y Desempeño Institucional contenidas en el nuevo Modelo Integrado de Planeación y Gestión - MIPG, que sirven de marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión en la Entidad.

ALCANCE

Las políticas contenidas en este manual deben ser aplicados por todos los colaboradores de la Agencia en el desarrollo de sus funciones.

Este manual podrá ser actualizado con las políticas que se definan y las necesidades de la Entidad, conforme con lo dispuesto en el procedimiento para la elaboración y control de documentos previstos por el Sistema Integrado de Gestión Institucional.

DEFINICIONES

SIGI: Sistema Integrado de Gestión Institucional, un conjunto de subsistemas de gestión que tiene como propósito orientar y fortalecer la gestión institucional, estableciendo responsabilidades e instancias decisorias orientadas a la planificación, implementación, articulación y sostenibilidad del sistema, de conformidad con la normatividad vigente, las características y desarrollo institucional de la Entidad, constituido por los subsistemas de Gestión; de Calidad -SGC-, Subsistema de Gestión de Seguridad y Salud en el Trabajo - SG-SST-, Subsistema de Gestión de Seguridad y Privacidad de la Información - SGSPI-.

1. ANTECEDENTES

La Agencia Nacional de Defensa Jurídica del Estado, adoptó el Modelo Integrado de Planeación y Gestión -MIPG (versión 2), las Políticas de Gestión y Desempeño Institucional enunciadas en el Artículo 2.2.22.2.1. del Decreto 1499 de 2017, complementadas y articuladas son las Políticas de los Subsistemas de Gestión de Calidad -SGC, de Seguridad y Salud en el Trabajo - SG-SST y de Seguridad y Privacidad de la Información - SGSPI- desarrolladas por la Entidad, y el Manual Operativo del Departamento Administrativo de Función Pública, como un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión la Entidad para el cumplimiento de las metas institucionales y de Gobierno.

Asimismo, las directrices del Decreto 2609 de 2012, que define los criterios para la elaboración e implementación de un Programa de Gestión Documental, que incluye la definición de una política de gestión documental, entre otras.

2. ORIENTACIÓN ESTRATÉGICA DE LA AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO

2.1. IDENTIFICACIÓN Y NATURALEZA

La Agencia Nacional de Defensa Jurídica del Estado-ANDJE-, es una entidad descentralizada del orden nacional, que hace parte de la Rama Ejecutiva. Está adscrita al Ministerio de Justicia y del Derecho, tiene autonomía administrativa y financiera, patrimonio propio y personería jurídica[1] .

La Agencia tiene como objetivos principales, el diseño de estrategias, planes y acciones dirigidos a dar cumplimiento a las políticas de defensa jurídica de la Nación y del Estado definidas por el Gobierno Nacional; la formulación, evaluación y difusión de las políticas en materia de prevención de las conductas antijurídicas por parte de servidores y entidades públicas, del daño antijurídico y la extensión de sus efectos, y la dirección, coordinación y ejecución de las acciones que aseguren la adecuada implementación de las mismas, para la defensa de los intereses litigiosos de la Nación[2].

2.2. MISIÓN

Liderar la defensa jurídica de la Nación a través de la generación de conocimiento que permita a las entidades públicas prevenir el daño antijurídico y fortalecer la defensa de los intereses litigiosos del Estado, con el fin de garantizar los derechos constitucionales y optimizar los recursos públicos en beneficio de los colombianos.

2.3. VISIÓN

En el 2018 la ANDJE habrá logrado fortalecer la gestión de defensa jurídica de la Nación y contribuido a la eficiencia fiscal del Estado.

2.4. PRINCIPIOS BÁSICOS DE LA GESTIÓN DE LA AGENCIA NACIONAL DE DEFENSA JURIDICA DEL ESTADO

Atendiendo las directrices establecidas en el Artículo 3, Capitulo II de la Ley 489 de 1998, la ANDJE desarrolla su gestión dando cumplimiento a los siguientes principios de la función administrativa: buena fe, igualdad, moralidad, celeridad, economía, imparcialidad, eficacia, eficiencia, participación, publicidad, responsabilidad y transparencia, consagrados en la Constitución de Colombia de 1991.

2.5. ESTRUCTURA ORGANIZACIONAL

A través del Decreto 4085 del 01 de noviembre de 2011 se definió la estructura y funciones de la Agencia, la cual se refleja en el siguiente organigrama:

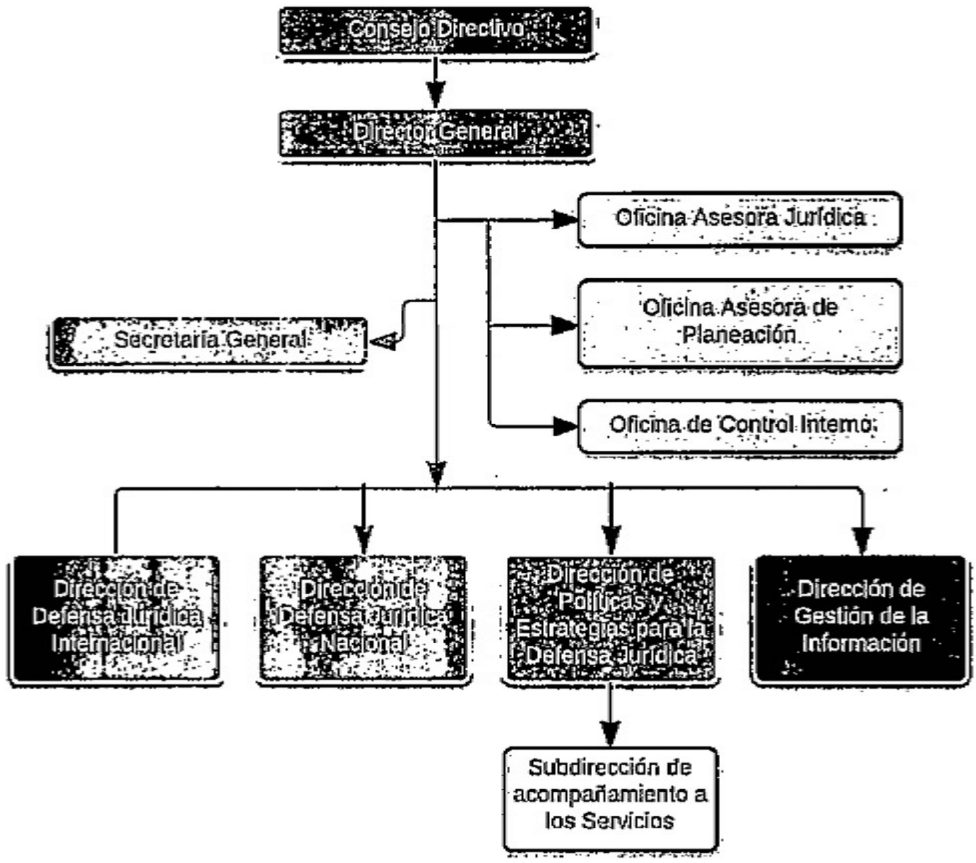


Gráfico 1. Organigrama Agencia Nacional de Defensa Jurídica

3. POLÍTICAS DE LA AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO

3.1 POLÍTICA DEL SISTEMA INTEGRADO DE GESTIÓN INSTITUCIONAL

La Alta Dirección definió la Política del Sistema Integrado de Gestión Institucional - SIGI-, la cual está alineada con la planeación estratégica de la entidad, así:

"La Agencia Nacional de Defensa Jurídica del Estado-ANDJE, se compromete a adelantar su gestión atendiendo las directrices establecidas por el Gobierno Nacional, apoyar la definición, divulgación e implementación de políticas, estrategias, planes y acciones que aseguren la defensa de los intereses litigiosos de la nación y la protección efectiva del patrimonio público.

Las acciones adelantadas por la entidad se enmarcan en los principios éticos establecidos en la Constitución Política y la mejora continua de su Sistema Integrado de Gestión Institucional en términos de eficiencia, eficacia y efectividad, con el propósito de superar las necesidades y expectativas de sus clientes".

3.1.1 DESPLIEGUE DE LA POLÍTICA DEL SISTEMA INTEGRADO DE GESTIÓN INSTITUCIONAL

Se habla de una política integrada porque recoge aspectos relacionados con el Subsistema de

Gestión de Calidad -SGC-, Este subsistema se estructura de acuerdo con lo establecido en la norma NTC ISO 9001:2015 y demás normas concordantes y vigentes que le sean aplicables. Despliega esas directrices a toda la Entidad a través de la Planeación Estratégica y el Subsistema de Gestión de Calidad. El despliegue de la política, se presenta a continuación.

3.1.1.1 Adecuada al Objeto y coherente con el PND

... a adelantar su gestión atendiendo las directrices establecidas por el Gobierno Nacional, apoyar la definición, divulgación e implementación de políticas, estrategias, planes y acciones que aseguren la defensa de los intereses litigiosos de la nación y la protección efectiva del patrimonio público...

3.1.1.2 Compromiso de cumplir los requisitos de sus clientes

... apoyar la definición, divulgación e implementación de políticas, estrategias, planes y acciones que aseguren la defensa de los intereses litigiosos de la nación y la protección efectiva del patrimonio público...

