TABLA DE CONTENIDO

1. OBJETIVO

El objetivo de este documento es presentar la Política de Seguridad de la información del Ministerio de Justicia y del Derecho, que representan formalmente la directriz general para orientar todas las decisiones alrededor del tratamiento de los riesgos generados por la afectación de la Confidencialidad, Integridad y Disponibilidad de la Información de la Entidad. Igualmente se presentan los Objetivos de Seguridad de la Información de la Entidad, definidos en el marco de la mencionada política, el alcance, roles y responsabilidades de la seguridad de la información y las políticas detalladas de los diferentes dominios de control del Anexo A de la Norma Técnica ISO 27001. Estos lineamientos están basados en el Estándar ISO 27001 vigente y en el Modelo de Seguridad y Privacidad de la Información (MSPI) de la Política de Gobierno Digital.

2. ALCANCE

La Política de Seguridad de la Información, sus directrices y objetivos, aplican para los procesos cubiertos por el alcance del Sistema de Gestión de Seguridad de la Información (SGSI) del Ministerio de Justicia y del Derecho, clasificados según el Mapa de Procesos vigente, en:

- Procesos Estratégicos.
- Procesos Misionales.
- Procesos de apoyo.
- Procesos de Evaluación.

Aplica igualmente para todos los funcionarios, contratistas, proveedores y visitantes del Ministerio de Justicia y del Derecho, quienes son responsables de su cumplimiento al 100%.

3. GLOSARIO

Activo de información: Cualquier elemento que tiene valor para el Ministerio. Para la gestión de riesgos de seguridad de la información se consideran los siguientes tipos: información o datos, software, hardware (incluso redes y elementos de comunicaciones), personal o roles e infraestructura.

Confidencialidad: Propiedad de la información que hace que no sea revelada a individuos, entidades o procesos no autorizados.

Consecuencias: Resultado del evento que puede ser cierto o incierto y tener efectos positivos o negativos para la entidad y que puede expresarse en términos cualitativos o cuantitativos. Una consecuencia inicial puede tener mayor impacto considerando los efectos secundarios.

Custodio de activos de información: Es el rol encargado de administrar y gestionar los controles de seguridad que el responsable de la dependencia a cargo de los activos de información haya definido, para mantener la confidencialidad, integridad y disponibilidad de los mismos.

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012).

Derecho de autor: es la protección que le otorga el Estado al creador de las obras literarias o artísticas desde el momento de su creación y por un tiempo determinado. [1]

Derechos conexos: con esta expresión se conocen en su conjunto, los derechos de los artistas, intérpretes o ejecutantes, productores de fonogramas y organismos de radiodifusión, en relación con sus interpretaciones o ejecuciones, fonogramas y emisiones de radiodifusión, respectivamente.[2]

Descripción de Programa: presentación completa de procedimientos en forma idónea, lo suficientemente detallada para determinar un conjunto de instrucciones que constituya el programa de computador correspondiente.[2]

Disponibilidad: Propiedad de la información de ser accesible y utilizable ante la demanda de una entidad autorizada, en el momento y forma requerida.

Evento de seguridad de la información: Ocurrencia detectada en el estado de un sistema, servicio o red que indica una posible violación de las políticas de seguridad de la información, fallo de los controles o situación desconocida que podría llegar a ser relevante para la seguridad de la información de la Entidad.

Fraude: se entiende por fraude cualquier acto u omisión, incluyendo la realización de declaraciones falsas, que, a sabiendas o por falta de diligencia, inducen a error, o pretenden inducir a error a los funcionarios de la entidad, con la finalidad de obtener una ventaja financiera o de cualquier tipo, para evitar una obligación.[3]

Hardware: Conjunto de partes físicas o componentes tangibles de las plataformas tecnológicas. Elementos, equipos de cómputo y comunicaciones que soportan el procesamiento de la información.

Incidente de seguridad de la información: Evento o serie de eventos de seguridad no deseados que amenazan la seguridad de la información de la Entidad. Puede ser un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; impedimento intencional en la operación normal de las redes, sistemas o recursos informáticos, o una violación confirmada a las políticas de seguridad de la información de la Entidad.

Infraestructura: Son las ubicaciones físicas que prestan servicios relacionados con la información, como edificios, oficinas o secciones especiales de la Entidad.

Integridad: Propiedad de la información de precisión y completitud. La información, una vez generada, debe mantenerse libre de modificaciones no autorizadas.

Material auxiliar: todo material, distinto de un programa de computador o de una descripción de programa, creado para facilitar su comprensión o aplicación, como por ejemplo, descripción de problemas e instrucciones para el usuario.[2]

---

[1] Definiciones extraídas de la página de la Dirección Nacional de Derechos de Autor. www.derechodeautor.gov.co
[2] Definiciones extraídas del Decreto 1360 de 1989.
[3] Definiciones extraídas del documento "Marco Uniforme para la Prevención y la Lucha contra el Fraude y la Corrupción", aprobado en septiembre de 2006.

MSPI: Modelo de Seguridad y Privacidad de la Información. Modelo de operación establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones, en el marco de la Política de Gobierno Digital, que permite a las entidades gestionar adecuadamente la seguridad y privacidad de sus activos de información.

