**MANUAL DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÒN**

**DIRECCIÒN NACIONAL DE DERECHO DE AUTOR**

**DNDA**

**AGOSTO DE 2017**

CONTENIDO

[CONTENIDO 2](#_Toc490144998)

[INTRODUCCIÒN 3](#_Toc490144999)

[OBJETIVO GENERAL 3](#_Toc490145000)

[OBJETIVOS ESPECÍFICOS 4](#_Toc490145001)

[ALCANCE 5](#_Toc490145002)

[DEFINICIONES 5](#_Toc490145003)

[POLITICA DE SEGURIDAD DE LA INFORMACIÒN 6](#_Toc490145004)

[SANCIONES PARA LA POLITICA DE SEGURIDAD DE LA INFORMACION 8](#_Toc490145005)

[ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION 9](#_Toc490145006)

[ROLES Y RESPONSABILIDAD 9](#_Toc490145007)

[- Comité de Seguridad de la Información 9](#_Toc490145008)

[- Responsable de la Seguridad Informática 10](#_Toc490145009)

[- Jefes de proceso 10](#_Toc490145010)

[- Responsable del proceso de Gestión del Talento Humano 10](#_Toc490145011)

[- Responsable del Proceso de Comunicaciones y Atención al Ciudadano 11](#_Toc490145012)

[- Responsable del Proceso de Tecnologías de la Información 11](#_Toc490145013)

[- Responsable de la Oficina Asesora Jurídica 11](#_Toc490145014)

[- Usuarios de la Información 11](#_Toc490145015)

[- Responsable de la Oficina de Control Interno 12](#_Toc490145016)

[Aspectos Generales 12](#_Toc490145017)

[USO DE CONEXIONES REMOTAS 13](#_Toc490145018)

[VINCULACION DE FUNCIONARIOS 13](#_Toc490145019)

[USO DE TOKENS DE SEGURIDAD 14](#_Toc490145020)

[USO DE MEDIOS DE ALMACENAMIENTO 14](#_Toc490145021)

[CONTROL DE ACCESO 14](#_Toc490145022)

[ADMINISTRACION DE ACCESO DE USUARIOS 14](#_Toc490145023)

[CONTROL DE ACCESO A SISTEMAS Y APLICATIVOS 15](#_Toc490145024)

[SEGURIDAD PARA LOS EQUIPOS INSTITUCIONALES 15](#_Toc490145025)

[COPIAS DE RESPALDO DE LA INFORMACION 15](#_Toc490145026)

[CONTROL AL SOFTWARE 16](#_Toc490145027)

[ASEGURAMIENTO DE LAS REDES DE DATOS 16](#_Toc490145028)

[USO DEL CORREO ELECTRONICO 16](#_Toc490145029)

[USO ADECUADO DE INTERNET 17](#_Toc490145030)

[REDUNDANCIA 17](#_Toc490145031)

[PRIVACIDAD Y PROTECCION DE DATOS PERSONALES 17](#_Toc490145032)

# INTRODUCCIÒN

La DIRECCIÓN Nacional de Derecho de Autor – DNDA tiene como objetivo y función el diseño, la dirección, la administración y la ejecución de las políticas gubernamentales en materia de derecho de autor. Su misión es la de ser una entidad líder, dinámica y reconocida que contribuya en forma permanente a la plena vigencia del respeto al derecho de autor y los derechos conexos.

Para el cumplimiento de su misión institucional la DNDA considera de vital importancia elaborar una estrategia cuyo enfoque se base en los procesos de la organización, por lo cual se han definido procesos documentados del sistema de gestión de seguridad de la información.

La Dirección Nacional de Derecho de Autor reconoce la información como un activo importante para la gestión de sus políticas y así mismo para la obtención de sus logros institucionales, por lo cual considera de carácter vital definir lineamientos que permitan mitigar los posibles riesgos para la custodia de la información institucional.

# OBJETIVO GENERAL

En este documento se establecen el alcance del Sistema de Gestión de Seguridad de la Información para la Dirección Nacional de Derecho de Autor, así como los parámetros que orientan el plan de seguridad de la información y las acciones a seguir para prevenir la aparición o repetición de no conformidades en la Entidad relacionadas con este tema.