... con el propósito de superar las necesidades y expectativas de sus clientes.

3.1.1.3 Compromiso de mejorar continuamente la eficacia, eficiencia y efectividad del SGC

...se compromete... la mejora continua de su Sistema Integrado de Gestión Institucional en términos de eficiencia, eficacia y efectividad...

3.1.1.4 Compromiso de contribuir al logro de los fines esenciales del Estado

La Agencia Nacional de Defensa Jurídica del Estado -ANDJE-, se compromete a adelantar su gestión atendiendo las directrices establecidas por el Gobierno Nacional...

Las acciones adelantadas por la entidad se enmarcan en los principios éticos establecidos en la Constitución Política...

3.2 POLÍTICAS DE GESTIÓN Y DESEMPEÑO INSTITUCIONAL

Entendiendo como políticas de gestión y desempeño institucional, la definición de un conjunto de lineamientos que orientan a la Entidad hacia el mejoramiento de su gestión, dando como resultado el cumplimiento de los objetivos institucionales, según lo definido en el Decreto 1499 de 2017, la ANDJE adoptó las políticas de gestión y desempeño institucional establecidas en este Decreto[3], y las incorporó en su planeación estratégica a través de las diferentes actividades definidas por cada una de las dependencias. Dichas políticas se relacionan a continuación.

Para la implementación y/o ejecución y/o sostenibilidad de las Políticas de Gestión y Desempeño Institucional, se conforman los equipos temáticos que se señalan en los siguientes cuadros, que deberán presentar propuestas y estrategias de operación al Comité Institucional de Gestión y Desempeño para su aprobación y/o realizar los ajustes que éste considere necesarios, respecto de las correspondientes políticas:

Cuadro 1: Responsables y Equipos temáticos para la implementación y/o sostenibilidad de las Políticas de Gestión y Desempeño Institucional

No	Dimensión	Política	Responsable	Equipos temáticos

1	Talento Humano	Gestión Estratégica del Talento Humano	Secretario General	Coordinador del Grupo Interno de Gestión de Talento Humano
		Integridad		
2	Direccionamiento Estratégico y Planeación	Planeación institucional	Jefe Oficina Asesora de Planeación	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 Resultado	Fortalecimiento organizacional y simplificación de procesos	Jefe Oficina Asesora de Planeación	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, antes Gobierno en Línea	Jefe Oficina Asesora de Planeación	Director Gestión de la Información Líderes de los Procesos: Gestión de Tecnologías de la Información, Gestión Documental, Gestión con Grupo de Interés y Comunicaciones
		Segundad Digital	Líder Proceso Gestión de Tecnologías de la Información	Líder Proceso Gestión de Tecnologías de la Información Jefe Oficina Asesora de Planeación Director Gestión de la Información
		Defensa jurídica	Jefe Oficina Asesora Jurídica	Oficina Asesora Jurídica Líderes de proceso
		Servicio al Ciudadano	Secretario General	Jefe Oficina Asesora de Planeación Responsable Atención al Ciudadano Líderes de proceso
		*Racionalización de Trámites	N.A	N.A
		Participación ciudadana en la gestión pública	Líder Proceso Gestión con Grupo de Interés y Comunicaciones	Jefe Oficina Asesora de Planeación Líder Proceso Gestión con Grupo de Interés y Comunicaciones Líderes de proceso
4	Evaluación de Resultados	Seguimiento y evaluación del desempeño institucional	Jefe Oficina Asesora de Planeación	Directores Subdirector Secretario General Jefes de Oficina Líderes de proceso
5	Información y Comunicación	Gestión documental	Secretario General	Líder Proceso Gestión Documental Líderes de proceso
		Transparencia, acceso a la Información pública y lucha contra la corrupción	Jefe Oficina Asesora de Planeación	Líder Proceso Gestión con Grupo de Interés y Comunicaciones Jefe Oficina Asesora de Planeación Líderes de proceso

6	Gestión del Conocimiento y la Innovación	Gestión del Conocimiento y la Innovación	Jefe Oficina Asesora de Planeación	Director de Gestión de la Información Director de Políticas y Estrategias Jefe Oficina Asesora de Planeación Líderes de proceso
7	Control Interno	Control Interno	Jefe Oficina de Control Interno	Jefe Oficina de Control Interno

*De acuerdo con el objeto y funciones que desarrolla la Agencia Nacional de Defensa Jurídica del Estado, no ejerce funciones administrativas que conlleven a la realización de un trámite u otro procedimiento administrativo orientado a ningún tipo de usuario, por tanto, no se encuentra dentro del ámbito de aplicación de la política de racionalización de trámites (Concepto emitido por el Departamento Administrativo de la Función Pública).

Cuadro 2: Responsables y Equipos temáticos la implementación y/o ejecución y/o sostenibilidad de las Políticas de los Subsistemas del Sistema Integrado de Gestión Institucional

Política y objetivos	Responsable	Apoyan
Subsistema de Gestión de Calidad	Jefe Oficina Asesora de Planeación	Colaboradores de la Oficina Asesora de Planeación
Subsistema de Gestión de Seguridad y Salud en el Trabajo	Coordinador del Grupo Interno de Gestión de Talento Humano	Secretario General Colaboradores del Grupo Interno de Gestión de Talento Humano
Subsistema de Gestión de Seguridad y Privacidad de la Información	Líder del Proceso de Gestión de Tecnologías de la Información	Secretario General Colaboradores del proceso Gestión de Tecnologías de la Información Oficina Asesora de Planeación Oficina Asesora Jurídica Gestión Documental

3.3 POLÍTICA DE SEGURIDAD Y SALUD EN EL TRABAJO

La Política de Seguridad y Salud en el Trabajo debe atender las directrices establecidas en el Decreto 1072 de 2015 Artículo 2.2.4.6.5. Política de Seguridad y Salud en el Trabajo -SST. El empleador o contratante debe establecer por escrito una política de Seguridad y Salud en el Trabajo -SST que debe ser parte de las políticas de gestión de la empresa, con alcance sobre todos sus centros de trabajo y todos sus trabajadores, independiente de su forma de contratación o vinculación. Esta política debe ser comunicada al Comité Paritario de Seguridad y Salud en el Trabajo.

El Artículo 2.2.4.6.6. del Decreto antes citado, señala que los requisitos de la Política de Seguridad y Salud en el Trabajo debe entre otros, cumplir con los siguientes requisitos:

- Establecer el compromiso de la empresa hacia la implementación del SST de la empresa para la gestión de los riesgos laborales;

- Ser específica para la empresa y apropiada para la naturaleza de sus peligros y el tamaño de la organización;

- Ser concisa, redactada con claridad, estar fechada y firmada por el representante legal de la empresa;

- Debe ser difundida a todos los niveles de la organización y estar accesible, a todos los

trabajadores y demás partes interesadas, en el lugar de trabajo; y

- Ser revisada como mínimo una vez al año y de requerirse, actualizada acorde con los cambios tanto en materia de Seguridad y Salud en el Trabajo -SST, como en la empresa.

Así mismo señala el Artículo 2.2.4.6.7, que debe contener unos Objetivos de la Política de Seguridad y Salud en el Trabajo -SST, donde la organización expresa su compromiso así:

- Identificar los peligros, evaluar y valorar los riesgos y establecer los respectivos controles;

- Proteger la seguridad y salud de todos los trabajadores, mediante la mejora continua del Sistema de Gestión de la Seguridad y Salud en el Trabajo SG

- SST en la empresa; y

- Cumplir la normatividad nacional vigente aplicable en materia de riesgos laborales

Dando cumplimiento a lo anterior, se presenta la política del sistema de Gestión de Seguridad y Salud en el Trabajo, actualizada por medio de la resolución 020 de enero de 2016:

POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO

"La Agencia Nacional de Defensa Jurídica del Estado, se compromete con la implementación, desarrollo y fortalecimiento de un Sistema de Gestión de Seguridad y Salud en el Trabajo para sus servidores, contratistas y comunidad que interactúa con la Agencia, dirigido a la prevención de lesiones, accidentes de trabajo y enfermedades laborales, por medio de la identificación y control de los riesgos asociados a sus labores y el cumplimiento de la legislación laboral vigente, enmarcados en un ciclo de mejoramiento continuo.

Así mismo se promoverá una cultura de Seguridad y Salud en el Trabajo, orientada a la generación de ambientes seguros, mediante el desarrollo de actividades destinadas a la promoción de la salud y el bienestar de los servidores y contratistas."

OBJETIVOS: Establézcanse como objetivos del Sistema de Seguridad y Salud en el Trabajo los siguientes:

- Diseñar y establecer los lineamientos para la implementación del Sistema de Gestión de Seguridad y Salud en el Trabajo, en concordancia con las disposiciones legales vigentes, aplicables a la Agencia Nacional de Defensa Jurídica del Estado, con el fin de prevenir lesiones, accidentes de trabajo y enfermedades laborales.

- Establecer y desarrollar, programas y actividades encaminados a la prevención de accidentes y promoción de la salud, el mejoramiento de las condiciones y el medio ambiente de trabajo de los colaboradores.