Parte involucrada: Persona u organización que puede afectar, verse afectada o verse a sí misma como afectada por una decisión o una actividad.

Piratería: Es cualquier acción, omisión, actividad o acto ilegal caracterizado por engaño, ocultación o violación de la confianza y la verdad, con la finalidad de plagiar o hacer uso indebido de las invenciones o creaciones científicas o literarias o de creación intelectual.

Programa de computador: expresión de un conjunto organizado de instrucciones, en lenguaje natural o codificado, independientemente del medio en que se encuentre almacenado, cuyo fin es el de hacer que una máquina capaz de procesar información indique, realice u obtenga una función, una tarea o un resultado específico.[2]

Propiedad intelectual: es una disciplina normativa que protege las creaciones intelectuales provenientes de un esfuerzo, trabajo o destreza humanos, dignos de reconocimiento jurídico. La Propiedad Intelectual comprende: el derecho de autor y los derechos conexos. [2]

Responsable de la dependencia a cargo de los activos de información: Es el rol encargado de garantizar que los activos de información se clasifican adecuadamente, de definir y revisar periódicamente las restricciones y clasificaciones de acceso y de delegar los custodios de información para cada activo.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

SGSI: Sistema de Gestión de Seguridad de la Información. Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Software: el soporte lógico (software) se considera como una creación propia del dominio literario y comprende uno o varios de los siguientes elementos: el programa de computador, la descripción de programa y el material auxiliar.[2]

Tratamiento de riesgos: acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

4. DESARROLLO

4.1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Información es la declaración general que representa la posición de la Alta Dirección del Ministerio con respecto a la protección de sus activos de información y a la implementación del Sistema de Gestión de Seguridad de la Información; así como al apoyo a su divulgación y mejora continua. En este sentido, la Política de Seguridad de la Información para el Ministerio de Justicia y del Derecho es:

El Ministerio de Justicia y del Derecho, como responsable de formular, gestionar e implementar las políticas, planes, programas y proyectos de orden nacional, en materia de justicia en el Estado Colombiano; está comprometido con la seguridad de la información, a través de una adecuada gestión de riesgos, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información que esté bajo su responsabilidad; en concordancia con los marcos legales, normativos, regulatorios y contractuales que le apliquen a la Entidad.

4.2. RESPONSABILIDADES DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

- La Alta Dirección del Ministerio de Justicia y del Derecho es responsable de liderar la implantación de la política de seguridad de la información y su difusión entre todos los colaboradores (funcionarios, contratistas, proveedores), visitantes y partes interesadas de la Entidad; promoviendo su cumplimiento y revisión periódica; así como la concienciación y capacitación del personal.

- Los directivos del Ministerio se encargarán de comprometer a los funcionarios, contratistas y proveedores que trabajan bajo su supervisión, en la protección de la información, de acuerdo con esta política y todas las demás políticas específicas definidas en el marco del SGSI.

- Todo el personal será responsable civil y penalmente, por la mala utilización de la información. La Alta Dirección implementará sanciones por incumplimientos de la presente política.

4.3. OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

El Ministerio de Justicia y del Derecho establece los siguientes objetivos generales de la gestión de seguridad de la información:

- Cumplir con el marco legal y regulatorio del Ministerio de Justicia y del Derecho para los aspectos de seguridad de la Información, teniendo en cuenta el cumplimiento de la Ley de Protección de Datos Personales y la Política de Gobierno Digital.

- Realizar una adecuada gestión de riesgos de seguridad de la información que permita mantener el perfil de riesgo en el nivel aceptable definido por la Alta Dirección de la Entidad.

- Fortalecer el conocimiento y compromiso de todos los funcionarios, contratistas, proveedores y partes interesadas del Ministerio, con la seguridad de la información.
- Gestionar y atender oportunamente los incidentes de seguridad de la información para mitigar su efecto sobre los procesos de la Entidad.

