Agencia Nacional de Defensa Jurídica del Estado

MANUAL DE POLÍTICAS INSTITUCIONALES Y DE DESARROLLO ADMINISTRATIVO

UNIDAD ADMINISTRATIVA ESPECIAL
AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO
MAYO DE 2016

TABLA DE CONTENIDO

OBJETIVO

Proporcionar directrices para facilitar la formación de las Políticas de Desarrollo Administrativo en la Agencia Nacional de Defensa Jurídica del Estado-ANDJE, de ahora en adelante, atendiendo la normativa vigente y garantizando su correcta alineación con la Planeación Institucional.

ALCANCE

Este documento define las políticas institucionales y de desarrollo administrativo dando cumplimiento a los requerimientos normativos que rigen la gestión de la entidad y el cumplimiento de las normas técnicas aplicables. Los criterios aquí establecidos deben ser aplicados por todos los Servidores Públicos de la ANDJE en el desarrollo de sus funciones.

DEFINICIONES

Políticas de Desarrollo Administrativo: Conjunto de lineamientos que orientan a las entidades en el mejoramiento de su gestión para el cumplimiento de las metas institucionales y de Gobierno, a través de la simplificación de procesos y procedimientos internos, el aprovechamiento del talento humano y el uso eficiente de los recursos administrativos, financieros y tecnológicos[1].

Política del Sistema Integrado de Gestión Institucional: Política que integra las intenciones de la Alta Dirección en términos del Sistema de Gestión de Calidad y las directrices establecidas en las Políticas de Desarrollo Administrativo, incluidas en el Decreto 2482 de 2012, con el propósito de alcanzar los propósitos establecidos.

Rendición de Cuentas: es la obligación de un actor de informar y explicar sus acciones a otro(s) que tiene el derecho de exigirla, debido a la presencia de una relación de poder, y la posibilidad de imponer algún tipo de sanción por un comportamiento inadecuado o de premiar un comportamiento destacado[2].

SIGI: Sistema Integrado de Gestión Institucional, constituido por el Sistema de Gestión de Calidad, el Sistema de Control Interno y el Sistema de Desarrollo Administrativo.

SG-SST: Sistema de Gestión de Seguridad y Salud en el Trabajo

1. ANTECEDENTES

Las políticas de desarrollo administrativo surgieron como una alternativa para direccionar a las entidades públicas hacia la mejora continua de su gestión, y fueron establecidas en primera instancia a través de la Ley 489 de 1998, que además incluyó los principios de la función administrativa y estableció las directrices respecto al Sistema de Desarrollo Administrativo.

[1] Decreto 2482 de 2012, Articulo 2

[2] CONPES 3654, Política de Rendición de Cuentas de la Rama Ejecutiva a los Ciudadanos.

Estas políticas fueron modificadas a través del Decreto 3622 de 2005 que las presentó de una manera más integral. En diciembre de 2012, a través de la expedición del Decreto 2482, se derogó el Decreto 3622 y se definieron nuevamente las políticas de desarrollo administrativo, las cuales son objeto de este documento.

Asociadas a las directrices del Decreto 2482, también existen una serie de normas como el 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.

Adicionalmente existen normas y técnicas como la NTCGP 1000:2009, la NTC 9001:2015, Directiva Presidencial N°4 de 2012 y la Circular N°005 de 2012 , la ley 1562 de 2012, el Decreto 1072 del 2015, la NTC ISO 27001:2013, que dan pautas para la implementación de los Sistemas de Gestión de Calidad, Ambiental, Seguridad y Salud en el Trabajo y el Sistema de Seguridad de la Información, que dentro de los requisitos a cumplir está la definición de una política asociada al sistema correspondiente.

2. ORIENTACIÓN ESTRATEGICA DE LA AGENCIA NACIONAL DE DEFENSA JURIDICA 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[3].

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[4].

2.2. MISION

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. VISION

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

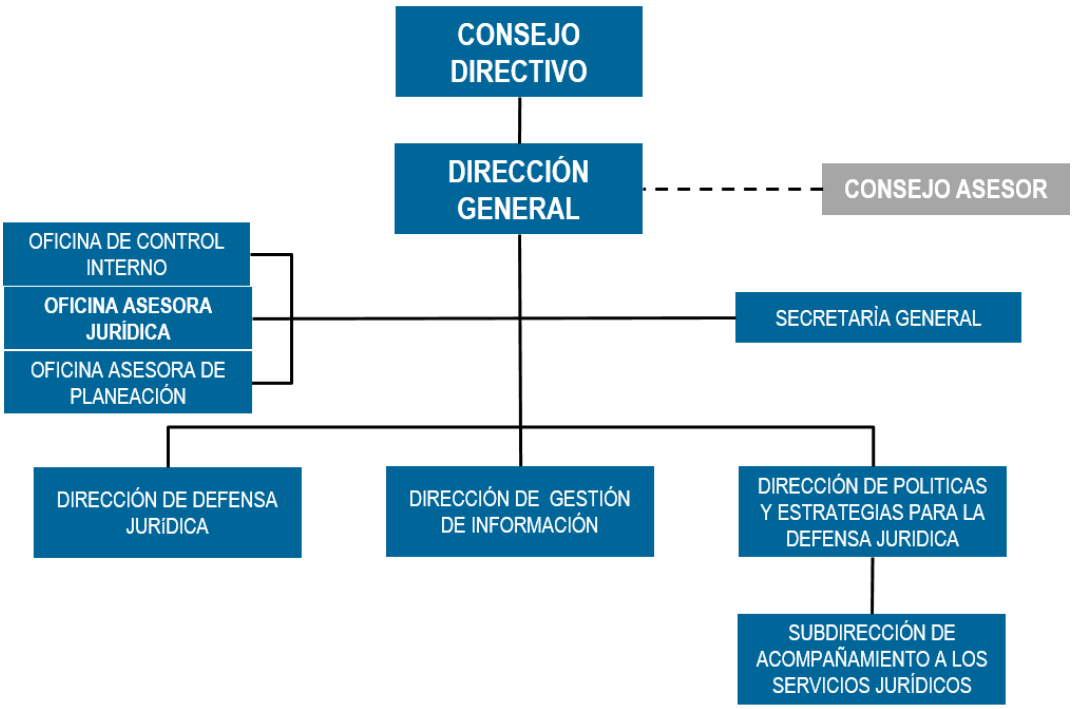
[3] Decreto 4085 de 2011, Articulo 1.
[4] Decreto 4085 de 2011, Articulo 2.