La Dirección Nacional de Derecho de Autor está comprometida con la protección, preservación, aseguramiento de la confidencialidad, integridad, disponibilidad, accesibilidad, legalidad, confiabilidad y no repudio de sus activos de información, analizando para cada caso el riesgo correspondiente, y aplicando en la implementación de su mitigación la implementación, el monitoreo y la mejora continua. Así mismo, propende continuamente por el establecimiento de una cultura de Seguridad de la Información entre sus funcionarios, contratistas, estudiantes en práctica y, en general, todas aquellas personas con acceso a su infraestructura informática.

# OBJETIVOS ESPECÍFICOS

* Integridad de la Información, que consiste en proteger y garantizar que los activos de información a su cargo no sufran cambios no autorizados.
* Confidencialidad de la Información, que implica la labor de proteger y garantizar que los activos de información no sean accesibles o divulgados por o a personas no autorizadas.
* Disponibilidad de la Información, cuyo objetivo es el de garantizar que los activos de información, entre ellos los servicios asociados a los procesos de tecnologías de la información y la comunicación, estén disponibles en todo momento, garantizando la continuidad del servicio para el cumplimento de los objetivos misionales de la entidad.
* Accesibilidad de la Información, por el cual se debe garantizar el acceso a la información con las limitaciones legales y establecer el grado en el que los funcionarios y usuarios pueden utilizar los activos de la información de forma satisfactoria.
* Legalidad de la Información, por el cual se debe propender por garantizar que los activos de información, de la Dirección Nacional de Derecho de Autor, cumplan con los parámetros legales, normativos nacionales e internacionales, así como con la reglamentación interna sobre la seguridad de la información de la entidad.
* Confiabilidad de la Información Se debe garantizar la confiabilidad de la Información de la DNDA, es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones de la entidad.
* No Repudio de la Información, objetivo por el cual se debe garantizar que la información enviada, trasmitida y/o recibida en desarrollo de los servicios de red de la entidad se puede probar y no pueda ser negada posteriormente.

# ALCANCE

El Manual de Gestión de la Seguridad de la Dirección Nacional de Derecho de Autor está basado en la norma internacional ISO 27001:2005, es una herramienta fundamental de la Política de Seguridad del Subsistema de Gestión de Seguridad de la Información; en esta norma se encuentran plasmadas las especificaciones para la creación de un sistema de gestión de la seguridad de la información (SGSI). El manual contempla la estructura de gobierno y los lineamientos principales para la seguridad de la información en la Dirección Nacional de Derecho de Autor, los cuales aplican a todos los procesos institucionales de acuerdo con su Sistema de Gestión de Calidad y por lo tanto deben ser conocidos, aceptados y cumplidos por funcionarios, contratistas, judicantes, pasantes o auxiliares y, en general, por todos los terceros que tengan acceso, almacenen, procesen o transmitan información de la institución.

# DEFINICIONES

* **SEGURIDAD INFORMÀTICA:** Consiste en asegurar que los recursos del sistema de información en una organización se utilicen de la manera que se decidió.
* **DISPONIBILIDAD:** Capacidad de un servicio de unos datos o de un sistema a ser accesible y utilizable por los usuarios o procesos autorizados cuando lo requieran. También se refiere a la capacidad de que la información pueda ser recuperada en el momento que se necesite.
* **CONFIDENCIALIDAD:** Cualidad que debe poseer un documento o archivo para que éste solo se entienda de manera comprensible o sea leído por la persona o sistema que esté autorizado**.**
* **INTEGRIDAD:** Cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original.
* **AUTENTICACIÒN:** Situación en la cual se puede verificar que un documento ha sido elaborado o pertenece a quien el documento dice.
* **HARDWARE:** Conjunto de todos los elementos físicos de un sistema informático como CPU, terminales, cableados, medios de almacenamiento secundarios, tarjeta de red, etc..**.**
* **SOFTWARE:** Conjunto de programas lógicos que hacen funcionar el hardware tanto sistemas operativos como aplicaciones.
* **DATOS:** Conjunto de información lógica que amenazan el software y el hardware como por ejemplo paquetes que circulan por un cable de red o entradas de una base de datos.
* **INUNDACIÒN:** Tipo de ataque de denegación de servicio) se produce cuando un sistema queda sobrecargado con múltiples mensajes de correo electrónico.
* **CONFIDENCIALIDAD:** Es un riesgo asociado al envío de correo electrónico a otra persona a través de Internet.