4.4. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

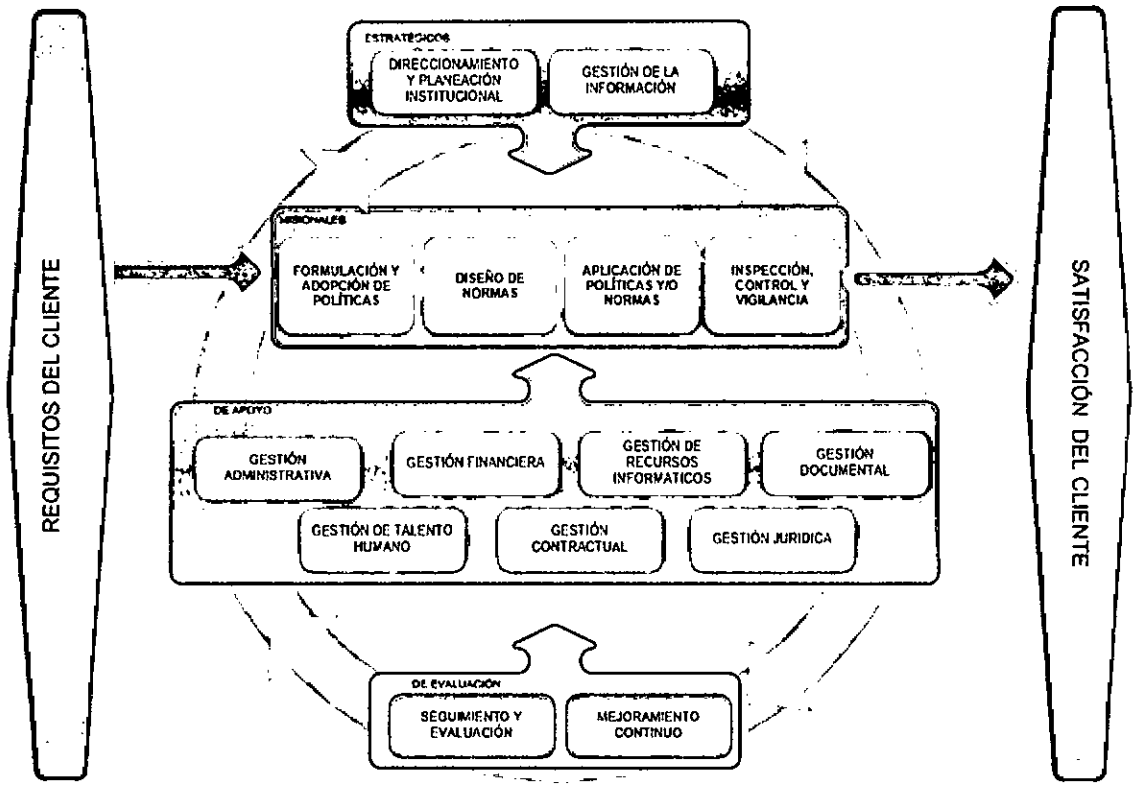
El Sistema de Gestión de Seguridad de la Información del Ministerio de Justicia y del Derecho, implementado en el marco del Modelo de Seguridad y Privacidad de la Información y los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones; en concordancia con las buenas prácticas y estándares internacionales, como parte de las Políticas de Gobierno Digital y de Seguridad Digital y en cumplimiento de la normatividad vigente, tiene el siguiente alcance para la Entidad.

4.4.1. SEDES Y UBICACIONES

El Sistema de Gestión de Seguridad de la Información SGSI cubre con su alcance su sede principal, administrativa y de atención al ciudadano, ubicada en la Calle 53 No 13-27, en Bogotá. Igualmente cubre la sede del Archivo Central del Ministerio de Paloquemao, ubicada en la Carrera 27 # 15-85, administrada por el Grupo de Gestión Documental, que depende de Secretaría General del Ministerio de Justicia.

4.4.2. PROCESOS

El SGSI aplica para todos los procesos del Ministerio de Justicia y del Derecho. Son en total 15, a continuación se encuentra el Mapa de Procesos.



La Entidad tiene dos procesos estratégicos:

- Direccionamiento y Planeación Institucional
- Gestión de la Información

Los procesos misionales son:

- Formulación y adopción de políticas
- Formulación de proyectos normativos (diseño de normas)
- Aplicación de políticas y/o normas
- Inspección, control y vigilancia

Como procesos de apoyo están:

- Gestión administrativa
- Gestión financiera
- Gestión de recursos informáticos
- Gestión documental
- Gestión de talento humano
- Gestión contractual
- Gestión jurídica

Y los procesos de evaluación son:

- Seguimiento y evaluación

- Mejoramiento continuo

4.4.3. ESTRUCTURA

El alcance del SGSI, cubre todas las dependencias que conforman el Ministerio de Justicia y del Derecho, es decir el Despacho del Ministro, los Viceministerios, la Secretaría General, los Grupos, Direcciones, Subdirecciones y Oficinas.

4.4.4. ACTIVOS DE INFORMACIÓN

El alcance del SGSI cubre todos los activos de información gestionados en el Ministerio de Justicia y del Derecho, así como la información que se genera en sus procesos y es remitida a otras partes interesadas. Esto incluye los siguientes tipos de activos:

- Información o tipo dato: Todos los archivos, documentos, bases de datos que sean de interés para la organización y que son necesarios para su gestión, cumplimiento normativo, misional y de sus procesos. Dependiendo del tipo de soporte, medio de creación y almacenamiento se clasifica como digital, electrónica o análoga, de acuerdo con la Ley de Transparencia y Acceso a la Información Pública.
- Hardware: los elementos físicos de los sistemas de información y comunicaciones son el medio utilizado para realizar la captura, procesamiento, almacenamiento, uso, difusión y divulgación de la información. Incluye toda la infraestructura tecnológica que soporta la gestión de los procesos del Ministerio, como servidores, firewall, switches, computadores personales de escritorio y portátiles, etc.
- Software: Son todos los componentes lógicos requeridos para la operación de las plataformas tecnológicas de la Entidad y que contribuyen al procesamiento de la información de los procesos de del Ministerio, en especial aplicaciones y sistemas de información.
- Infraestructura: ubicaciones físicas que prestan servicios relacionados con la seguridad de la información. Pueden ser edificios, oficinas o secciones especiales de la Entidad (como archivo y data center).
- Personas (roles): Roles desempeñados por funcionarios y/o contratistas que debido a la criticidad de la información que manejan o su acceso privilegiado a los sistemas de información, son representativos para la seguridad de la información de la Entidad.