2.4. PRINCIPIOS BASICOS 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:



3. RELACIÓN DE LA PLANEACIÓN ESTRATEGICA DE LA AGENCIA CON LAS POLITICAS DE DESARROLLO ADMINISTRATIVO

Las Políticas de Desarrollo Administrativo enunciadas en el Decreto 2482 de 2012, artículo 3°, se despliegan por toda la entidad a través de diferentes mecanismos, entre los que se encuentra principalmente el Plan Estratégico 2014-2018. Este Plan se extiende por todas las dependencias que finalmente formulan Planes Operativos de Acción Anuales alineados al Plan Estratégico, en los cuales están definidas las acciones a desarrollar en la vigencia, alineadas con las Políticas de Desarrollo Administrativo.

La evaluación de la implementación de estas políticas, se adelanta según lo dispuesto por el Departamento Administrativo de la Función Pública a través del Formulario Único Reporte de Avances de la Gestión – FURAG y del cual se pueden desprender acciones a incluir en la planeación de la entidad.

A continuación se visualiza la relación que existe entre la Política del Sistema Integrado de Gestión Institucional, los Objetivos Estratégicos y las Políticas de Desarrollo Administrativo:

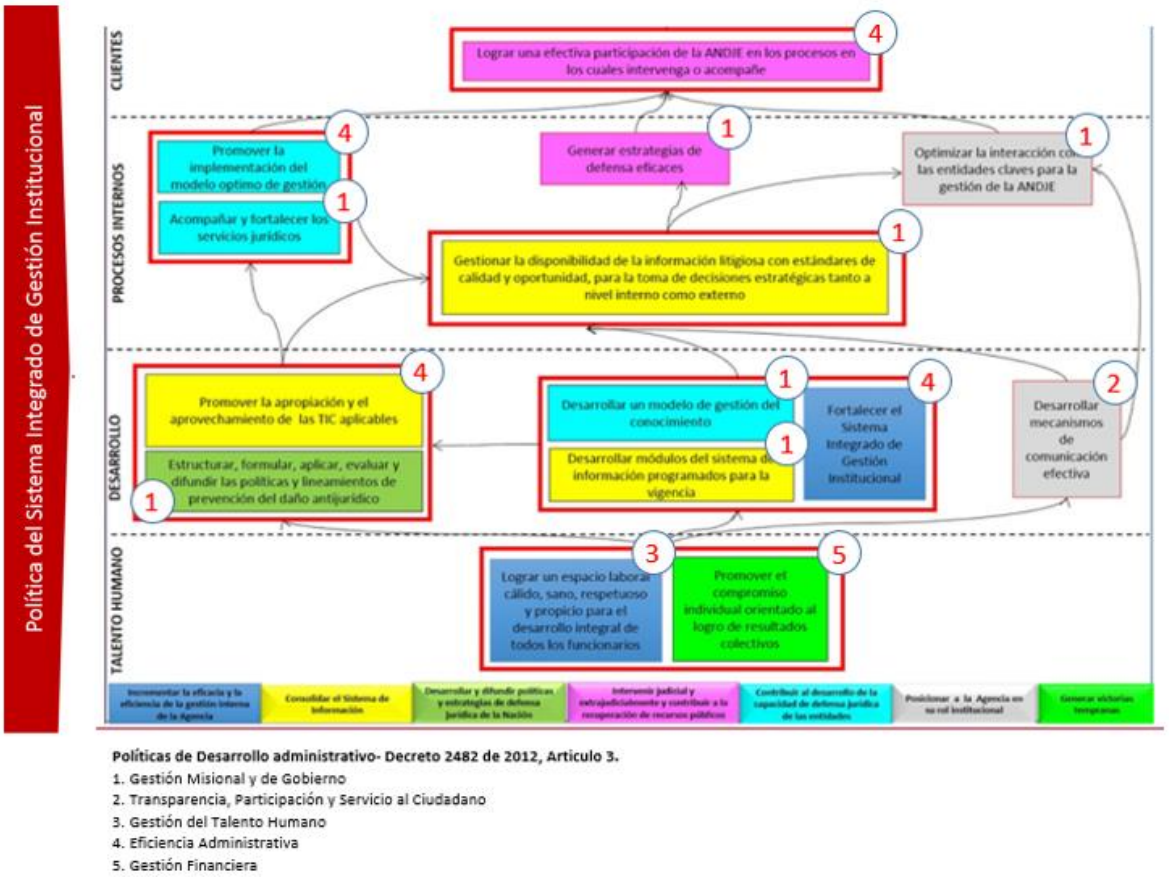


Grafico1. Relación de la Política del Sistema Integrado de Gestión Institucional, las Políticas de Desarrollo Administrativo y los Objetivos Estratégicos planteados para el 2015.