# POLITICA DE SEGURIDAD DE LA INFORMACIÒN

La Dirección General de la Dirección Nacional de Derecho de Autor, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad. Para la Dirección Nacional de Derecho de Autor, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados. De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

* Minimizar el riesgo en las funciones más importantes de la entidad.
* Cumplir con los principios de seguridad de la información.
* Cumplir con los principios de la función administrativa.
* Mantener la confianza de sus usuarios.
* Apoyar la innovación tecnológica.
* Proteger los activos tecnológicos.
* Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
* Fortalecer la cultura de seguridad de la información en los funcionarios, contratistas, judicantes, pasantes y estudiantes en práctica de la Dirección Nacional de Derecho de Autor
* Garantizar la continuidad del servicio frente a incidentes.

La Dirección Nacional de Derecho de Autor 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 misionales, y a los requerimientos regulatorios.

A continuación, se establecen 12 principios de seguridad que soportan el SGSI de la Dirección Nacional de Derecho de Autor:

• Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.

• La Dirección Nacional de Derecho de Autor protegerá la información generada, procesada o resguardada por los procesos misionales, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (contratistas, estudiantes en práctica, judicantes, pasantes, etc.), o como resultado de un servicio interno en outsourcing.

• La Dirección Nacional de Derecho de Autor protegerá la información creada, procesada, transmitida o resguardada por sus procesos misionales, 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 Dirección Nacional de Derecho de Autor protegerá su información de las amenazas originadas por parte del personal.

• La Dirección Nacional de Derecho de Autor protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

• La Dirección Nacional de Derecho de Autor controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

• La Dirección Nacional de Derecho de Autor implementará control de acceso a la información, sistemas y recursos de red.

• La Dirección Nacional de Derecho de Autor garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

• La Dirección Nacional de Derecho de Autor 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 Dirección Nacional de Derecho de Autor garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

• La Dirección Nacional de Derecho de Autor garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

# SANCIONES PARA LA POLITICA DE SEGURIDAD DE LA INFORMACION

Las Políticas de Seguridad de la Información pretenden construir un adecuado ambiente de manejo en cuanto a la información que el funcionario y el usuario externo utiliza. Por tal razón, es necesario que la misma sea catalogada y evaluada, conforme a los conceptos anteriormente descritos, y que las contravenciones a la misma podrán incluir la cancelación de la respectiva cuenta de acceso para el/los funcionarios, contratistas o terceros que la hayan cometido, sin perjuicio de demás acciones disciplinarias o contractuales a que hubiere lugar.

La DNDA, en su objetivo de proteger y administrar su información y la de sus usuarios, procurará crear conciencia en el personal sobre los métodos y procedimientos en seguridad de la información para la correcta gestión de los mismos y ejecutando el respectivo proceso disciplinario necesario cuando se incumplan las normas de seguridad de la información de la entidad.

Todos los funcionarios de la DNDA, deben ser cuidadosos, precavidos y prudentes de no divulgar información confidencial de la entidad, de sus usuarios y sus archivos en lugares públicos, en conversaciones y/o situaciones que pongan en riesgo la seguridad y el buen nombre de la Dirección Nacional de Derecho de Autor.

Así mismo la DNDA, asegurará que sus funcionarios sean desvinculados, reasignados y/o sancionados según sea el caso de incumplimiento y la gravedad de sus acciones, promoviendo la ejecución de tareas de una forma ordenada, controlada y segura.

# ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION

La DNDA, establecerá un esquema de seguridad de la información que contenga actividades, programas, obras y contratos de administración, operación, gestión y evaluación de la seguridad de la información, con base en las funciones asignadas a cada usuario de la red, de manera que pueda realizar sus labores en condiciones de seguridad sin afectar la seguridad de los documentos alojados en la infraestructura institucional, sean propios o ajenos.