El alcance del SGSI también abarca la infraestructura de redes y comunicaciones del Ministerio de Justicia y del Derecho.

4.4.5. SERVICIOS A LA CIUDADANÍA

El Sistema de Gestión de Seguridad de la Información cobija los servicios prestados por la Entidad a la ciudadanía, así como los trámites disponibles; los cuales están publicados en la página web del Ministerio de Justicia y del Derecho.
https://www.minjusticia.gov.co

4.5. ROLES Y RESPONSABILIDADES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Sistema de Gestión de Seguridad de la Información (SGSI), establecido en el Marco del Modelo de Seguridad y Privacidad de la Información (MSPI) de la Política de Gobierno Digital, debe ser transversal en el Ministerio de Justicia y del Derecho y por tal razón, con independencia de los cargos de los funcionarios y su tipo de vinculación, se han establecido una serie de obligaciones para el personal de la Entidad.

4.5.1. COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO

El Comité Sectorial de Gestión y Desempeño del Sector Justicia y del Derecho tiene entre sus funciones la dirección y articulación de las entidades en la operación de las directrices impartidas por la Presidencia de la República y el Ministerio de Tecnologías de la Información y las Comunicaciones, en materia de Gobierno y Seguridad Digital.
El Comité Institucional de Gestión y Desempeño del Ministerio de Justicia y del Derecho hará las veces de Comité de Seguridad de la Información para asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad, digital y de la información y tendrá a cargo las demás funciones que tengan relación directa con la implementación, desarrollo y evaluación del Modelo Integrado de Planeación y Gestión (el cual incluye las políticas de Seguridad Digital y Gobierno Digital).
Lo anterior con base en la Resolución 0254 del 20 de marzo de 2018, del Ministerio de Justicia y del Derecho.

4.5.2. PERSONAL DIRECTIVO

El(La) Señor(a) Ministro(a), los Viceministros, Secretario General, Directores, Subdirectores, Jefes de Oficina y Coordinadores de Grupo deben conocer y promulgar las políticas de seguridad de la información del Ministerio, promoviendo su cumplimiento entre los funcionarios a su cargo, con el fin de aunar esfuerzos de toda la organización en el cumplimiento de la política y objetivos del SGSI.

4.5.3. COMITÉ OPERATIVO DE SEGURIDAD DE LA INFORMACIÓN

El Comité Operativo de Seguridad de la Información ha sido delegado para planear y ejecutar las acciones efectivas de implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información del Ministerio de Justicia y del Derecho.
Esto incluye la recolección, preparación, revisión y difusión de toda la información requerida, aprobada por parte de los líderes de cada proceso, con el fin de realizar acciones en cuanto al inventario y evaluación de riesgos de activos de información, definición e implementación de controles, así como la verificación del cumplimiento y aplicación de las políticas de seguridad de la información. Igualmente desarrollarán acciones de sensibilización de los demás funcionarios y contratistas de sus procesos y promoverán que los mismos realicen el reporte de los eventos e incidentes de seguridad de la información detectados al Oficial de Seguridad de la Información de la Entidad.
Este Comité es liderado por el Oficial de Seguridad de la Información, está constituido por al menos un delegado de cada uno de los procesos del Ministerio de Justicia y del Derecho y se reúne periódicamente para establecer planes de trabajo, revisar el avance de los mismos, socializar entregables y evaluar la efectividad de las acciones tomadas.

4.5.4. OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

El Oficial de Seguridad de la Información es el rol encargado de liderar la planeación, implementación, mantenimiento y mejora del SGSI del Ministerio de Justicia y del Derecho.
Sus responsabilidades son:

- Coordinar y controlar el avance en la planeación, implementación, mantenimiento y mejora del SGSI de la Entidad.
- Gestionar la definición y actualización, documentación y difusión de las políticas, metodologías y procedimientos del Ministerio, en materia de seguridad de la información.
- Gestionar la realización y actualización del análisis y evaluación del riesgo sobre los activos de información de la Entidad, por parte de los propietarios de los mismos.
- Dar lineamientos para la definición e implantación de los controles de seguridad de la información de la Entidad.
- Coordinar con la Oficina de Control Interno que las auditorías internas del SGSI, se planeen y realicen, de acuerdo con las necesidades del sistema y en cumplimiento de los requisitos de la Norma ISO/IEC 27001:2013.
- Definir y comprobar la aplicación de las políticas y los procedimientos asociados a la seguridad de la información en la Entidad.
- Preparar y presentar informes de avances, resultados de desempeño y eficacia y los planes de acción del SGSI en el Marco del MSPI, a la Alta Dirección y entes de control internos y externos, según se requiera.
- Velar por el cumplimiento y difusión de todos los componentes y requisitos del SGSI, implementados en la Entidad.
- Propender por la seguridad de la información en todos los procesos de la Entidad, en especial en los procesos estratégicos y misionales.
- Verificar la ejecución del plan de seguridad informática de la Entidad, definido y en ejecución.
- Promover la definición, ejecución y evaluación de planes de sensibilización y concienciación para los funcionarios del Ministerio, en el tema de seguridad de la información.
- Solicitar a las áreas responsables, la ejecución de acciones de formación para los funcionarios y contratistas de la Entidad, en materia de seguridad de la información.
- Autorizar el escalamiento interno y externo de incidentes de seguridad de la información con autoridades y entes competentes (SIJIN, Fiscalía, ColCERT, CSIRT,etc)
- Mantenerse actualizado en nuevas amenazas y vulnerabilidades existentes, con el fin de realizar una gestión proactiva de los riesgos de seguridad de la información.
- Determinar los requisitos legales vigentes del SGSI, evaluar el avance de la Entidad y proponer medidas para mantener el cumplimiento de la base legal establecida en la materia.