4. POLITICA DEL SISTEMA INTEGRADO DE GESTIÓN INSTITUCIONAL

Tomando como base las Políticas de Desarrollo Administrativo definidas a través del Decreto 2482 de 2012, las directrices establecidas en la Norma Técnica de Calidad en la Gestión Pública NTCGP 1000:2009, Numeral 5.3 Política de Calidad, la ANDJE, estableció como política del Sistema Integrado de Gestión Institucional la siguiente:

"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".

4.1. DESPLIEGUE DE LA POLITICA DEL SISTEMA INTEGRADO DE GESTIÓN INSTITUCIONAL.

Se habla de una política integrada porque recoge aspectos relacionados con el Sistema de Gestión de Calidad, de acuerdo con lo dispuesto en la Norma Técnica de Calidad en la Gestión Pública NTCGP 1000:2009 y las Políticas de Desarrollo Administrativo, establecidas en el Decreto 2482 de 2012. Despliega esas directrices a toda la Entidad a través de la Planeación Estratégica y el Sistema de Gestión de Calidad. El despliegue de la política, se presenta a continuación.

4.1.1. Adecuada al Objeto y coherente con el PND

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.

4.1.2. Compromiso de cumplir los requisitos de sus clientes

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.

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

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.

4.1.4 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, 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.

4.1.5 Compromiso con la Gestión misional y de Gobierno

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.

4.1.6 Compromiso con la transparencia, participación y servicio al ciudadano

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.

4.1.7 Compromiso con la gestión del talento humano

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.

4.1.8 Compromiso con la eficiencia administrativa

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.

4.1.9 Compromiso con la gestión financiera

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.

5 POLITICAS DE DESARROLLO ADMINISTRATIVO

Entendiendo como políticas de desarrollo administrativo, 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 2482 de 2012, la ANDJE adoptó las Políticas de Desarrollo Administrativo establecidas en este Decreto[5], y las incorporó en su planeación estratégica a través de las diferentes

[5] Decreto 2482 de 2012, Articulo 3.

actividades definidas por cada una de las dependencias. Dichas políticas se relacionan a continuación.

5.1 GESTIÓN MISIONAL Y DE GOBIERNO.

Orientada al logro de las metas establecidas, para el cumplimiento de su misión y de las prioridades que el Gobierno defina. Incluye, entre otros, para las entidades de la Rama Ejecutiva del Orden Nacional, los indicadores y metas de Gobierno que se registran en el Sistema de Seguimiento a Metas de Gobierno-SISMEG, administrado por el Departamento Nacional de Planeación-DNP.

5.2 TRANSPARENCIA, PARTICIPACIÓN Y SERVICIO AL CIUDADANO

Orientada a acercar el Estado al ciudadano y hacer visible la gestión pública. Permite la participación activa de la ciudadanía en la toma de decisiones y su acceso a la información, a los trámites y servicios, para una atención oportuna y efectiva. Incluye entre otros, el Plan Anticorrupción y de Atención al Ciudadano y los requerimientos asociados a la participación ciudadana, rendición de cuentas y servicio al ciudadano.

5.3 GESTIÓN DEL TALENTO HUMANO

Orientada al desarrollo y cualificación de los servidores públicos buscando la observancia del principio de mérito para la provisión de los empleos, el desarrollo de competencias, vocación del servicio, la aplicación de estímulos y una gerencia pública enfocada a la consecución de resultados. Incluye, entre otros el Plan Institucional de Capacitación, el Plan de Bienestar e Incentivos, los temas relacionados con Clima Organizacional y el Plan Anual de Vacantes.

5.4 EFICIENCIA ADMINISTRATIVA

Orientada a identificar, racionalizar, simplificar y automatizar trámites, procesos, procedimientos y servicios, así como optimizar el uso de recursos, con el propósito de contar con organizaciones modernas, innovadoras, flexibles y abiertas al entorno, con capacidad de transformarse, adaptarse y responder en forma ágil y oportuna a las demandas y necesidades de la comunidad, para el logro de los objetivos del Estado. Incluye, entre otros, los temas relacionados con gestión de calidad, eficiencia administrativa y cero papel, racionalización de trámites, modernización institucional, gestión de tecnologías de información y gestión documental.

5.5 GESTIÓN FINANCIERA

Orientada a programar, controlar y registrar las operaciones financieras, de acuerdo con los recursos disponibles de la entidad. Integra las actividades relacionadas con la adquisición de bienes y servicios, la gestión de proyectos de inversión y la programación y ejecución del presupuesto. Incluye, entre otros, el Programa Anual Mensualizado de Caja – PAC, programación y ejecución presupuestal, formulación y seguimiento a proyectos de inversión y el Plan Anual de Adquisiciones.