# Compromiso de la Dirección con la Seguridad de la información

La Dirección General de la Dirección Nacional de Derecho de Autor apoya activamente la seguridad de la información dentro de la Entidad con un rumbo claro, con un compromiso y una asignación explícita y el conocimiento de las responsabilidades asignadas a cada uno de los intervinientes con respecto a la implementación de este concepto.

* Este compromiso se ve reflejado a través de:
* La creación del Comité de Seguridad de la Información;
* Aprobación del documento de políticas de seguridad de la información
* Asignación de roles y responsabilidades asociadas al cumplimiento DE LA seguridad de la información.

# ROLES Y RESPONSABILIDADES

Las Políticas de seguridad de la información deben ser conocidas y cumplidas por todos los funcionarios, contratistas y cualquier tercero que utilice los recursos informáticos de la Dirección Nacional de Derecho de Autor, sea cual fuere su nivel jerárquico. La Dirección General de la Dirección Nacional de Derecho de Autor debe aprobar esta política, y así mismo se deben establecer dentro de la organización los siguientes roles que garanticen su cumplimiento:

# Comité de Seguridad de la Información

El Comité de Seguridad de la Información de la Dirección Nacional de Derecho de Autor debe aprobar esta política y es responsable de su implementación y sus modificaciones, razón por la cual deben crearse dentro de la organización los siguientes roles que garanticen su cumplimiento:

* El Comité de Seguridad de la Información de la DNDA, debe proponer a la alta Dirección de la Entidad, para su aprobación, las acciones para cumplir con la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información.
* Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas ya existentes y a las nuevas que se vayan presentando.
* Tener conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
* Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.
* Acordar y aprobar metodologías y procesos específicos relativos a seguridad de la información
* Garantizar que la seguridad sea parte del proceso de planificación de la información
* Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios
* Promover la difusión y apoyo a la seguridad de la información dentro de la Dirección Nacional de Derecho de Autor
* Coordinar el proceso de administración de la continuidad de las actividades de la Dirección Nacional de Derecho de Autor

# Responsable de la Seguridad Informática

El Responsable de Seguridad Informática cumplirá funciones relativas a la seguridad de los sistemas de información de la Dirección Nacional de Derecho de Autor, lo cual incluye la supervisión de todos los aspectos inherentes a los temas tratados en la PSI.

# Jefes de proceso

Los Jefes de Proceso en su calidad de Propietarios de la Información son responsables de clasificarla de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada, y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

# Responsable del proceso de Gestión del Talento Humano

El Responsable del proceso de Gestión del Talento Humano cumplirá la función de notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan y las tareas de capacitación continua en materia de seguridad.

# Responsable del Proceso de Comunicaciones y Atención al Ciudadano

El Responsable del Área de Prensa, tendrá a su cargo la notificación de la PSI a todo el personal, de los cambios que en ella se produzcan, la implementación de los Compromisos de Confidencialidad, etc.

# Responsable del Proceso de Tecnologías de la Información

El Responsable del Área de Tecnología, cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la Dirección Nacional de Derecho de Autor.

Adicionalmente tendrá la función de efectuar las tareas de desarrollo y mantenimiento de soluciones informáticas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

# Responsable de la Oficina Asesora Jurídica

El Responsable de la Oficina Asesora Jurídica verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la Dirección Nacional de Derecho de Autor con sus funcionarios y con terceros. Asimismo, asesorará en materia legal a la Dirección Nacional de Derecho de Autor en lo que se refiere a la seguridad de la información.

# Usuarios de la Información

Los usuarios de la información de la Dirección Nacional de Derecho de Autor son responsables de conocer y dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.

# Responsable de la Oficina de Control Interno

El responsable de la Oficina de Control Interno, o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por la Políticas de Seguridad de la Información y por las normas, procedimientos y prácticas que de ella surjan.