4.5.5. LIDER DE SEGURIDAD INFORMÁTICA

- Establecer los controles y medidas técnicas y administrativas necesarias para asegurar la infraestructura tecnológica, los sistemas y los activos de información del Ministerio.

- Evaluar, emitir conceptos y avalar las nuevas soluciones o plataformas tecnológicas a adquirir o implementar en la Entidad, teniendo en cuenta el cumplimiento de los requisitos de seguridad de la información.
- Analizar, evaluar y seleccionar herramientas que faciliten la labor de seguridad de la información para su implementación en la Entidad.
- Liderar la creación, actualización e implementación del plan de seguridad informática.
- Gestionar los riesgos y eventos de seguridad y su registro, solución y/o escalamiento interno y externo con autoridades y entes competentes (SIJIN, Fiscalía, ColCERT, CSIRT, etc), previa autorización del Oficial de Seguridad de la Información.
- Liderar, verificar y controlar la implementación de controles de seguridad informática sobre las plataformas tecnológicas del Ministerio, de acuerdo con las políticas y evaluaciones de riesgos generadas en el marco del SGSI.
- Para el cumplimiento de estas responsabilidades, contará con el equipo de ingenieros encargados de las plataformas tecnológicas y soluciones de software de la Entidad.
- Liderar la protección, mediante recursos lógicos, de los datos que se procesan, almacenan o transmiten a través de la infraestructura tecnológica del Ministerio, así como la correcta utilización de los servicios de Internet, correo electrónico y herramientas colaborativas; así como el monitoreo, detección y reporte de anomalías.

4.5.6. SUBDIRECCION DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN

La Subdirección velará por la correcta utilización de los recursos tecnológicos de hardware, software y comunicaciones de la Entidad, como son los equipos de cómputo, sistemas de información, redes informáticas, procesamiento de datos e información y los canales de comunicación.
Para todo lo anterior, esta dependencia contará con el aval de la Dirección de Tecnologías y Sistemas de Información; así como con el compromiso del personal directivo y de todos los funcionarios y contratistas de la Entidad.

4.5.7. SERVIDORES PÚBLICOS DEL MINISTERIO DE JUSTICIA Y DEL DERECHO

Los servidores públicos del Ministerio de Justicia y del Derecho, sin importar su tipo de vinculación (carrera administrativa, planta provisional, libre nombramiento y remoción, contratistas, practicantes) son responsables de conocer, aplicar y dar estricto cumplimiento a las políticas, normas y procedimientos de la Entidad, en materia de seguridad de la información.

4.6. POLÍTICAS ESPECÍFICAS POR DOMINIOS DE CONTROL

4.6.1. POLITICAS DEL DOMINIO DE CONTROL: CUMPLIMIENTO

4.6.1.1. CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

4.6.1.1.1. DERECHOS DE PROPIEDAD INTELECTUAL: POLÍTICA ANTIFRAUDE Y ANTIPIRATERÍA

4.6.1.1.1.1. OBJETIVO

La política antifraude y antipiratería establecida por el Ministerio de Justicia y del Derecho tiene como objetivo evitar, detectar y sancionar conductas encaminadas a la vulneración de los derechos de autor, que busquen el beneficio propio o para terceros de una obra o creación intelectual; así como actos u omisiones que induzcan a error a los funcionarios de la entidad, con la finalidad de obtener una ventaja financiera o de cualquier tipo, para evitar una obligación.

4.6.1.1.1.2. ALCANCE

La presente política aplica para todos los funcionarios y contratistas de la Entidad, quienes deben velar por el cumplimiento de la normatividad vigente respecto a las creaciones científicas, literarias y artísticas, así como los derechos de propiedad intelectual que pueda poseer una persona física o jurídica, sin desconocer los casos en los que se cumplan los requisitos legales para la patentabilidad del software.

4.6.1.1.1.3. DESARROLLO

El Ministerio de Justicia y del Derecho velará porque se respeten las normas de protección a la propiedad intelectual y los derechos de autor. La Entidad se compromete a evitar el uso indebido de cualquier tipo de software o archivo de audio, digital o video que no esté debidamente licenciado, así como cualquier forma de uso indebido de las invenciones de carácter intelectual. El Ministerio asume el compromiso de combatir la realización por parte de sus funcionarios y contratistas, de actos contrarios a la Constitución, al Estatuto Anticorrupción o al Código Disciplinario, que puedan ser considerados como fraude o piratería.