6 OTRAS POLITICAS INSTITUCIONALES

Adicional a las políticas de Desarrollo Administrativo, existen una serie de políticas que se generan por la implementación de sistemas como el de Seguridad y Salud Trabajo, el Sistema de Gestión Ambiental y el Sistema de Seguridad de la Información, las cuales se relacionan a continuación.

6.1 POLITICA DE ADMINISTRACIÓN DE RIESGOS

En atención a los criterios que respecto a la gestión de los riesgos establece el **Modelo Estándar de Control Interno – MECI** y demás documentos metodológicos expedidos por el Departamento Administrativo de la Función Pública-DAFP, las orientaciones dadas por la Secretaría de Transparencia de la Presidencia de la Republica 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[6]:

6.1.1 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.

6.1.2 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

[6] Guía para la Administración del Riesgo, Departamento Administrativo de la Función Pública.

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.

6.1.3 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.

6.1.4 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.

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.**

6.2 POLITICA AMBIENTAL Y DE CERO PAPEL

La Política ambiental y de cero papel debe atender las directrices establecidas en la Directiva Presidencial N°4 de 2012 y la Circular N°005 de 2012, la Agencia Nacional de Defensa Jurídica del Estado, al definir su Política Ambiental y de cero papel debe dar cumplimiento a los siguientes criterios:

La Alta Dirección debe definir la política ambiental y de cero papel de la entidad y asegurarse que dentro del alcance definido, la política:

- Sea apropiada a la naturaleza, magnitud e impactos ambientales de las actividades, productos y servicios de la entidad;
- Incluya el compromiso de la agencia con la mejora continua y prevención de la contaminación;
- Incluya el compromiso de cumplir con los requisitos legales aplicables y con otros requisitos que la entidad suscriba relacionados con sus aspectos ambientales;
- Proporcione el marco de referencia para establecer y revisar los objetivos y las metas ambientales;
- Sea documentada, implementada y se mantiene.
- Sea comunica a todos los servidores públicos de la agencia o los que en nombre de ella adelanten gestión; y
- Esté a disposición del público.

Dando cumplimiento a lo anterior, se presenta la política Ambiental y de cero papel, que fue adoptada a través de la resolución 076 de Abril de 2014.

POLÍTICA AMBIENTAL Y DE CERO PAPEL

La Agencia Nacional de Defensa Jurídica del Estado, como una Unidad Administrativa especial, que tiene como objetivo la estructuración, formulación, aplicación, evaluación y difusión de las políticas de prevención del daño antijurídico, así como la defensa y protección efectiva de los intereses litigiosos de la Nación, en las actuaciones judiciales de las entidades públicas, en procura de la reducción de la responsabilidad patrimonial y la actividad litigiosa; es consciente de la importancia que tiene garantizar y promover el respeto y cuidado por el medioambiente.

Expresando su interés, preocupación y compromiso, se compromete a fomentar la responsabilidad en todos sus colaboradores, con el fin de minimizar el impacto socio-ambiental que puedan surgir en las actividades propias de la Entidad.

Para lograrlo, los directivos de la Agencia Nacional de Defensa Jurídica del Estado, destinan permanentemente los recursos necesarios para implementar, monitorear y evaluar los lineamientos en materia ambiental y de cero papel logrando una eficaz implementación y cumpliendo la legislación colombiana vigente y los demás requisitos aplicables al cuidado del Medio Ambiente.

6.3 POLITICA 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 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 lo son: Grupos itinerantes, Intranet, carteleras, correo electrónico, inducción y reinducción y página web.

6.4 POLITICA 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 la 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 integrara 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 12 políticas de seguridad que soportan el SGSI para la AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO:

La AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO ha decidido **definir, implementar, operar y mejorar** de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.

Las **responsabilidades** frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de **los empleados, contratistas o terceros**.

La AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO **protegerá la información** generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.

La AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO **protegerá la información** creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un **uso incorrecto** de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

La AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO **protegerá su información** de las amenazas originadas por parte **del personal**.

La AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO **protegerá las instalaciones** de procesamiento y la infraestructura tecnológica **que soporta sus procesos críticos**.

La AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO **controlará la operación** de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

La AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO **implementará control de acceso** a la información, sistemas y recursos de red.

La AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

La AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

La AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO **garantizará la disponibilidad** de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

La AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO garantizará el cumplimiento de las **obligaciones legales, regulatorias y contractuales establecidas.**

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

6.4.1 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.

6.4.2 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.

6.4.3 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 las 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.

6.4.4 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 llevar a 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.

6.4.5 POLÍTICA DE USO DE CORREO ELECTRONICO

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.

6.4.6 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 la 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.

6.4.7 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.

6.4.8 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.

Todo 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 el 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.

6.4.9 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.

6.4.10 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 la información CONFIDENCIAL protegida bajo llave.

6.4.11 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.

6.4.12 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 el 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.

6.4.13 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 crítica 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 copias, 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 almacenar a información resultado de sus actividades laborales en la carpeta “Documentos” a la cual se realiza back-up.