- Identificar los peligros y valorar los riesgos en Seguridad y Salud en el Trabajo asociados a las labores y establecer medidas de intervención que permitan un control de los mismos.

- Desarrollar el análisis de vulnerabilidad como insumo para elaborar la estrategia en prevención, preparación y respuesta ante emergencias.

RECURSOS. La Agencia se compromete a establecer y asignar los recursos físicos, financieros, tecnológicos y humanos necesarios para la implementación y desarrollo del Sistema de Gestión

de Seguridad y Salud en el Trabajo.

REVISIÓN. La Política de Salud y Seguridad en el Trabajo será revisada al menos una vez al año, para su actualización o confirmación.

DIVULGACIÓN. Comunicar la Política de Salud y Seguridad en el Trabajo, al Comité Paritario de Seguridad y Salud en el Trabajo y a todos los niveles de la organización, a través de los medios de comunicación empleados por la Agencia, como to son: Grupos itinerantes, Intranet, carteleras, correo electrónico, inducción y reinducción y página web.

3.4 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Dando cumplimiento a las directrices establecidas en la Norma Técnica Colombiana NTC ISO 27001:2013, numeral 5.2, la Agencia Nacional de Defensa Jurídica del Estado, al definir su Política de Seguridad de la Información deber dar cumplimiento a los siguientes criterios:

Debe definir una política del Sistema de Gestión de Seguridad de la Información que:

- Sea adecuada al propósito de la Agencia.

- Incluya objetivos de seguridad de la información o proporcione el marco de referencia para el establecimiento de los objetivos de la seguridad de la información.

- Incluya el compromiso de cumplir los requisitos aplicables relacionados con la seguridad de la información

- Incluya el compromiso de mejora continua del sistema de gestión de la seguridad de la información.

- Estar disponible como información documentada

- Comunicarse dentro de la organización

- Estar disponible para las partes interesadas, según sea apropiado

A continuación, se presenta la política y alcance del sistema de gestión de seguridad de la información - SGSI:

POLÍTICA DE SEGURIDAD DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN -SGSI

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de la AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de Información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

La AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Cumplir con los principios de seguridad de la información de acuerdo a lo normatividad ISO 27001 y Ja estrategia GEL del Ministerio de Tecnologías de la Información y las Comunicaciones.

- Apoyar la innovación tecnológica.

- Implementar el sistema de gestión de seguridad de la información, estableciendo las políticas, procedimientos e instructivos en materia de seguridad de la información

- Proteger los activos de información de la AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO.

- Fortalecer la cultura de seguridad de la información en los funcionarios, contratistas y terceros de la AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO.

- Garantizar la continuidad del negocio asegurando los activos de información claves para la entidad.

Alcance/Aplicabilidad

Esta política aplica a todos los procesos, funcionarios, contratistas y terceros de la AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO, y su desarrollo se ejecutará por fases y/o procesos de la Agencia, iniciando por los procesos misionales hasta abarcar la totalidad de los procesos

Este sistema SGSI se integrará a los sistemas que ya existen en la AGENCIA NACIONAL DE DEFENSA JURÍDICA DE EL ESTADO.

Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

A continuación, se establecen las políticas de seguridad que soportan el SGSI para la AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO:

3.4.1 Política de roles y responsabilidades.

Objetivo: Establecer los Roles y Responsabilidades con respecto al Sistema de Gestión de seguridad de la Información - SGSI, con el fin de su adecuada planeación e implementación.

Todos los Colaboradores y terceros autorizados por la Agencia Nacional de Defensa Jurídica del Estado - ANDJE a que accedan a la plataforma tecnológica y de procesamiento de información, son responsables del cumplimiento de las políticas, procedimientos, normas y estándares definidos por la Entidad.

Todos los Colaboradores de la ANDJE no deben divulgar información CONFIDENCIAL o RESERVADA en espacios públicos o privados, mediante conversaciones o situaciones que puedan comprometer la seguridad o el buen nombre de la ANDJE. Esta restricción se debe cumplir inclusive después de la terminación del vínculo laboral y debe estar incluida en los Acuerdos de Confidencialidad establecidos por la entidad.

Todos los activos de Información de la ANDJE deben tener identificado su propietario y su

custodio, y solo los dueños de los procesos, de acuerdo al mapa de procesos de la ANDJE, pueden desempeñar el rol de propietarios de activos de información, por lo cual deben tomar las medidas necesarias para proteger el activo en términos de confidencialidad, integridad, disponibilidad.

Los responsables de Tecnología de la Información y de las Áreas de Gestión Humana, Gestión Contractual y Seguridad de la Información, deben identificar los Roles y Responsabilidades para cada usuario que accede a los sistemas de información e infraestructura tecnológica de la ANDJE, para ello debe crearse un procedimiento formal de solicitud, modificación, eliminación y/o inactivación de privilegios de usuarios.

La Matriz de Roles y Responsabilidades debe ser actualizada periódicamente o cada vez que surja un cambio, de acuerdo a un requerimiento formal por parte del Líder del Proceso.

Los privilegios asignados de acuerdo al rol dentro de la ANDJE deben ser informados al usuario, adicionalmente se debe capacitar sobre el uso y la responsabilidad que implica tener esos privilegios.

La Secretaria General deberá designar los responsables que apoyen y orienten en los diferentes lineamientos relacionados con la seguridad de la información, para ello se deberá contar con responsables da las oficinas de Gestión Documental, Oficina de Planeación, Oficina Asesora Jurídica y Oficina de Tecnología.

El Comité Institucional de Desarrollo Administrativo será el encargado de tomar las decisiones finales en lo que respecta al Sistema de Gestión de Seguridad de la Información.

3.4.2 Política de dispositivos móviles

Objetivo: Determinar los lineamientos para el uso y protección de la información almacenada en los dispositivos móviles institucionales y personales que tengan acceso a la información de la ANDJE.

La ANDJE proveerá los mecanismos para el manejo de los dispositivos móviles institucionales que hagan uso de los servicios de la Agencia entre los cuales encontramos:

Los usuarios deben establecer un método de bloqueo como contraseñas, patrones, biométrico o reconocimiento de voz para que pasado un tiempo de inactividad pasen automáticamente a modo de seguro y, en consecuencia, se active el bloqueo de pantalla el cual requerirá el método de desbloqueo configurado.

Se debe llevar un registro de todos los dispositivos móviles que posee la entidad y el responsable al que se asigna.

Para el caso de los PC portátiles, estos deben permanecer con la guaya asignada, cuando se encuentren en los puestos de trabajo, o en un sitio con riesgo de pérdida del equipo.

Los dispositivos móviles que son propiedad de la ANDJE pueden estar sometidos a un control sobre el tipo y la versión de aplicaciones instaladas, al igual que pueden estar sometidos a restricciones de conexión hacia ciertos servicios de información que sean considerados maliciosos.

Los usuarios de los dispositivos móviles institucionales y personales que hagan uso de

información de la ANDJE, deben garantizar que solo accedan a redes seguras y con la protección adecuada para evitar acceso o divulgación no autorizada de la información almacenada y procesada.

Los dispositivos móviles de propiedad de los Colaboradores solo pueden conectarse a la red de datos de la ANDJE, una vez realicen el procedimiento formal de solicitud de servicios de tecnología.

3.4.3 Política de teletrabajo

Objetivo: Determinar los directrices adecuadas para proteger y asegurar la información que es creada, procesada y almacenada por los colaboradores que operan en modalidad de teletrabajo para la ANDJE.

Los colaboradores que operan en la modalidad de teletrabajo deberán conectarse a través de la VPN suministrada por el proceso de gestión de tecnologías de la información, estableciendo una conexión desde de una red segura y con la protección adecuada, por ningún motivo los colaboradores deberán conectarse a la red de la Agencia a través de redes públicas.

La información creada y procesada en modalidad de teletrabajo deberá ser almacenada en los servidores de la agencia destinados para tal fin, de acuerdo al perfil y área correspondiente del colaborador.

La ANDJE proveerá los mecanismos de cierre de sesión por inactividad del usuario y, en consecuencia, se active el bloqueo de conexión de VPN para que solicite nuevamente el sistema de logueo de usuario.

La ANDJE tiene potestad para verificar las características operativas, de seguridad física, equipos de cómputo y redes de comunicaciones usadas por los colaboradores que se encuentran en modalidad de teletrabajo.

Las conexiones en modalidad de teletrabajo estarán sujetas a verificación o monitoreo, el cual incluye, hora y duración de la conexión, tamaño de datos transmitidos o recibidos desde y hacia la Infraestructura de la ANDJE, direcciones IP de origen de la conexión, entre otros.

La ANDJE brindara el asesoramiento y acompañamiento para la instalación y configuración de los servicios de tecnología necesarias para operar en la modalidad de teletrabajo, garantizando el óptimo y correcto uso de los accesos a la infraestructura de la Agencia.

La ANDJE expedirá una resolución dónde se establearen las normas para promover y regular el teletrabajo.

3.4.4 Seguridad de los recursos humanos

Objetivo: Proteger la información de la ANDJE por medio de la validación, formación y concientización del recurso humano que hará uso de la misma; entendiendo sus responsabilidades y las funciones de sus roles dentro de la Agencia.