La alta dirección del Ministerio es responsable por la administración, prevención y detección del riesgo de fraude y piratería, acompañando en todo momento las políticas establecidas por el Gobierno Nacional sobre el particular. Todos los funcionarios y contratistas de la Entidad son responsables por evitar incurrir en alguna de estas conductas y denunciar su detección, en caso tal de tener conocimiento de las mismas. Así mismo, la Subdirección de Tecnologías y Sistemas de Información tiene a cargo la gestión del licenciamiento del software adquirido por la Entidad, de acuerdo con las políticas de seguridad de la información y de tecnologías de la información.

4.6.2. POLITICAS DEL DOMINIO DE CONTROL: GESTIÓN DE ACTIVOS

4.6.2.1. OBJETIVO

Determinar lineamientos para un manejo óptimo por parte de los funcionarios y contratistas de la Entidad, de los activos de información que se encuentran bajo la gestión de la Entidad, con el fin de custodiar, proteger y asegurar su confidencialidad, disponibilidad e integridad.

4.6.2.2. ALCANCE

La presente política aplica para todos los funcionarios y contratistas de la Entidad, quienes deben velar por el cuidado, uso correcto y protección de los activos de información a los cuales tienen acceso por motivo de su gestión, labores asignadas u obligaciones contractuales. Igualmente se debe hacer extensiva a los terceros, proveedores o colaboradores, a través de los correspondientes contratos o acuerdos aplicables. Esto abarca la información o activos tipo dato en formato análogo, digital o electrónico[4], la infraestructura, roles, hardware y software gestionado por el Ministerio de Justicia y del Derecho.

4.6.2.3. DESARROLLO

El Ministerio de Justicia y del Derecho se compromete a velar por el buen uso, gestión y custodia de los activos de información administrados por la Entidad, con motivo de su misionalidad y en cumplimiento de sus obligaciones legales y contractuales, de acuerdo con la identificación de activos reflejada en los inventarios aprobados por los responsables en todas las dependencias, así como la responsabilidad y custodia determinados para ellos.
La gestión de activos, así como la gestión de riesgos de seguridad de la información se definirá y realizará en el marco del Sistema de Gestión de Seguridad de la Información de la Entidad, con base en la normatividad vigente, las buenas prácticas basadas en la serie de normas ISO 27000 y el Modelo de Seguridad y Privacidad de la Información de MinTIC.

4.6.2.3.1. RESPONSABILIDAD POR LOS ACTIVOS DE INFORMACIÓN

Se elabora y aprueba el inventario de activos de información tipo dato, del cual se obtiene el registro de activos de información y el índice de información clasificada y reservada del Ministerio de Justicia y del Derecho, en cumplimiento de la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional – Ley 1712 de 2014. Igualmente se elabora y actualiza un inventario de hardware y software a cargo de la Subdirección de Tecnologías y Sistemas de Información, así como un inventario de infraestructura y roles, administrado por el Oficial de Seguridad de la Información o quien haga sus veces. Cada uno de estos inventarios contiene la identificación de los activos, clasificación y valor para la Entidad; así como el responsable de la dependencia a cargo de los activos de la información (rol denominado "propietario" en las

[4] Activo en formato análogo: información que se encuentra guardada en soportes físicos como: papel, video, casettes, cinta, película, microfilm y otros.
Activo digital: documento que permite la reproducción de información que se generó de manera analógica o en formato físico, en uno que sólo puede leerse o interpretarse por computador.
Activo electrónico: registro de la información generada, recibida, almacenada, y comunicada por medios electrónicos, que permanece en estos medios durante su ciclo vital.
Conceptos extraídos del Acuerdo 027 de 2006 del Archivo General de la Nación.

guías de MinTIC) y los custodios para cada uno de ellos. Todos los inventarios de activos serán actualizados al menos una vez al año.

Los responsables de las dependencias a cargo de los activos de información tienen el compromiso de[5]:

- Realizar y mantener actualizado y veraz el inventario de activos de información.
- Asegurar que la confidencialidad de la información contenida en los activos tipo dato ha sido categorizada como clasificada y/o reservada, según lo previsto en la normatividad vigente.
- Delegar los custodios para cada activo según sus competencias y las funciones correspondientes a su cargo.
- Controlar el cumplimiento de las responsabilidades relativas a los activos de información, por parte de los custodios designados.
- Definir y revisar periódicamente las restricciones y clasificaciones de acceso a los activos, teniendo en cuenta las políticas de control de acceso aplicables.
- Asegurarse del manejo apropiado del activo cuando es eliminado o destruido, de acuerdo con la normatividad vigente, las políticas y procedimientos de gestión de bienes, gestión documental y las tablas de retención documental de la Entidad.

Los custodios de los activos de información tienen la responsabilidad de gestionar la aplicación de los controles necesarios para mantener la confidencialidad, integridad y disponibilidad de los activos de información; en el marco de las políticas de Seguridad de la información del Ministerio de Justicia y del Derecho y en cumplimiento de la Ley 1712 de 2014 – Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, Ley 1581 de 2012 de Protección de Datos Personales, así como cualquier normativa que las reglamente, reforme, modifique o adicione.