Todos los usuarios son responsables de realizar los 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 el desempeño de las funciones laborales, es propiedad de la ANDJE y cada usuario es responsable por proteger su integridad, confidencialidad y disponibilidad.

6.5 POLITICA 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 2609 de 2012, Artículo 6, en el cual se establecen los componentes mínimos que debe incorporar. Dicha política fue aprobada por el Comité Institucional de Desarrollo Administrativo.

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 presupuestales.
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.

- *Tomada del Programa de Gestión Documental – PGD 2014 – 2017, aprobado en sesión de CIDA del 30 de enero del 2014.*

7 COMO SE IMPLEMENTAN LAS POLITICAS INSTITUCIONALES Y DE DESARROLLO ADMINISTRATIVO

7.1 GESTIÓN MISIONAL Y DE GOBIERNO.

Tomando como base las disposiciones establecidas en el Plan Nacional de Desarrollo vigente en cada cuatrienio, la Agencia Nacional de Defensa Jurídica participará en la elaboración del Plan Estratégico Sectorial, liderado por el Ministerio de Justicia y del Derecho, del cual se derivan las actividades a incluir en el Plan Estratégico Institucional que se despliegan en el Plan de Acción Institucional. El Comité Institucional de Desarrollo Administrativo, tiene la responsabilidad de priorizar los indicadores a registrar en el SISMEG, y la Oficina Asesora de Planeación tiene la responsabilidad de acompañar a las dependencias dueñas de dichos indicadores en la creación y/o modificación de los mismos, siguiendo las instrucciones impartidas por el Departamento Nacional de Planeación.

Según lo dispuesto en la Directiva Presidencial 021 de 2011, a más tardar el día 10 de cada mes los responsables de los indicadores deben actualizar la información de los indicadores en el aplicativo SISMEG administrado por el DNP y la Oficina Asesora de Planeación debe efectuar el seguimiento a la actualización de la información, evaluar su calidad y presentar las observaciones que considere necesarias para garantizar la coherencia y consistencia de lo registrado, adicionalmente debe preparar el informe a presentar en los Comités Sectoriales de Desarrollo Administrativo.

La priorización de los indicadores se puede adelantar teniendo en cuenta los criterios establecidos por el Departamento Nacional de Planeación en el documento **"Guía Metodológica para la formulación de indicadores".**

7.2 TRANSPARENCIA, PARTICIPACIÓN Y SERVICIO AL CIUDADANO.

Atendiendo lo establecido en el Decreto 2482 de 2012, el desarrollo de la política de transparencia, participación y servicio al ciudadano incluye cinco componentes a tener en cuenta: Plan Anticorrupción y de Atención al Ciudadano, Transparencia, Acceso a la Información pública, Participación Ciudadana, Rendición de Cuentas y Servicio al Ciudadano. Estos componentes se desarrollan de la siguiente manera:

Plan Anticorrupción y de Atención al Ciudadano

La Ley 1474 de 2011 en el Artículo 73 establece la obligatoriedad de elaborar y Publicar a más tardar el 31 de enero de cada año el Plan Anticorrupción y de Atención al Ciudadano, este Plan debe incluir las actividades a ejecutar durante la vigencia en los siguientes cuatro componentes: Mapa de riesgos de corrupción, Estrategia Anti tramites, Estrategia de Rendición de Cuentas, Mecanismo para mejorar la atención al ciudadano. Cada una de las cuales se debe planificar atendiendo las directrices establecidas en el documento **"Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano"**, de la Secretaría de Transparencia de la Presidencia de la Republica.

Cada componente del plan se debe desarrollar de la siguiente manera y reflejarse en el Plan Operativo Institucional:

a. **Mapa de Riesgos de Corrupción:** la documentación de estos riesgos, se debe adelantar atendiendo la metodología establecida para los riesgos asociados a los procesos, teniendo en cuenta que las categorías para los riesgos de corrupción deben ser inaceptable o intolerable, su impacto siempre será catastrófico y la probabilidad de materialización considera los criterios "casi seguro" o "posible". Las opciones de tratamiento para estos riesgos son: "Evitar el riesgo" y "Reducir el riesgo". La documentación del mapa de riesgos se hace en el formato establecido por la Secretaría de Transparencia de la Presidencia de la Republica en el documento **"Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano"**. El seguimiento o monitoreo a estos riesgos de corrupción debe efectuarlo cada responsable de proceso en el que se documentaron los riesgos por lo menos tres (3) veces al año con corte a 30 de abril, 31 de agosto y 31 de diciembre; y en caso de ser necesario deberá formular las acciones necesarias para su mitigación.

b. **Estrategia Anti trámites:** Este componente debe estar alineado con la Política de Racionalización de Tramites establecida por el Departamento Administrativo de la Función Pública - DAFP, incorporada en el Artículo 75 de la Ley 1474 de 2011. Para la Agencia mediante radicado No.20155010210771-DAFP, La Dirección de Control Interno y Racionalización de Trámites del Departamento Administrativo de la Función Pública manifiesta lo siguiente: "(…) que de acuerdo

con el objeto y funciones que desarrolla la Agencia Nacional de Defensa Jurídica del Estado, esta entidad al no ejercer funciones administrativas que conlleven a la realización de un trámite u otro procedimiento administrativo orientado a ningún tipo de usuario, no se encuentra dentro del ámbito de aplicación de la política de racionalización de trámites, lo que implica que no será valorada dicha política en el Formulario Único del Reporte de Avance de la Gestión - FURAG ni en la estrategia anti trámites contenida en el plan anticorrupción y de atención al ciudadano (…)". Este oficio del DAFP fue radicado en la agencia con el número 20158001888782 y fecha 21 de diciembre de 2015.