Para el caso de los funcionarios, las funciones y responsabilidades en materia de seguridad de la información, serán incorporadas en la descripción de funciones esenciales de los Manual Específico y de Competencias Laborales para los empleados de la planta de personal de la Agencia Nacional de Defensa Jurídica del Estado.

Para el caso de los contratistas, las funciones y responsabilidades en materia de seguridad de la información, serán incorporadas en las obligaciones generales del contratista de los estudios previos contratación servicios profesionales y de apoyo a la gestión de la entidad.

- Acuerdo de Confidencialidad

Todos los Colaboradores que ingresen a laborar con la Agencia Nacional de Defensa Jurídica del Estado - ANDJE, deberán firmar como parte de sus términos y condiciones iniciales de trabajo, un Acuerdo de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información de la entidad, en los términos de la Ley 1581 de 2012 y las demás normas que la adicionen, modifiquen, reglamenten o complementen, así como el Decreto 1377 de 2013. El acuerdo (documento original) debe ser retenido en forma segura por el Área de Talento Humano o el Grupo de Gestión Contractual, según el caso, si tal acuerdo de confidencialidad de la información no estuviere incluido como una cláusula del respectivo contrato de prestación de servicios o en el Acta de Posesión del funcionario.

Así mismo, mediante el acuerdo de confidencialidad el Colaborador declaran conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo.

- Selección de personal

Dentro de los procesos de contratación de personal o de prestación de servicios, debe realizarse la verificación de antecedentes cuando así lo amerite y en los casos que se considere necesario se debe contemplar la realización del estudio de seguridad. Esto aplica especialmente cuando el Colaborador vaya a tener acceso a información de la ANDJE que haya sido clasificada como CONFIDENCIAL o RESERVADA.

Talento humano y contratos son los responsables de realizar la verificación de antecedentes, para lo cual pueden llevará cabo cualquiera de las siguientes actividades: verificación de referencias personales y laborales, validación de la hoja de vida del postulado, confirmación de calificaciones académicas y profesionales, revisión de documentación de identidad alterna (pasaporte, tarjeta de conducción, etc.), revisión de antecedentes disciplinarios y judiciales, etc.

- Entrenamiento, concientización y capacitación

Los Colaboradores de la ANDJE deben ser entrenados y capacitados para las funciones/actividades y cargos a desempeñar, con el fin de proteger adecuadamente los recursos y la información de la institución; y garantizar la comprensión del alcance y contenido de las políticas y lineamientos de Seguridad de la información y la necesidad de respaldarlas y aplicarlas de manera permanente. En los casos en que así se establezca, este entrenamiento deberá extenderse al personal de contratistas o terceros, cuando sus responsabilidades así lo exijan.

- Formación y Capacitación en Materia de Seguridad de la Información

Todos los Colaboradores de la ANDJE y, cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en la entidad, recibirán una adecuada capacitación y actualización periódica en materia de las políticas, normas y procedimientos de la entidad, relacionadas con Seguridad de la Información. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación sobre uso correcto de las instalaciones de procesamientos de información y uso correcto de los recursos tecnológicos informáticos que

provee la entidad para el desempeño de sus funciones laborales.

- Procesos disciplinarios

En lo pertinente a la violación de las políticas de seguridad de la información de la entidad, a los Colaboradores, se les aplicará lo establecido en la ley, particularmente en el Código Único Disciplinario (Ley 734 de 2002), el Estatuto Anticorrupción (Ley 1474 de 2011) y demás normas que las adicionen, modifiquen, reglamenten o complementen.

3.4.5 Política de uso de correo electrónico

Objetivo: Definir pautas generales del buen uso del correo electrónico, con el fin de asegurar una adecuada protección de la información de la ANDJE.

- Usos aceptables del servicio

Debe utilizarse exclusivamente para las actividades propias del desempeño de las funciones laborales a desarrollar en la ANDJE, no debe utilizarse para ningún otro fin, así mismo se debe utilizar de manera ética, razonable, eficiente, responsable, no abusiva y sin generar riesgos para la operación de equipos o sistemas de información de la ANDJE.

Los usuarios autorizados para usar el servicio de correo electrónico son responsables de todas las actividades realizadas con sus credenciales de acceso a los buzones de correo, así como de mantener un comportamiento ético y acorde a la ley (especialmente a la Ley 1273 de 2009 de Delitos Informáticos), y de evitar prácticas o usos que puedan comprometer la seguridad de la información de la ANDJE.

Cuando un Proceso, Programa o Dependencia, tenga información de interés institucional para divulgar, lo debe hacer a través de la Oficina de Comunicaciones de la ANDJE o el medio formal autorizado para realizar esta actividad.

Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por la ANDJE y deberán conservar en todos los casos el mensaje legal corporativo.

El único servicio de correo electrónico controlado en la entidad es el asignado directamente por el proceso de Gestión de Tecnologías de la Información, el cual cumple con todos los requerimientos técnicos y de seguridad.

Todo colaborador es responsable por la destrucción de los mensajes cuyo origen sea desconocido y por lo tanto asumirá la responsabilidad y las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En estos casos no se debe contestar dichos mensajes, ni abrir los archivos adjuntos y se debe notificar a través del sistema de gestión de servicios tecnológicos.

Cuando a un usuario al que le haya sido autorizado el uso de una cuenta de acceso a la red y al servicio de correo corporativo se retire de la ANDJE, el Proceso de Gestión de Tecnología de Información, deberá verificar que los servicios sean cancelados.

Cada usuario se debe asegurar que, en el reenvío de correos electrónicos, la dirección de destino es correcta, de manera que esté siendo enviado a las personas apropiadas. Si tiene listas de distribución se deben depurar en el mismo sentido. El envío de información a personas no autorizadas es responsabilidad de quien envía el mensaje de correo electrónico.

Las cuentas institucionales (Ejemplo: Comunicaciones, atención al ciudadano, Soporte, etc.) deben tener una persona responsable que haga depuración del buzón.

El proceso de Gestión de Tecnologías de la Información se reserva el derecho de filtrar los tipos de archivo que vengan anexos al correo electrónico para evitar amenazas de virus y otros programas destructivos. Todos los mensajes electrónicos serán revisados para evitar que tengan virus u otro programa destructivo.

El usuario no debe responder mensajes donde les solicitan información personal o financiera que indican que son sorteos, ofertas laborales, ofertas comerciales o peticiones de ayuda humanitaria. Por el contrario, debe notificar a través del sistema de gestión de servicios de tecnología, con el fin de ejecutar las actividades pertinentes como bloquear por remitente y evitar que esos mensajes lleguen a más Colaboradores.

Todo mensaje electrónico dirigido a otros dominios debe contener una sentencia o cláusula de confidencialidad.

Todos los usuarios de correo electrónico, tienen como tamaño máximo para recibir o enviar mensajes de 20 MB (incluyendo la suma de todos los adjuntos).

- Usos no aceptables del servicio

Envío de correos masivos que no hayan sido autorizados por un propietario de un proceso misional, estratégico, mejora continua o de apoyo, de acuerdo al mapa de procesos de la ANDJE.

Envío, reenvío o intercambio de mensajes no deseados o considerados como SPAM, cadena de mensajes o publicidad.

Envío o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, racista, o cualquier contenido que represente riesgo de virus.

Envío o intercambio de mensajes que promuevan la discriminación sobre la base de raza, nacionalidad, género, edad, estado marital, orientación sexual, religión o discapacidad, o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluidas el lavado de activos.

Crear, almacenar o intercambiar mensajes que atenten contra las leyes de derechos de autor.

Distribuir o divulgar información de la ANDJE, no PÚBLICA, a otras entidades o ciudadanos sin la debida autorización.

Abrir o hacer uso y revisión no autorizada de la cuenta de correo electrónico de otro usuario sin su autorización.

Adulterar o intentar adulterar mensajes de correo electrónico.

Enviar correos masivos, con excepción de funcionarios con nivel de Director o superior, quienes sean previamente autorizados por estos para ello, o de funcionarios que en calidad de sus funciones amerite la excepción.

Cualquier otro propósito inmoral, ilegal o diferente a los considerados en el apartado "Usos aceptable del servicio" de la presente política.

3.4.6 Política de uso de internet

Objetivo: Establecer los parámetros para el buen uso del internet, con el fin de evitar posibles riesgos informáticos asociados a la navegación dentro las redes de Ja ANDJE.

- Usos aceptables del servicio

La solicitud del servicio de internet, se debe hacer mediante el procedimiento gestión de servicios de tecnología, dicho servicio debe utilizarse exclusivamente para el desempeño de las funciones y actividades desarrolladas durante su contratación en la ANDJE y no debe utilizarse para ningún otro fin.

Los usuarios autorizados para hacer uso del servicio de Internet son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información de la ANDJE.

Todas las comunicaciones establecidas mediante este servicio pueden ser revisadas por el administrador del servicio.

El acceso a internet por cada usuario, depende del rol que desempeñe en la ANDJE y para los cuales este formal y expresamente autorizado.