# Aspectos Generales

Este ítem contempla una serie de pautas sobre aspectos específicos de la Seguridad de la Información, que incluyen los siguientes tópicos:

**Organización de la Seguridad:**

Orientado a administrar la seguridad de la información dentro de la Dirección Nacional de Derecho de Autor y establecer un marco gerencial para controlar su implementación. ­

**Clasificación y Control de Activos:**

Destinado a mantener una adecuada protección de los activos de la Dirección Nacional de Derecho de Autor. ­

 **Seguridad del Personal:**

Orientado a reducir los riesgos de error humano, comisión de ilícitos contra la Dirección Nacional de Derecho de Autor o uso inadecuado de instalaciones.

**Seguridad Física y Ambiental:**

Destinado a impedir accesos no autorizados, daños e interferencia a las estaciones e información de la Dirección Nacional de Derecho de Autor. ­

**Gestión de las Comunicaciones y las Operaciones:**

Dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación. ­

**Control de Acceso:**

Orientado a controlar el acceso lógico a la información. ­

**Desarrollo y Mantenimiento de los Sistemas:**

Orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su desarrollo y/o implementación y durante su mantenimiento. ­

**Administración de la Continuidad del funcionamiento de la Dirección Nacional de Derecho de Autor:**

Orientado a contrarrestar las interrupciones del funcionamiento y proteger los procesos críticos de los efectos de fallas significativas o desastres.

**Cumplimiento:**

Destinado a impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.

A fin de asegurar la implementación de las medidas de seguridad comprendidas en las PSI, la Dirección Nacional de Derecho de Autor debe identificar los recursos necesarios y realizar las gestiones tendientes a garantizar las partidas presupuestarles correspondientes para ejecutar las soluciones informáticas en aspectos de seguridad. El Comité de Seguridad de la Información debe revisar periódicamente las PSI dados los continuos cambios tecnológicos y creación de nuevas amenazas informáticas, a efectos de mantenerla actualizada. Así mismo, efectuará toda modificación que sea necesaria en función a posibles cambios que puedan afectar su definición, como son: cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad, etc.

# USO DE CONEXIONES REMOTAS

El acceso remoto a los recursos institucionales sólo podrá ser realizado por los funcionarios de la Unidad de Sistemas con el fin de prestar el soporte mínimo necesario para garantizar el correcto funcionamiento de los servicios institucionales. Siempre que ello se realice se deberá diligenciar el respectivo soporte en el que conste la justificación del ingreso, así como el horario y labores realizadas.

# VINCULACION DE FUNCIONARIOS

La DNDA, identifica y promueve el factor humano en el óptimo cumplimiento de sus respectivas labores, seleccionando el mejor personal, apto y capacitado que cuente con los respectivos conocimientos de los temas, para poder así, desarrollar son eficacia la labor encomendada. En tal sentido, sólo la Subdirección Administrativa podrá solicitar la creación, eliminación o actualización de las cuentas y permisos de los usuarios de la Red, bien se trate de funcionarios, contratistas, judicantes, pasantes, estudiantes en práctica, para lo cual informará los datos del usuario, el proceso para el cual trabajará y el rango de tiempo durante el cual deberán asignársele permisos de acceso a la Red de datos de la DNDA. El responsable del proceso para el cual el aspirante al acceso a la red institucional prestará sus servicios será quien relacione los permisos que se le deben conceder al nuevo usuario por parte de la Unidad de Sistemas.

# USO DE TOKENS DE SEGURIDAD

La DNDA, facilitará las condiciones de manejo de los tokens de seguridad en los procesos que se utilizan y velará porque los funcionarios hagan un uso responsable y correcto de los mismos, conforme el procedimiento de entrega de bienes para el cumplimiento de las funciones asignadas a cada uno de ellos.

# USO DE MEDIOS DE ALMACENAMIENTO

El uso de medios de almacenamiento en los recursos de la plataforma tecnológica de la DNDA será reglamentado por la Coordinación de Sistemas, considerando y evaluando las labores realizadas por los funcionarios y su necesidad de uso.