c. **Estrategia de Rendición de Cuentas:** Según las disposiciones establecidas a través del Conpes 3654 de 2010, anualmente la Agencia debe formular una estrategia de rendición de cuentas que incluya actividades asociadas a los tres componentes Información, Dialogo e Incentivos. A través de estas actividades se debe informar, explicar y dar a conocer los resultados de la gestión. La estrategia de rendición de cuentas debe elaborarse e implementarse teniendo en cuenta las actividades, descritas en la **"Metodología para la implementación del Modelo Integrado de Planeación y Gestión"**, expedida por la Presidencia de la República y el DAFP:

   Según lo dispuesto en la Ley 489 de 1998 respecto a la evaluación de las Audiencias Públicas de Rendición de Cuentas, el **documento "Audiencias Públicas en la Ruta de la Rendición de Cuentas a la Ciudadanía de la Administración Pública Nacional"** emitido por el Departamento Administrativo de la Función Pública, así como la Ley 1474 de 2011, el Documento **"Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano"** emitido por la Secretaría de Transparencia de la Presidencia de la Republica, el Decreto 2482 de 2012, la **"Metodología para la implementación del Modelo Integrado de Planeación y Gestión"**, La Oficina de Control Interno debe adelantar una evaluación individual de cada una de las actividades incluidas en la estrategia de rendición de cuentas y una evaluación general de toda la estrategia de rendición de cuentas y generar un informe con los resultados de dicha evaluación que debe ser publicado en la página web de la entidad.

d. **Servicio al Ciudadano:** Este componente debe desarrollarse atendiendo las disposiciones establecidas por el Departamento Nacional de Planeación, como líder de la Política de Servicio al Ciudadano y lo definido en la Ley 1474 de 2011.

   Las actividades a desarrollar deben estar enmarcadas en tres etapas definidas en el documento **"Estrategias para la construcción del Plan Anticorrupción y de Atención al Ciudadano"**, el cual además define los aspectos mínimos a tener en cuenta para la implementación de este componente, las etapas a tener presentes son: i)desarrollo institucional para el servicio al ciudadano, ii)afianzar la cultura de servicio al ciudadano en los servidores públicos y iii)fortalecimiento de los canales de atención.

Las actividades definidas deben ser incorporadas en el Plan Anual de Acción de la Agencia para garantizar su ejecución y la disponibilidad de recursos, así como el seguimiento a la implementación de las mismas.

7.3 GESTIÓN DEL TALENTO HUMANO

Esta política se desarrolla a través de cuatro componentes, mediante los cuales se busca desarrollar y cualificar a los servidores públicos, enfocado en el logro de objetivos. Los componentes a desarrollar son:

7.3.1 Plan Estratégico de Recursos Humanos

Se entiende por estrategia de Recursos Humanos el "conjunto de prioridades o finalidades básicas que orientan las políticas y prácticas de gestión de Recursos Humanos, para ponerlas al servicio de la estrategia organizativa"7.
La referencia a los planes estratégicos de recursos humanos está dada en el artículo 15 de la Ley 909 de 2004, en el cual se determinan las funciones específicas de las Unidades de Personal. Estos planes están en estrecha relación con las disposiciones del literal b) del artículo 17 de la Ley 909 de 2004 y se dirigen a prever y adelantar las acciones necesarias para la mejor utilización de los recursos humanos en función de los objetivos institucionales y de las necesidades de desarrollo y crecimiento del mismo personal, por lo cual la Agencia Nacional de Defensa Jurídica debe velar porque se dé estricto cumplimiento a las disposiciones establecidas en la ley, mediante el diseño, implementación y actualización del Plan Estratégico de Recursos, de acuerdo con la normativa vigente .

Según lo establecido por el Modelo Integrado de Planeación y Control, a través del Decreto 2482 de 2012, la Política de Gestión de Talento Humano está orientada al desarrollo y cualificación de los servidores públicos buscando la observancia del principio de mérito para la provisión de los empleos, el desarrollo de competencias, vocación del servicio, la aplicación de estímulos y una gerencia pública enfocada a la consecución de resultados.

Incluye, principalmente la Planeación Estratégica de Recursos Humanos como herramienta que integra el Plan Anual de Vacantes, el Plan Institucional de Capacitación-PIC-, el Programa de Bienestar e Incentivos, los temas relacionados con Clima Organizacional.

7.3.2 Plan Anual de vacantes

Es un instrumento que apoya la programación de la provisión de los empleos con vacancia definitiva que deben ser provistos en la siguiente vigencia fiscal siempre y cuando se cuente con la disponibilidad presupuestal, este documento debe ser elaborado atendiendo las disposiciones establecidas por el Departamento Administrativo de la Función Pública a través del documento "Lineamientos para la elaboración del Plan de vacantes", en el cual están establecidas las directrices que deben atenderse para su elaboración y los instrumentos que deben utilizarse para tal fin.