Todos los usuarios son responsables del uso de sus credenciales de acceso a las cuales les fue otorgado el acceso a internet,

No se permite el acceso a páginas con contenido restringido como pornografía, anonimizadores, actividades criminales y/o terrorismo, crímenes computacionales, hacking, discriminación, contenido malicioso, suplantación de identidad, spyware, adware, redes peer to peer (p2p) o páginas catalogadas como de alto riesgo.

No se permite la descarga, uso, intercambio o instalación de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software de libre distribución, información o productos que atenten contra la propiedad intelectual, archivos ejecutables que comprometan la seguridad de la información, herramientas de hacking, entre otros.

La ANDJE se reserva el derecho de realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los colaboradores. Así mismo, revisar, registrar y evaluar las actividades realizadas durante la navegación.

Todos los usuarios que se encuentren autorizados son responsables de dar un uso adecuado de este recurso y por ninguna razón pueden hacer uso para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente, las políticas de seguridad de la información, la seguridad de la información, entre otros.

Este recurso puede ser utilizado para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de la ANDJE.

La descarga de archivos de Internet debe ser con propósitos laborales y de forma razonable para no afectar el servicio de Internet/Intranet, en forma específica el usuario debe cumplir los requerimientos de la política de uso de internet descrita en este manual.

- Usos no aceptables del servicio

Envío, descarga o visualización de información con contenidos restringidos y que atenten contra la integridad moral de las personas o instituciones.

Cualquier otro propósito diferente al considerado en el apartado de Usos aceptables del servicio de la presente política.

3.4.7 Política de clasificación de la información

Objetivo: Asegurar que la información de la ANDJE está clasificada y etiquetada, con el fin de que sea tratada y protegida adecuadamente.

Esquema de Clasificación de la Información

Toda la información de la ANDJE debe ser Identificada y clasificada de acuerdo a los niveles de clasificación definidos por la entidad.

El proceso de Gestión de Tecnologías de la Información, Proceso de Gestión Documental y el Proceso de Gestión Legal son los responsables de definir las directrices de clasificación de la información y las medidas de tratamiento y manejo de la información.

De acuerdo a la clasificación establecida por la entidad y el manejo y almacenamiento de la Información, se debe tener en cuenta lo siguiente:

Acceso a la información sólo de personal autorizado.

Llevar un registro formal de acceso a la información que se maneja desde Gestión Documental, y los sistemas Orfeo y Ekogui.

Conservar y mantener los medios de almacenamiento de información en un ambiente seguro.

- Etiquetado y manejo de Información

Todos los Colaboradores y terceros cuando sea el caso, deben mantener organizado el archivo de gestión, siguiendo los lineamientos establecidos por el Proceso de Gestión Documental.

Los Directores, Jefes de Oficina, Coordinadores de Grupo deben establecer mecanismos de control de documentos, con el fin de garantizar y mantener la disponibilidad, integridad y confidencialidad de la información.

Todos los Colaboradores y terceros cuando sea el caso de la ANDJE son responsables de la organización, conservación, uso y manejo de los documentos.

La plataforma tecnológica usada para salvaguardar, conservar y facilitar la información de los documentos en medios magnéticos, debe garantizar los principios fundamentales de la seguridad como son la integridad, confidencialidad y disponibilidad de la información.

- Usos no aceptables

Dañar o dar como perdido los expedientes, documentos o archivos que se encuentren bajo su administración por la naturaleza de su cargo.'

Divulgación no autorizada de los expedientes, documentos, información o archivos. Realizar actividades tales como borrar, modificar, alterar o eliminar información de la ANDJE de manera

malintencionada.

3.4.8 Política de control de acceso

Objetivo: Definir las directrices generales para asegurar el acceso controlado, lógico y físico a la información de la plataforma tecnológica y de información de la ANDJE. Control de Acceso a Redes y Servicios en Red

El ANDJE suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible. Es responsabilidad del usuario el manejo que se les dé a las claves asignadas.

Solo personal designado por el Proceso de Tecnologías de la Información está autorizado para instalar software o hardware en los equipos, servidores e infraestructura de tecnología de la ANDJE.

Toda actividad que requiera acceder a los servidores, equipos o a las redes de la ANDJE, se debe realizar en las instalaciones. No se debe realizar ninguna actividad de tipo remoto sin la debida autorización del Proceso de Tecnologías de la Información.

La conexión remota a la red de área local de la ANDJE debe ser establecida a través de una conexión VPN segura aprovisionada por la entidad, la cual debe ser autorizada por el Proceso de Tecnologías de la Información, que cuenta con el monitoreo y registro de las actividades necesarias.

Mediante el registro de eventos en los diversos componentes de la plataforma tecnológica, se efectúa el seguimiento a los accesos realizados por los usuarios, con el fin de minimizar los riesgos de pérdida de integridad, disponibilidad y confidencialidad de la información.

No se permite la conexión de módems externos o internos en la red de la ANDJE, previa solicitud autorizada por el proceso de Gestión de Tecnologías de la Información a través del sistema de gestión de servicios de tecnología.

- Gestión de Acceso a Usuarios

La creación y retiro de usuarios en los sistemas de información en producción debe seguir un procedimiento de Creación, Edición y Eliminación de Usuarios.

Los usuarios pueden elegir y cambiar sus claves de acceso periódicamente, inclusive antes de que la cuenta expire, estas contraseñas deben contener mayúsculas, minúsculas, números y por lo menos un carácter especial, de una longitud mayor a 8 caracteres y no reutilizar la misma contraseña hasta 10 anteriores. Lo anterior aplica para los sistemas que se autentican con el LDAP.

El sistema debe obligar a los colaboradores a cambiar la contraseña por lo mínimo 1 vez cada 45 días, todos los usuarios en su primer inicio de sesión deben cambiar las contraseñas suministrada por la mesa de servicios. Lo anterior aplica para los sistemas que se autentican con el LDAP.

Todos los colaboradores deben dar buen uso a las claves de acceso suministradas y no deben escribirlas o dejarlas a la vista, almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional.

Se debe cambiar todas las claves de acceso que vienen predeterminadas por el fabricante, una vez instalado y configurado el software y el hardware (por ejemplo, appliance, impresoras, routers, switch, herramientas de seguridad, etc.).

Los colaboradores No deben prestar, divulgar o difundir la contraseña de acceso asignadas a compañeros, Jefes u otras personas que lo soliciten.

Todos los usuarios deben dar cumplimiento a Las políticas de seguridad de la información de uso y selección de las contraseñas de acceso, por lo tanto, son responsables de cualquier acción que se realice utilizando el usuario y contraseña asignados.

Reportar a través del sistema de gestión de servicios de tecnología sobre cualquier incidente o sospecha de que otra persona esté utilizando su contraseña o usuario asignado.

Las contraseñas de acceso a los servidores y administración de los Sistemas de Información deben ser cambiadas mínimo cada cuatro (4) meses.

El acceso a Bases de Datos, Servidores y demás componentes tecnológicos de administración de la Plataforma y Sistemas de Información, debe estar autorizado por et Proceso de Tecnologías de la Información.

- Revisión de los derechos de acceso de los Usuarios

Los derechos de acceso de los usuarios a la información y a la Plataforma Tecnológica y de procesamiento de información de la ANDJE, debe ser revisada periódicamente y cada vez que se realicen cambios de personal en los procesos o grupos de trabajo.

- Retiro de los derechos de acceso

Cada uno de los procesos de la Entidad y supervisores de contratos son responsables de comunicar a la Oficina de Talento Humano y Gestión Contractual, el cambio de cargo, funciones o actividades o la terminación contractual de los Colaboradores pertenecientes al proceso. La Oficina de Talento Humano y Gestión Contractual son las encargadas de comunicar al Proceso de Tecnologías de la Información a través del sistema de gestión de servicios de tecnología sobre estas novedades, con el fin de retirar los derechos de acceso a los servicios informáticos y de procesamiento de información.

3,4.9 Política seguridad física y del entorno

Objetivo: Adoptar los mecanismos necesarios en términos de seguridad física y del entorno con el fin de evitar accesos físicos no autorizados a las instalaciones de procesamiento de información, que atenten contra la confidencialidad, integridad o disponibilidad de la Información de la ANDJE.

- Perímetro de Seguridad Física

Todas las entradas que utilizan sistemas de control de acceso deben permanecer cerradas y es responsabilidad de todos los Colaboradores y terceros autorizados evitar que las puertas se dejen abiertas.

Todos los colaboradores sin excepción deben portar su carnet en un lugar visible mientras permanezcan dentro de las instalaciones de la ANDJE.

Los visitantes deben permanecer acompañados de un colaborador de la ANDJE, cuando se encuentren en las oficinas o áreas donde se maneje información.

Es responsabilidad de todos los Colaboradores de la ANDJE borrar la Información escrita en los tableros o pizarras al finalizar las reuniones de trabajo. Igualmente, no se debe dejar documentos o notas escritas sobre las mesas al finalizar las reuniones.

Los visitantes que requieran permanecer en las oficinas de la ANDJE por periodos superiores a dos (2) días deben ser presentados al personal de oficina donde permanecerán.

El horario autorizado para recibir visitantes en las instalaciones de la ANDJE es de 8:00 AM a 5:00 PM. En horarios distintos se requerirá de la autorización del Director, Jefe de Oficina o Coordinador del Grupo correspondiente.