# CONTROL DE ACCESO

La Coordinación de Sistemas de la DNDA como responsable de la red de datos y los recursos de red de la entidad, debe velar porque dicha red sea debidamente protegida contra accesos y modificaciones no autorizados tanto internos como externos mediante diferentes mecanismos de control de acceso lógico y físico.

# ADMINISTRACION DE ACCESO DE USUARIOS

La DNDA establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la DNDA. Así mismo, velará porque los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

Para tal efecto se contará con una definición de permisos a través del directorio activo de accesos a la red institucional, y así mismo se garantizará que el acceso a los documentos de gestión que reposan en las series documentales sean estrictamente los definidos por los responsables de cada proceso, y la Unidad de Sistemas será la responsable de implementar y garantizar que los permisos concedidos sean exactamente los que fueron definidos por los responsables de los procesos en sus respectivas series documentales.

# CONTROL DE ACCESO A SISTEMAS Y APLICATIVOS

La Coordinación de Sistemas, como responsable de los sistemas de información y aplicativos que complementan los procesos de la entidad, velarán por la asignación, modificación y cancelación de privilegios de acceso a sus sistemas o aplicativos.

Además, como responsable de la administración de tales sistemas de información, procurara que estos sean debidamente protegidos contra accesos no autorizados a través de diferentes mecanismos de control de acceso lógico, y que así mismo sean retirados cuando se pierda la calidad bajo la cual fueron concedidos.

# SEGURIDAD PARA LOS EQUIPOS INSTITUCIONALES

La DNDA para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica y sistemática de la entidad que se encuentren dentro de sus instalaciones, proporcionará los recursos que garanticen la mitigación de riesgos e impactos negativos sobre dicha plataforma tecnológica.

# COPIAS DE RESPALDO DE LA INFORMACION

La Unidad de Sistemas de la DNDA certificará la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades.

Así mismo, la entidad velará porque los medios que contienen la información de registro de sus usuarios, sean almacenados en una ubicación que garantice el cumplimiento de los controles de seguridad física y digital.

# CONTROL AL SOFTWARE

La DNDA, a través de la Coordinación de Sistemas, establecerá procedimientos para controlar la instalación de software, tanto operativo como no operativo, se cerciorará además de contar con el soporte de los proveedores de dicho software y asegurará también la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el software operativo es actualizado. Así mismo verificará que sólo se instale software del cual se cuente con la respectiva licencia, solicitando cuando sea del caso el apoyo jurídico que se requiera para realizar dicha verificación.

# ASEGURAMIENTO DE LAS REDES DE DATOS

La DNDA establecerá, a través de la Coordinación de Sistemas, los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; así mismo, velará por que se cuente con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos.

#

# USO DEL CORREO ELECTRONICO

La DNDA, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre funcionarios y terceras partes, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

Adicionalmente la Unidad de Sistemas realizará las copias de seguridad que permitan garantizar el acceso a los mensajes remitidos desde y hacia las cuentas del correo institucional cuando sean solicitadas por los funcionarios autorizados.

# USO ADECUADO DE INTERNET

La DNDA consciente de la importancia de Internet como una herramienta para el desempeño de labores de la entidad, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran y para el desarrollo de sus actividades diarias en La DIRECCIÓN; para ello se contará con un canal de datos de ancho de banda preferencial hacia el Centro de Datos en que se alojen los aplicativos de carácter institucional, y adicionalmente un canal de acceso a Internet que permitirá servir de redundancia en caso de falla y que facilitará el acceso a la información y sitios diferentes a los de uso misional.

# REDUNDANCIA

La DNDA propenderá por la existencia de una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables para el buen funcionamiento, tanto a nivel de alojamiento como a nivel de conectividad; ello se garantiza a través de una redundancia que permita, en caso de que el primer recurso no se encuentre disponible, que se tenga acceso a un recurso adicional con el fin de garantizar la continuidad de los servicios, tanto de almacenamiento como de conectividad.

# PRIVACIDAD Y PROTECCION DE DATOS PERSONALES

La DNDA establecerá términos, condiciones y finalidades como responsable de los datos personales obtenidos a través de sus distintos canales de atención y tratará la información de todos los usuarios registrados y funcionarios que hacen parte de la Familia de la DNDA.