7.3.3 Capacitación

[7] Tomado de la Metodología para la implementación del Modelo Integrado de Planeación y Gestión.

Está directamente relacionado con la formulación del Plan Institucional de Capacitación, el cual debe formularse anualmente con las necesidades identificadas por la entidad. Para adelantar esta actividad se deben tener en cuenta las recomendaciones dadas por el Departamento Administrativo de la Función Pública en la "Guía para la formulación del Plan Institucional de Capacitación-PIC", el cual debe estar alineado con el Plan Nacional de Formación y Capacitación de Empleados Públicos establecido a través del Decreto 4665 de 2007.
El Plan Institucional de Capacitación debe incluir los proyectos de aprendizaje en equipo que sean formulados por lo empleados.

7.3.4 Bienestar e incentivos

El Programa de Bienestar Social e Incentivos debe elaborarse con la participación de la Comisión de Personal de la Agencia o de la instancia que realice las funciones que a esta le han sido asignadas. Para su elaboración deben atenderse las disposiciones establecidas en el Decreto 1227 de 2004, en los Artículos 70 y 75 y debe incorporar el área de calidad de vida y el área de protección y servicios sociales. L a Agencia debe efectuar al menos una medición del clima laboral cada dos años y definir e implementar las acciones que se consideren necesarias para mejorar los aspectos que necesiten ser reforzados para garantizar un clima laboral adecuado y el reconocimiento del esfuerzo de los servidores públicos que laboran en la Agencia y los equipos de trabajo que propicien e implementen mejores prácticas que beneficien a la entidad.

7.4 EFICIENCIA ADMINISTRATIVA

Según lo establecido en el Decreto 2482 de 2012, el desarrollo de la política de eficiencia administrativa incluye seis componentes a tener en cuenta: Gestión de la Calidad, Eficiencia Administrativa y Cero Papel, Racionalización de Tramites, Modernización Institucional, Gestión de Tecnologías de Información y Gestión Documental. Estos componentes se desarrollan de la siguiente manera:

7.4.1 Gestión de la calidad

La implementación, mantenimiento y mejora del Sistema de Gestión de Calidad se adelanta atendiendo las disposiciones establecidas en la Norma Técnica de Calidad en la Gestión Pública NTCGP 1000:2009, NTC 9001:2015 y el Modelo Estándar de Control Interno – MECI 1000:2005.

7.4.2 Eficiencia Administrativa y cero papel

Este componente está directamente relacionado con el componente de Gestión de la Calidad, la Estrategia de Cero Papel liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones y la Dirección de Gobierno en Línea y los componentes de Gestión de Tecnologías de Información y Gestión Documental. De acuerdo con los lineamientos dados en la Directiva Presidencial 04 de 2012 expedida por la Presidencia de la Republica, se debe adelantar la identificación, racionalización, simplificación y automatización de los trámites, procesos, procedimientos y servicios internos, de manera que se garantizar la eficiente, eficaz y oportuna prestación de los servicios y entrega de los productos especificados. Las actividades a desarrollar son las siguientes:

i) Implementar buenas prácticas para la reducción del consumo de papel, teniendo como referencia la "Guía de Buenas Prácticas para reducir el consumo de papel" elaborado por el Programa Gobierno en línea". ii) Elaboración de documentos electrónicos, para lo cual debe efectuarse un análisis de los procesos y servicios de la entidad, identificar los requisitos y necesidades, evaluación los sistemas existentes, definición de las estrategias y diseño del sistema requerido, lo anterior atendiendo lo definido en el parágrafo 1 del artículo 6 de la Ley 962 de 2005 y los Artículos 55 a 59, de la Ley 1437 de 2011. iii) Procesos y procedimientos internos electrónicos, para los cual es necesario: i) Caracterizar todos los procesos y procedimientos, ii) Analizar, priorizar y racionalizar los procesos y procedimientos, iii) Automatizar los procesos y procedimientos prioritarios y complejos y iv) Mejorar los procesos y procedimientos automatizados.

7.4.3 Modernización institucional

El proceso de modernización de la Agencia debe adelantarse guardando estricto cumplimiento de las normas vigentes que establecen las directrices para llevar a cabo dicha labor y los documentos metodológicos establecidos por el Departamento Administrativo de la Función Pública. Para llevar a cabo un proceso de modernización institucional, la entidad debe cumplir como mínimo los parámetros establecidos en el documento "Metodología para la Implementación del Modelo Integrado de Planeación y Gestión", la "Guía de modernización de entidades Públicas", el "Manual para la elaboración de la memoria justificativa", expedido por la Secretaría Jurídica de la Presidencia de la Republica y demás documento que las entidades competentes expidan al respecto.

7.4.4 Gestión de tecnologías de información

Este componente se desarrolla a través de la Estrategia de Gobierno en Línea, para el desarrollo del mismo se debe adelantar: i) Una revisión de ajuste tecnológico, para determinar las condiciones tecnológicas de la entidad, con el fin de identificar los ajustes requeridos incluyendo un análisis de la infraestructura tecnológica, los riesgos sobre seguridad física y del entorno y seguridad informática y el crecimiento de la capacidad de la infraestructura, incluyendo un plan para la recuperación ante desastres. Por otro lado debe implementarse un programa de correcta disposición final de los residuos tecnológicos, estrategias de computación en la nube, uso de esquemas de computación por demanda o uso de centros de datos centralizados que generen ahorros de consumo de energía. ii) Determinar e implementar un plan de transición del protocolo IPv4 al protocolo IPv6, según las directrices del Ministerio de Tecnologías de la Información y las Comunicaciones. iii) Diseño e implementación del Sistema de Gestión de Seguridad de la Información. iv) Implementación de servicios de intercambio de información – RAVEC: identificación, automatización y publicación de los servicios de intercambio de información.