Los dispositivos removibles, así como toda información CONFIDENCIAL de la ANDJE, independientemente del medio en que se encuentre, deben permanecer guardados bajo seguridad durante horario no hábil o en horarios en los cuales el Colaborador responsable no se encuentre en su sitio de trabajo.

Las instalaciones de la ANDJE deben estar dotadas de un circuito cerrado de TV con el fin de monitorear y registrar las actividades de colaboradores, terceros y visitantes.

- Controles de Acceso Físico

Las áreas seguras, dentro de las cuales se encuentran el Centro de Datos, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, deben contar con mecanismos de protección física y ambiental, y controles de acceso adecuados para la protección de la información.

En las áreas seguras, bajo ninguna circunstancia se puede fumar, comer o beber.

Las actividades de limpieza en las áreas seguras deben ser controladas y supervisadas por un colaborador del proceso. El personal de limpieza se debe capacitar acerca de las precauciones mínimas a seguir durante el proceso de limpieza y se prohíbe el ingreso de maletas, bolsos u otros objetos que no sean propios de las tareas de aseo.

- Ubicación y Protección de los equipos.

La plataforma de infraestructura tecnológica (Hardware, software y comunicaciones) debe contar con las medidas de protección física y eléctrica, con el fin de evitar daños, fraudes, interceptación de la información o accesos no autorizados.

Se debe instalar sistemas de protección eléctrica en el centro de cómputo y comunicaciones de manera que se pueda interrumpir el suministro de energía en caso de emergencia. Así mismo, se debe proteger la infraestructura de procesamiento de información mediante contratos de mantenimiento y soporte.

- Seguridad de los equipos fuera de las instalaciones

Los equipos portátiles no deben estar a la vista en el interior de los vehículos. En casos de viaje siempre se debe llevar como equipaje de mano.

En caso de pérdida o robo de un equipo portátil se debe Informar inmediatamente al Proceso de

Gestión Administrativa y Tecnologías de la Información y debe poner la denuncia ante las autoridades competentes y debe hacer llegar copia de la misma.

Cuando los equipos portátiles se encuentren desatendidos deben estar asegurados con una guaya, dentro o fuera de las instalaciones de la ANDJE.

Para el caso de los equipos que cuentan con puertos de transmisión y recepción de Infrarrojo y Bluetooth estos deben estar deshabilitados.

Todos los equipos de cómputo deben ser registrados al ingreso y al retirarse de las instalaciones de la ANDJE.

- Seguridad en la reutilización o eliminación de los equipos

Cuando un equipo de cómputo sea reasignado o dado de baja, se debe realizar una copia de respaldo de la información que se encuentre almacenada. Posteriormente debe ser sometido la guía de borrado seguro de la información, con el fin de evitar pérdida de la información o recuperación no autorizada de la misma.

- Retiro de Activos

Ningún equipo de cómputo, información o software debe ser retirado de la ANDJE sin una autorización formal.

Se debe realizar periódicamente comprobaciones puntuales para detectar el retiro no autorizado de activos de la ANDJE.

3.4.10 Política de escritorio despejado y pantalla despejada

Objetivo: Definir los lineamientos generales para mantener el escritorio y la pantalla despejada, con el fin de reducir el riesgo de acceso no autorizado, pérdida y daño de la información de la ANDJE.

Todo el personal de la ANDJE debe conservar su escritorio libre de información propia de la entidad, que pueda ser copiada, utilizada o estar al alcance de terceros o por personal que no tenga autorización para su uso o conocimiento.

Todo el personal de la ANDJE debe bloquear la pantalla de su equipo de cómputo cuando no estén haciendo uso de ellos o que por cualquier motivo deban dejar su puesto de trabajo.

Todos los usuarios al finalizar sus actividades diarias, deben salir de todas las aplicaciones y apagar las estaciones de trabajo. Exceptuando el personal que por sus labores deba dejar su estación de trabajo encendida (Desarrolladores y Profesionales de Infraestructura Tecnológicas).

Al imprimir documentos de carácter CONFIDENCIAL, estos deben ser retirados de las impresoras inmediatamente. Así mismo, no se deben reutilizar papel que contenga información CONFIDENCIAL.

En horario no hábil o cuando los lugares de trabajo se encuentren desatendidos, los usuarios deben dejar Ja información CONFIDENCIAL protegida bajo llave.

3.4.11 Política de separación de ambientes de desarrollo, pruebas y producción

Objetivo: establecer los mecanismos necesarios que aseguren la separación de ambientes de desarrollo, pruebas y producción, con el fin de Reducir riesgos asociados a modificaciones, alteraciones, cambios o accesos no autorizados en sistemas en producción de la ANDJE.

La ANDJE debe establecer y mantener ambientes separados de Desarrollo, Pruebas y Producción, dentro de la infraestructura de Desarrollo de Sistemas de Información de la Entidad. Esto aplica para sistemas que contengan información catalogada con criticidad alta de acuerdo al inventario y clasificación de activos de información.

El ambiente de desarrollo se debe utilizar para propósitos de implementación, modificación, ajuste y/o revisión de código. Por su parte, el ambiente de pruebas se debe utilizar para realizar el conjunto de validaciones funcionales y técnicas del software, aplicación o sistema de información, teniendo como base los criterios de aceptación y los requerimientos de desarrollo. Por último, el ambiente de producción debe utilizarse para la prestación de un servicio que involucra el manejo de datos reales y que tiene un impacto directo sobre las actividades realizadas como parte de un proceso de la entidad.

No se deben realizar pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción. Esto puede conducir a fraude o inserción de código malicioso.

En los ambientes de desarrollo y pruebas no se deben utilizar datos reales del ambiente de producción, sin antes haber pasado por un proceso de ofuscamiento.

Se debe restringir el acceso a compiladores, editores y otros utilitarios del sistema operativo en el ambiente de producción, cuando no sean indispensables para el funcionamiento del mismo.

Se deben utilizar controles de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas.

Los ambientes deben estar claramente identificados, para evitar así confusiones en la aplicación de tareas o en la ejecución de procesos propios de cada uno.

3.4.12 Política de protección contra código malicioso

Objetivo: Definir las medidas de prevención, detección y corrección frente a las amenazas causadas por códigos maliciosos en la ANDJE.

La ANDJE deberá asegurar que la infraestructura de procesamiento de información de la ANDJE, cuenta con un sistema de detección y prevención de intrusos, herramienta de Anti-Spam, antivirus y sistemas de control de navegación, con el fin de asegurar que no se ejecuten virus o códigos maliciosos.

Se debe restringir la ejecución de aplicaciones y mantener instalado y actualizado el antivirus, en todas las estaciones de trabajo y servidores de la ANDJE.

Se debe restringir la ejecución de código móvil, aplicando políticas a nivel de sistemas operativos, navegadores y servicio de control de navegación.

Todos los Colaboradores y terceros que hacen uso de los servicios de tecnología de la información y comunicaciones de la ANDJE son responsables del manejo del antivirus para analizar, verificar y (si es posible) eliminar virus o código malicioso de la red, el computador, los dispositivos de almacenamiento fijos, removibles, archivos, correo electrónico que estén

utilizando para et desempeño de sus funciones laborales.

Los equipos de terceros que son autorizados para conectarse a la red de datos de la ANDJE deben tener antivirus y contar con las medidas de seguridad apropiadas.

Se debe hacer revisiones y análisis periódicos del uso de software no malicioso en las estaciones de trabajo y servidores. La actividad debe ser programada de forma automática con una periodicidad semanal y su correcta ejecución y revisión estará a cargo del proceso de Gestión de Tecnologías de la Información.

Los Colaboradores de la ANDJE pueden iniciar en cualquier momento un análisis bajo demanda de cualquier archivo o repositorio que consideren sospechoso de contener software malicioso. En cualquier caso, los Colaboradores siempre podrán consultar al proceso de Gestión de Tecnologías de la Información sobre el tratamiento que debe darse en caso de sospecha de malware.

Los usuarios no podrán desactivar o eliminar la suite de productos de seguridad, incluidos los programas antivirus o de detección de código malicioso, en los equipos o sistemas asignados para el desempeño de sus funciones laborales.

El único servicio de antivirus autorizado en la entidad es el asignado directamente por el proceso de Gestión de Tecnologías de la Información, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para evitar ataques de virus, spyware y otro tipo de software malicioso. Además, este servicio tiene diferentes procesos de actualización que se aplican de manera periódica y segura. Excepcionalmente se podrá realizar la ejecución de otro programa antivirus, únicamente por personal autorizado por el proceso de Gestión de Tecnologías de la Información, a efectos de reforzar el control de presencia o programación de virus o código malicioso.

El proceso de Gestión de Tecnologías de la Información se reserva el derecho de filtrar los contenidos que se trasmitan en la red de la ANDJE, con el fin de evitar amenazas de virus.

3.4.13 Política de backup

Objetivo: Establecer los medios y mecanismos para asegurar el respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba periódicamente con el fin de garantizar la continuidad de los mismos.

El proceso de Gestión de Tecnologías de la Información, debe realizar periódicamente un análisis de las necesidades del negocio para determinar la información critica que debe ser respaldada y la frecuencia con que se debe realizar.