Lo anterior sin perjuicio de la responsabilidad de la Subdirección de Tecnologías y Sistemas de Información, de aplicar los controles de seguridad informática definidos; así como de hacer un uso responsable de los accesos privilegiados a los sistemas de información y los datos. Se pueden presentar casos en los cuales los activos de información como las bases de datos de sistemas de información y portales sean custodiadas técnicamente por parte de dicha Subdirección, lo cual implica la prestación de los servicios tecnológicos de administración, soporte, mantenimiento y copias de respaldo de las bases de datos. Sin embargo, la calidad de la información será responsabilidad de la(s) dependencia(s) que, de acuerdo con sus funciones, deba(n) gestionarla.

Los activos de información que pertenecen o están bajo la gestión del Ministerio de Justicia y del Derecho deben utilizarse exclusivamente con propósitos funcionales, en concordancia con la ética y en cumplimiento de la normatividad y políticas internas vigentes.

Para el uso aceptable de activos de hardware, software y en general recursos tecnológicos, consultar las Políticas de Tecnologías de la Información y las Comunicaciones vigentes y publicadas dentro de la documentación del Sistema Integrado de Gestión.

[5] En virtud de lo expuesto en el Decreto 2573 de 2014, compilado en el Decreto 1078 de 2015, Decreto Único Reglamentario del Sector TIC, y la Guía para la gestión y clasificación de activos de información de MinTic (2016).

En el evento en que se dé por terminada la relación contractual o laboral con el MJD o se presente un cambio de cargo, rol, funciones o un traslado a otra dependencia de la Entidad, los funcionarios o contratistas deberán realizar la devolución formal de los activos de información que en su momento le habían sido asignados o que se encontraba gestionando en virtud de sus funciones o actividades a cargo, de conformidad con los procesos de Gestión de Recursos Informáticos y de Administración del Talento Humano vigentes.

4.6.2.3.1.1. Protección de la confidencialidad

Cada funcionario, contratista o tercero que haga uso de un activo de información debe verificar el nivel de clasificación de confidencialidad del activo de acuerdo con el inventario de activos de información. Si de acuerdo con su rol no debe tener acceso, se abstendrá de hacerlo, informará del hecho a su jefe inmediato o supervisor de contrato y lo reportará como un evento de seguridad de la información.

El usuario que accede a la información únicamente puede compartir dicha información con los usuarios debidamente autorizados, de acuerdo con los controles definidos por el responsable de la dependencia a cargo del activo. Es indispensable contar con la autorización expresa de dicho responsable para suministrar o intercambiar información clasificada o reservada con otras personas de la entidad o entes externos.

4.6.2.3.1.2. Protección de la integridad

Cada funcionario, contratista o tercero que haga uso de un activo de información debe verificar el nivel de clasificación de integridad del activo de acuerdo con el inventario de activos de información. Si de acuerdo con su rol debe tener restricciones para modificar la información, debe abstenerse de hacerlo, informar del hecho a su jefe inmediato o supervisor de contrato y reportarlo como un evento de seguridad de la información.

4.6.2.3.1.3. Protección de la disponibilidad

Cada funcionario, contratista o tercero que haga uso de un activo de información debe verificar el nivel de clasificación del activo frente a su disponibilidad, de acuerdo con el inventario de activos de información. El usuario que tenga acceso y pueda realizar acciones que afecten la disponibilidad del activo, como por ejemplo eliminarlo, destruirlo, sustraerlo o cambiar su ubicación, debe validar previamente con el responsable de la dependencia encargada de los activos de información. Dicho responsable debe velar porque se mantengan las especificaciones físicas, técnicas y ambientales necesarias para la adecuada conservación de los activos.

4.6.2.3.2. CLASIFICACIÓN DE LA INFORMACIÓN

Los activos de información se clasifican de acuerdo con la criticidad de su confidencialidad, integridad y disponibilidad y se asigna un valor, de acuerdo con los criterios definidos para la Entidad. La clasificación se encuentra registrada en el inventario de activos de información y permite la identificación de los activos críticos. Ver detalles en el documento de lineamientos para la identificación, clasificación y valoración de activos de información del Ministerio de Justicia y del Derecho.

De acuerdo con la clasificación de los activos de información en cuanto a su confidencialidad, dada por la información clasificada y/o reservada que contengan y en aplicación de la normatividad, las políticas de gestión documental, políticas de TIC y procedimiento de Gestión de Acceso a Recursos Informáticos, los responsables de las dependencias a cargo de los activos deben definir y revisar los permisos de acceso a los mismos, los cuales serán aplicados por los administradores de los sistemas de información o custodios.

Los activos con información clasificada y reservada deberán ser etiquetados de manera que puedan ser fácilmente identificados por parte de los usuarios de los mismos.

En el caso de generar, compartir o enviar copias de este tipo de activos a otras dependencias o entes externos, en el desarrollo de las funciones de la Entidad y con observancia de la normatividad aplicable, el responsable de la dependencia a cargo del activo deberá asegurar la firma de acuerdo de confidencialidad. Las copias serán igualmente etiquetadas, controladas y se debe asegurar la protección de las mismas con controles similares a los aplicados para los activos originales, de acuerdo con su nivel de clasificación.