7.4.5 Gestión Documental

A través del programa de Gestión Documental establecido por la Entidad, se da cumplimiento a la Ley General de Archivos, Ley 594 de 2000, que establece las directrices generales en el tema del manejo de los archivos de las entidades, y es a través del Decreto 2609 de 2012, que se desarrolla y dan líneas para su implementación,

este programa contiene todas las etapas para la planificación, manejo y organización de los documentos producidos y recibidos en la ANDJE, facilitando su trámite, utilización, conservación y consulta, a su vez la gestión documental en la Entidad se rige por los principios del proceso de gestión documental establecidos en el Articulo 5, del Decreto 2609 de 2012.

7.5 GESTIÓN FINANCIERA

El objetivo principal de esta política es definir reglas claras que faciliten a la Agencia la programación, control y registro de las operaciones que se adelanten con los recursos asignados a la entidad tanto en funcionamiento como en inversión. Esta política se desarrolla a través los siguientes cuatro requisitos establecidos en el Decreto 2482 de 2012:

7.5.1 Programación y ejecución presupuestal

La programación del presupuesto en la Agencia, se adelanta atendiendo los criterios anuales establecidos por la Dirección General de Presupuesto Público Nacional del Ministerio de Hacienda y el DNP a través de la Dirección de Inversiones y Finanzas Públicas. El Estatuto Orgánico de Presupuesto, Decreto 111 de 1996 y todas las normas que lo conforman y reglamentan establecen las disposiciones generales que debe atender la Agencia durante el ejercicio de estructuración de su presupuesto para cada vigencia.

7.5.2 PAC

Este instrumento de planificación de los pagos a efectuar con los recursos asignados a la entidad debe elaborarse según lo definido en las normas presupuestales vigentes, las directrices establecidas anualmente por el Ministerio de hacienda y enviado a la Dirección General de Crédito Público y Tesoro Nacional del Ministerio de Hacienda antes del 20 de diciembre de cada vigencia. Cuando por algún motivo, en el trascurso de la vigencia, se requieran modificaciones al PAC inicialmente programado, se deberán realizar oportunamente a través de los mecanismos dispuestos por la Dirección General de Crédito Público y Tesoro Nacional.

7.5.3 Proyectos de inversión

La Entidad deberá formular y hacer seguimiento a sus proyectos de inversión atendiendo las disposiciones establecidas por el Departamento Nacional de Planeación a través de la Dirección de Inversiones y Finanzas Públicas, y haciendo uso de las herramientas informáticas que para el efecto han sido creadas como son el Sistema Unificado de Inversiones y Finanzas Públicas – SUIFP, en el cual se registra toda la información de formulación de los proyectos de inversión, etapa que junto con la actualización de proyectos debe adelantarse según los tiempos establecidos para garantizar que le sean asignados los recursos y el Sistema de Seguimiento a Proyectos de Inversión – SPI, mediante el cual se adelanta el seguimiento mensual a la ejecución de los proyectos, etapa en la cual el gerente de proyecto registra el avance y la Oficina Asesora de Planeación debe verificar la oportunidad y calidad de la información registrada en el Sistema.

7.5.4 Plan Anual de Adquisiciones

Es la herramienta a través de la cual la Agencia programa las adquisiciones que debe realizar para garantizar su normal funcionamiento y el logro de los objetivos propuestos, recoge las necesidades a financiar con los recursos de funcionamiento e inversión y debe ser publicado en la página web de la entidad. La elaboración del PAA debe adelantarse siguiendo estrictamente las disposiciones y metodologías definidas por la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente, así como hacer uso de los formatos establecidos para el efecto. Como complemento a lo anterior, la Agencia debe efectuar la publicación del Plan Anual de Adquisiciones en el SECOP, así como las modificaciones que a este se realicen.

8 BIBLIOGRAFIA

Departamento Administrativo de la Función Pública, Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano.

Departamento Administrativo de la Función Pública, Guía para la administración del riesgo.

Departamento Administrativo de la Función Pública, Norma Técnica de Calidad en la Gestión Pública NTCGP 1000:2009.

Departamento Administrativo de la Función Pública, Planeación de los Recursos Humanos-Lineamientos de política, estrategias y orientaciones para la implementación.

Presidencia de la República - Secretaría de Transparencia, Documento "Estrategias para la construcción del Plan Anticorrupción y de Atención al Ciudadano.

Presidencia de la República – Alta Consejería Presidencial para el Buen Gobierno y la Eficiencia Administrativa, Modelo Integrado de Planeación y Gestión.

Elaboró	Revisó	Aprobó
Sandra García Martínez Profesional Oficina Asesora de Planeación	**Ivan Ernesto Morales Celis** Jefe Oficina Asesora de Planeación	**Adriana María Guillen Arango** Directora General ANDJE