EL proceso de Gestión de Tecnologías de la Información y el responsable de Seguridad de la Información junto a los propietarios de la información deben determinar los requerimientos para respaldar la Información y los datos en función de su criticidad, para lo cual se debe elaborar y mantener el inventario de activos de TI.

EL proceso de Gestión de Tecnologías de la Información debe disponer y controlar la ejecución de las coplas, así como la prueba periódica de su restauración. Para esto se debe contar con infraestructura de pruebas de restauración que garanticen la disponibilidad de toda la información y del software crítico de la ANDJE.

Se debe definir y documentar un esquema de respaldo de la información. El dueño de la información es responsable de definir claramente el periodo de retención de respaldos, en función de los requerimientos de las áreas funcionales.

Se debe verificar periódicamente, la integridad de las copias de respaldo que se están almacenando, con el fin de garantizar la integridad y disponibilidad de la información.

Se deben definir lineamientos para el respaldo de la información, que incluyan los siguientes parámetros:

Definir el protocolo de reemplazo de los medios de almacenamiento de copias de respaldo, una vez terminada la posibilidad de ser reutilizados de acuerdo a lo indicado por el proveedor, y asegurar la destrucción de los medios de información retirados o desechados.

Almacenar en una ubicación remota o externa las copias de respaldo recientes de información, junto con registros completos de las mismas y su plan de restauración.

Se deben asignar los niveles de protección física y ambiental adecuada a la información de respaldo según las normas aplicadas y las especificaciones dadas por el fabricante.

Se deben extender los mismos controles de seguridad aplicados a los activos de TI en el sitio principal al sitio alterno.

El proceso de Gestión de Tecnologías debe:

Efectuar las copias de información de los Servidores, cada vez que se realice un cambio significativo en los Sistemas Operativos o configuraciones Básicas.

Realizar una copia de respaldo diferencial diaria de los Servidores de Base de Datos, servidores Web, Sistemas de Información misionales.

Realizar un respaldo completo semanalmente de los Servidores de Base de Datos, servidores Web, Sistemas de Información, Aplicaciones, Desarrollo y dispositivos de red.

- Registro de Respaldo de Información

Debe existir una bitácora de administración y control de copias de respaldos que permita conocer qué información está respaldada y almacenada en las bóvedas de seguridad del sitio externo.

El proceso de Gestión Tecnologías debe aplicar la siguiente Normativa:

- Llevar el registro de los Respaldos de Información realizada de forma Diaria.

- Registro del retiro de las cintas de Backup del sitio externo.

- Registro del ingreso de las cintas de Backup al sitio externo.

- Inventario de cintas de Backup.

- Comprobación de Integridad de la Información.

La información respaldada debe ser probada como mínimo dos veces al año y se debe tomar muestras aleatorias, asegurando que es confiable, integra y que se estará disponible en el evento que se requiera para su utilización en casos de emergencia.

Se debe disponer de un inventario para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información.

El proceso de Gestión de Tecnologías de la Información, a través del Administrador de la Base de Datos, de Red y Servidores, debe aplicar los siguientes lineamientos: Restaurar por lo menos anualmente, el escenario adecuado para probar las copias de respaldo de los Servidores.

Configurar la herramienta de ejecución de copias de respaldo para que automáticamente registre el éxito o errores en la ejecución.

- Respaldo de Información para Usuarios Finales

Todos los usuarios deben almacenara información resultado de sus actividades laborales en la carpeta "Documentos" a la cual se realiza back-up.

Todos los usuarios son responsables de realizar Jos respaldos de información personal almacenada en los equipos asignados.

Ningún usuario puede realizar copias de respaldo en sus dispositivos de almacenamiento removibles personales, ya que esto puede ser denominado como fuga de información.

Es responsabilidad todos los Colaboradores almacenar la información crítica asociada con su labor en el servidor de archivos establecido, para garantizar que la información está siendo respaldada.

La información almacenada en los equipos de cómputo asignados para et desempeño de las funciones laborales, es propiedad de la ANDJE y cada usuario es responsable por proteger su integridad, confidencialidad y disponibilidad.

3.4.14 Políticas específicas gestión financiera

- Consideraciones Generales

-Ningún usuario de gestión financiera debe permitir que los técnicos de Sistemas realicen operaciones en los computadores sin su presencia.

-Ningún funcionario debe permanecer cerca del módulo de la Tesorera mientras está realizando operaciones en SIIF Nación o en el portal de la DIAN.

-Ningún funcionario debe dejar documentos sobre los escritorios del Grupo Financiero mientras éstos se encuentren ausentes.

Información Financiera

-Los colaboradores que hacen parte del Grupo de Gestión Financiera deberán ser responsables con el uso de la información contenida en el SIIF Nación y con la información que se produce al interior del proceso.

-Los colaboradores deberán propender por la oportunidad, veracidad, confiabilidad, confidencialidad e integridad de los datos que registra en el sistema SIIF Nación y a los que tiene acceso.

-Se considera falta grave: alterar, falsificar, introducir y borrar información del SIIF Nación.

-Se considera falta grave: Permitir voluntariamente el uso de su usuario del SIIF Nación tanto a un colaborador del área Financiera como a un tercero.

-Se debe ser cuidadoso con la información que genera el SIIF Nación, especialmente con los reportes que muestren información de los beneficiarios del sistema, en lo referente a cuentas bancarias e información que pueda ser utilizada por otras personas para hacer daño.

-Así mismo, ser cuidadoso con la papelería que se imprime como certificados de disponibilidad presupuestal, registros presupuéstales, para evitar intentos de fraude con modelos similares a los que genera el SIIF Nación.

-El grupo de Gestión Financiera deberá listar los documentos que se impriman del SIIF y que deben estar firmados por la Coordinadora del Grupo.

- Acceso al SIIF Nación

-Para ingresar al SIIF Nación los colaboradores solo podrán hacerlo utilizando la página WEB del Ministerio de Hacienda y el icono que identifica a SIIF Nación o el portal señalado (https://portal2.siifnacion.qov.co/dana-na/auth/url 39/welcome.cqi)

-No se debe utilizar páginas distintas a las indicadas por la Administración de SIIF Nación, para evitar ser engañado.

-Utilizar el sistema desde el computador de la entidad, no debe realizar transacciones desde computadores o lugares públicos, como cafés Internet, equipos o conexiones a internet desconocidos.

-Una vez haya ingresado al Sistema, si se va a ausentar ciérrelo, active el protector de pantalla con contraseña para bloquear el acceso a su equipo.

-Todo usuario debe ingresar con certificado digital y los correos, direcciones y teléfonos que provea a SIIF Nación deben ser de la entidad.

- Control de Usuarios SIIF

-La creación de usuario requiere el registro en el sistema y el envío de los documentos soporte solicitados al administrador de SIIF debidamente radicados en el Ministerio de Hacienda.

-Un usuario se puede inactivar o eliminar, si el usuario no utiliza SIIF en 15 días calendario el sistema crea una solicitud y lo expira. La entidad debe estar pendiente de las fechas de expiración de los usuarios.

-Si el usuario no ingresa a SIIF durante 3 meses, el sistema lo elimina y se debe realizar todo el procedimiento de creación de usuario para que vuelva a ingresar.

-Se debe solicitar al coordinador SIIF de la Entidad, Ja suspensión temporal o definitiva de su cuenta de usuario, cuando ocurran novedades de personal como retiro temporal (licencias, vacaciones), retiro definitivo, cambio de funciones, traslados del funcionario o cualquier otro evento que lo amerite.

- Certificado y Firma digital

-El dispositivo utilizado para el certificado digital es personal e intransferible, no se puede prestar y siempre debe estar mantenido bajo custodia del usuario.

-La firma digital es un mecanismo para garantizar la identidad de quien genera Ja información, la integridad (que la información generada no haya sido alterada) y el no repudio (no negación de quien originó los registros) de los registros realizados en el sistema tiene efectos legales establecidos en la Ley 527 de 1999 y demás normas que las complementen, modifiquen o remplacen.

-Cada usuario debe solicitar la revocación del certificado a la autoridad certificadora que lo emitió, cuando deje de requerir el uso del mismo, por ejemplo, cuando se retira de la entidad, cuando se pierda o dañe o bloquee el TOKEN criptográfico, o por alguno de los motivos de revocación establecidos por la entidad certificadora y a su vez se debe informar al Coordinador de Gestión Financiera de toda la gestión respecto al tema.

-El certificado digital utilizado en el SIIF Nación se almacena en dispositivos denominados TOKEN criptográficos, los cuales protegen el acceso no autorizado al certificado digital. El TOKEN criptográfico y su contraseña de acceso (PIN) son personales e intransferibles. No se debe prestar ni revelar su contraseña (PIN) de acceso a ninguna persona, se debe mantener siempre bajo poder del usuario y guardado de manera segura. No lo deje conectado al computador cuando se ausente.

- Reporte incidente de seguridad de Ja información

-Cuando se reciban llamadas o correos electrónicos que soliciten información de contraseña o información contenida en el sistema, que no correspondan a los correos oficiales de SIIF Nación cuyo dominio es @minhacienda.gov.co se deben reportar al responsable de seguridad de información de la Agencia, así como a SIIF Nación en el Ministerio de Hacienda y Crédito Público al teléfono 6021270 en Bogotá.