4.6.2.3.3. MANEJO DE MEDIOS

El uso de medios removibles como USBs o discos duros externos por ejemplo, debe limitarse con el fin de evitar que se extraiga información clasificada o reservada, a menos que sea autorizado por parte del responsable de la dependencia a cargo del activo. Si se autoriza la copia a algún medio removible, la información debe ser encriptada y protegida físicamente con el fin de evitar acceso por parte de personal no autorizado; para lo cual se solicitará soporte a la Mesa de Ayuda, de la Subdirección de Tecnologías y Sistemas de Información. En ningún caso se podrá realizar extracción o retiro de los activos de información originales que deban ser custodiados en la Entidad (sean análogos, digitales o electrónicos).

Los custodios delegados de los activos deberán gestionar el respaldo de la información clasificada o reservada, de manera que se mantenga una o varias copias de los activos análogos, digitales y electrónicos cuya disponibilidad sea crítica, preferiblemente en medios separados y/o diferentes ubicaciones, con el fin de reducir los riesgos de daño o pérdida de información. La Subdirección de Tecnologías y Sistemas de Información aplicará los controles requeridos para la información digital y electrónica, de acuerdo con las políticas, mejores prácticas, análisis de riesgos, con base en los recursos disponibles y en la gestión de los custodios.

Se debe garantizar que la información clasificada o reservada sea eliminada definitivamente de los medios a desechar o donar, de manera que ésta no pueda ser recuperada por personas no autorizadas. Para implementarlo, las dependencias deberán realizar una solicitud a la Mesa de Ayuda de la Subdirección de Tecnologías y Sistemas de Información.

El Grupo de Gestión Documental de la Secretaría General está a cargo de la supervisión del contrato con un servicio de transporte y mensajería e igualmente, la Subdirección de Tecnologías y Sistemas de Información tiene a cargo la supervisión del contrato con un proveedor de custodia de cintas magnéticas, para el almacenamiento de copias de respaldo de la información de los servidores. Ambos proveedores deben cumplir con los requisitos de protección contra daño físico de los medios transportados, de manera que se conserven apropiadamente, se aíslen de factores ambientales como calor, humedad o campos electromagnéticos y se garantice que terceros no autorizados no puedan tener acceso a dichos medios.

4.6.3. MARCO LEGAL

- Constitución Política de Colombia.
- Ley 23 de 1982- Ley sobre Derechos de autor.
- Decreto 1360 de 1989, Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor.
- Ley 44 de 1993, por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944.

- Ley 599 de 2000-Codigo Penal Colombiano.
- Ley 734 de 2002- Código Disciplinario Único.
- Ley 906 de 2004 - Código de Procedimiento Penal Colombiano.
- Ley 1273 de 2009 - Modifica el Código Penal, crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Ley 1437 de 2011 - Código de Procedimiento Administrativo y de lo Contencioso Administrativo
- Estatuto Anticorrupción - Ley 1474 de 2011.
- Ley 1581 de 2012- Ley de Protección de Datos Personales.
- Decreto 1377 de 2013 – Reglamenta parcialmente la Ley 1581 de 2012 y se dictan disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014 – Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- Leyes y normas que aprueban o adoptan convenios internacionales en materia de derechos de autor, propiedad intelectual e industrial.
- Resolución 3564 de 2015 del Ministerio de Tecnologías de la Información y las Comunicaciones.
- Decreto 1008 de 2018, Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

4.6.4. SANCIONES

Es deber de todos los funcionarios y contratistas del Ministerio de Justicia y del Derecho, poner en conocimiento de su jefe directo, del Grupo de Control Disciplinario Interno, el Oficial de Seguridad de la Información o quien haga sus veces, así como de las autoridades pertinentes, cualquier evento sobre fraude o piratería, para lo cual puede utilizar los diferentes canales de denuncia. El Ministerio protegerá los datos y la identidad del denunciante.

Cualquier tipo de infracción o incumplimiento de esta política será objeto de las acciones y sanciones legales pertinentes, las cuales se rigen conforme a los parámetros establecidos en Código Disciplinario Único, Código Penal y en el Código de Ética del Ministerio de Justicia y del Derecho (Resolución 867 del 27 de diciembre de 2012).

5. FORMATOS Y REGISTROS UTILIZADOS

CLASE	TITULO DEL DOCUMENTO	CÓDIGO

6. CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN DE CAMBIOS
1	Creación de la política
2	Ajuste de la política debido al cambio físico de sede del MJD. Inclusión del formato F-RI-G01-01 Planilla de Control de Acceso Data Center Formalización de la Política de seguridad de la información en el Sistema Integrado de Gestión
3	Ajuste general de toda la política conforme a los lineamientos que en materia de seguridad de la información, el Ministerio viene implementado. Eliminación del formato F-RI-G01-01 Planilla de Control de Acceso Data Center
4	Inclusión del alcance y de los roles y responsabilidades del Sistema de Gestión de Seguridad de la Información, política antifraude y antipiratería y política de activos de información.

RESPONSABILIDAD Y AUTORIDAD		
Elaboró / Actualizó:	**Revisó:**	**Aprobó:**
Firma:	Firma:	Firma:
Nombre: Adriana Aranguren	Nombre: Flavio Augusto Rodríguez Gutiérrez	Nombre: Carlos Eduardo Pimienta Tatis
Cargo: Contratista	Cargo: Subdirector de Tecnologías y Sistemas de Información	Cargo: Director de Tecnologías y Gestión de Información en Justicia