- Confidencialidad de la Información Financiera

-La información a la que se tiene acceso debe ser utilizada exclusivamente para el cumplimiento de sus funciones.

-Sea cuidadoso con el uso de la contraseña de acceso, recuérdela, no la preste, no la escriba en papeles o archivos que puedan ser vistos o accedidos por otras personas, no la escriba delante de otras personas, recuerde que la contraseña es de uso personal e intransferible.

- Contraseñas

-Para SIIF, es recomendable cambiar la clave con frecuencia o cuando perciba que la saben otras personas, puede hacerlo utilizando la funcionalidad de cambio de contraseña que está en la parte superior derecha de la pantalla del menú principal del sistema.

-La contraseña de acceso protege el acceso al sistema de personas no autorizadas, sea responsable con el uso de la misma. Por ejemplo, puede generarla a partir de una frase que recuerde, utilice contraseñas diferentes a las usadas en redes sociales, correo electrónico personal (Hotmail, Gmail, etc.), u otros sitios personales, evite el uso de claves triviales, tales como fechas o aniversarios, placas del auto, nombres de parientes, etc.

3.5 POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

En atención a los criterios que respecto a la gestión de los riesgos establece las metodologías expedidas por el Departamento Administrativo de la Función Pública-DAFP, las orientaciones dadas por la Secretaría de Transparencia de la Presidencia de la República en torno a los riesgos de corrupción, a través de la Ley 1474 de 2011 y que la política de administración de riesgos debe establecer la orientación que la entidad debe tomar respecto a las opciones de tratamiento y manejo de los efectos que pueda generar la materialización de los riesgos al interior y como esta materialización puede afectar el logro de los objetivos institucionales.

La ANDJE adoptó la metodología definida por el Departamento Administrativo de la Función Pública-DAFP e incorporada en el Modelo Estándar de Control Interno - MECI y la Guía de Administración del Riesgo. Al Interior de la entidad se establecieron las directrices para la administración del riesgo en la Guía de Administración de Riesgos de la ANDJE, que incluye: identificación, análisis, valoración de riesgos y la selección de las políticas de administración de los mismos, las cuales están definidas de la siguiente manera[4]:

a. Evitar el riesgo

Tomar las medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se genera cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas. Un ejemplo de esto puede ser el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.

b. Reducir el riesgo

Implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Se consigue mediante la optimización de los procedimientos y la implementación de controles.

Según lo definido Decreto 124 de 2016 expedido por el Departamento Administrativo de la Presidencia, la Función Pública y el Departamento Nacional de Planeación, señala como metodología para diseñar y hacer seguimiento a la estrategia de lucha contra la corrupción y de atención al ciudadano de que trata el artículo 73 de la Ley 1474 de 2011, la establecida en el Plan Anticorrupción y de Atención al Ciudadano contenida en el documento "Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano", para el caso de los riesgos de corrupción, las únicas opciones de tratamiento a seleccionar son Eliminar o Reducir, y se deben tomar acciones orientadas a reducir la materialización del riesgo.

c. Compartir o transferir

Reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Es así como, por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar.

d. Asumir

Luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el gerente del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

Aquellos riesgos que después de la valoración con controles hayan quedado ubicados en una zona de riesgo "Alta" o "Extrema", deberán contar con un plan de mejoramiento enfocado en la reducción de la calificación del mismo hasta dejarlo como mínimo en una zona de riesgo moderada.

Para aquellos riesgos que puedan afectar los productos o servicios generados por la agencia, el Comité Institucional de Desarrollo Administrativo debe efectuar la evaluación y priorización de los mismos para adelantar las acciones correspondientes.

3.5.1 Objetivo para la administración del riesgo

Implementar mecanismos que faciliten el monitoreo de los riesgos en la ANDJE, con el fin de apoyar el cumplimiento de los objetivos institucionales.

Estrategias para la administración del riesgo, las acciones a implementar para la administración del riesgo

- Elaborar y mantener actualizadas las metodologías y demás documentos necesarios para la documentación, monitoreo y mejora continua de los riesgos identificados.

- Capacitar a los enlaces de las dependencias en temas relacionados con administración de riesgos y divulgar aspectos generales a todos los servidores para fomentar cultura de autocontrol.

Las acciones a implementar para la administración del riesgo y los seguimientos a efectuar, están detallados en el documento Guía de Administración de Riesgos de la ANDJE MC-G-02.

3.6 POLÍTICA DE CONSERVACIÓN DOCUMENTAL - SIC

Para Garantizar la conservación y preservación de cualquier tipo de información, independientemente del medio o tecnología con la cual se haya elaborado, manteniendo atributos tales como unidad, integridad autenticidad, inalterabilidad, originalidad, fiabilidad, accesibilidad, de todos los documentos de la Agencia Nacional de Defensa Jurídica desde el momento de la producción o recepción, durante su período de vigencia y hasta su disposición final, se ha definido la política de conservación documental - SIC, la cual está contenida en el documento GD-PL-02, el cual puede ser consultado en la herramienta del sistema integrado de gestión institucional.

3.7 POLÍTICA DE GESTIÓN DOCUMENTAL

Esta política se definió e incorporó en el Programa de Gestión Documental 2014-2018 de la Entidad, para lo cual se tuvieron en cuenta las directrices definidas en el Decreto 1080 de 2015, en el cual se establecen los componentes mínimos que debe incorporar. A continuación, se presenta la Política de Gestión Documental de la Agencia:

POLÍTICA DE GESTIÓN DOCUMENTAL DE LA AGENCIA

La ANDJE está orientada a la gestión de la información física y electrónica, la implementación de estándares para la información y la documentación en cualquier soporte; al uso de

metodologías para la creación, uso, mantenimiento, retención, acceso y preservación de la información; la implementación del Programa de Gestión Documental; y la cooperación, articulación y coordinación permanente entre las dependencias, otros programas y sistemas a fines, y los productores de la información de la Agencia.

Los siguientes son los lineamientos generales de la política de gestión documental de la Agencia:

1. Gestión de la información física y electrónica.

La Agencia adoptará modelos de gestión para la formación física y electrónica, nacionales o internacionales homologados para Colombia por el Archivo General de la Nación, el Ministerio de Tecnologías de la Información y de las Comunicaciones, y/o el Instituto Colombiano de Normas Técnicas y Certificación - ICONTEC.

2. Estándares para la gestión de la información en cualquier soporte.

La Agencia adoptará estándares para la gestión de la información en cualquier soporte, nacionales o internacionales homologados para Colombia por el Archivo General de la Nación, el Ministerio de Tecnologías de la Información y de las Comunicaciones, y/o el Instituto Colombiano de Normas Técnicas y Certificación - ICONTEC.

3. Metodología general.

La Agencia analizará e identificará y aplicará las mejores prácticas en la creación, uso, mantenimiento, retención, acceso y preservación de la información, independiente de su soporte y medio de creación.

4. Programa de gestión de la información y documentos - PGD

La Agencia diseñará e implementará el Programa de Gestión Documental _ PGD como una estructura normalizada y herramienta de planificación estratégica a corte, mediano y largo plazo, debidamente soportado en diagnósticos, cronograma de implementación y recursos presupuéstales.

5. Cooperación, articulación y coordinación.

La Agencia fomentará la cooperación, articulación y coordinación permanente entre las áreas de tecnología, la oficina de Archivo, la Oficina Asesora de Planeación, los productores de la Información, y con otros programas y sistemas que permitan mejorar y complementar la gestión documental.

3.8 POLÍTICA EDITORIAL DEL SITIO WEB DE LA AGENCIA

La política establece los lineamientos de Política Editorial, que regirá la elaboración y publicación de contenidos en la página Web de la Agencia y que serán de uso obligatorio de todos los funcionarios y contratistas y aplican para todos los procesos y dependencias de la Entidad, está contenida en el documento GIC-PL-01, el cual puede ser consultado en la herramienta del sistema integrado de gestión institucional.

3.9 POLÍTICA AMBIENTAL

La Agencia Nacional de Defensa Jurídica del Estado promulga y apoya las diferentes actividades orientadas a la sostenibilidad y/o sustentabilidad del Ambiente, instaurando como prioritario el

cumplimiento de los requisitos legales, el control, prevención y mitigación de los impactos ambientales mediante la gestión sostenible de sus actividades, un consumo eficiente de los recursos y la promoción de buenas prácticas ambientales apuntadas al mejoramiento continuo del desempeño ambiental.

<NOTAS DE PIE DE PÁGINA>.

1. Decreto 4085 de 2011, Artículo 1.

2. Decreto 4085 de 2011, Artículo 2.

3. Decreto 1499 de 2017, Artículo 2.2.22.2.1.

4. Guía para la Administración del Riesgo, Departamento Administrativo de la Función Pública.

Disposiciones analizadas por Avance Jurídico Casa Editorial Ltda.
Normograma de la Administradora Colombiana de Pensiones - Colpensiones
ISSN 2256-1633
Última actualización: 31 de agosto de 2019