# POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

**Versión 3**

**DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA – DANE y FONDO ROTATORIO DEL DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA – FONDANE**

**2023**

# Contenido

# 1. Justificación y antecedentes

La Alta Dirección1 del DANE-FONDANE, adoptan la política general de seguridad de la información, con el propósito de salvaguardar, conservar y proteger la información que administra en el ejercicio de sus funciones. Esta política define los lineamientos para garantizar la confidencialidad, integridad y disponibilidad de la información.

El Modelo de Seguridad y Privacidad de la Información- MSPI, establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones- MinTIC2, es el referente utilizado para la formulación de la política; el cual recopila las buenas prácticas, nacionales e internacionales, suministrando los requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo en materia de seguridad de la información. En el ejercicio de la revisión de la política general se identificó la necesidad de actualizarla en los siguientes aspectos:

- Incluir el alcance que determine los límites de la implementación del MSPI.
- Excluir los asuntos relacionados con privacidad de la información, teniendo en cuenta que el DANE-FONDANE cuenta con una política y gobernanza propia para abordar el tratamiento y la protección de datos personales.
- Excluir la descripción de las políticas complementarias, teniendo en cuenta que se desarrollan en el manual de políticas de seguridad.
- Incluir indicadores que midan el cumplimiento de los objetivos de esta política.

[1] La Alta Dirección en el DANE es el Director, Subdirector y Representante legal de FONDANE. Decreto Ley 770 de 2015 Por el cual se establece el sistema de funciones y de requisitos generales para los empleos públicos correspondientes a los niveles jerárquicos pertenecientes a los organismos y entidades del Orden Nacional.

2 https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_1.pdf

## 2. Marco normativo

El artículo 15 de la Constitución Política de Colombia se establece que "(…) Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas (…)".

El artículo 74 de la Carta Política preceptúa que "(…) Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la Ley. El secreto profesional es inviolable (…)".

La 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.

Mediante la Ley 1581 de 2012 se expidió el Régimen General de Protección de Datos Personales, el cual, de conformidad con su artículo 1, tiene por objeto "(…) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma (…)".

La Ley 1712 de 2014, Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, tiene por objeto regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información, y constituye el marco general de la protección del ejercicio del derecho de acceso a la información pública en Colombia.

El artículo 133 de la Ley 1753 de 2015 "Por la cual se expide el Plan Nacional de Desarrollo 2014- 2018 "Todos por un nuevo país", establece la integración de todos los componentes del Sistema de Gestión de Calidad con el Sistema de Control Interno en un solo Sistema de Gestión a implementar en todas las entidades públicas del nivel nacional y territorial.

Mediante el Decreto Nacional 1078 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones", definió la estrategia de seguridad y privacidad de la información, estableciendo que la misma no se limita a este sólo aspecto, sino que comprende la seguridad digital y los requerimientos necesarios para garantizar la continuidad en la prestación de los servicios digitales, en los siguientes términos: "ARTÍCULO 2.2.17.5.6. Seguridad de la información y Seguridad Digital. Los actores que traten información en el marco del presente título deberán contar con una estrategia de seguridad y privacidad de la información, seguridad digital y continuidad de la prestación del servicio en la cual, deberán hacer periódicamente una evaluación del riesgo de seguridad digital, que incluya una identificación de las mejoras a implementar en su Sistema de Administración del Riesgo Operativo. Para lo anterior, deben contar con normas, políticas, procedimientos, recursos técnicos, administrativos y humanos necesarios para gestionar efectivamente el riesgo. En ese sentido, deben adoptar los lineamientos para la gestión de la seguridad de la información y seguridad digital que emita el Ministerio de Tecnologías de la Información y las Comunicaciones".

El artículo 5° de la ley 79 de 1993 establece que los datos individuales solicitados por el DANE en el desarrollo de Censos y Encuestas se encuentran amparados por la reserva estadística, la cual constituye una plena garantía de la intangibilidad del derecho a la intimidad de las personas naturales y jurídica. En virtud de la reserva estadística, los datos que sirven como insumo para la producción de información estadística no podrán darse a conocer al público ni a las entidades u organismos oficiales, ni a las autoridades sino únicamente en resúmenes numéricos, que no hagan posible deducir de ellos, información alguna de carácter individual para fines distintos a los estadísticos.

El Decreto 1499 de 2017, en su artículo 2.2.22.2.1 relacionado con las Políticas de Gestión y Desempeño Institucional indica que las políticas de Desarrollo Administrativo de que trata la Ley 489 de 1998, formuladas por el Departamento Administrativo de la Función Pública y los demás líderes, se denominarán políticas de Gestión y Desempeño Institucional y comprenderán, entre otras, la de Gobierno Digital, antes Gobierno en Línea, y la de Seguridad Digital.

Mediante el Decreto Nacional 1008 de 2018, que modificó el Decreto 1078 de 2015, se establecen "(…) lineamientos generales de la Política de Gobierno Digital para Colombia, antes estrategia de Gobierno en Línea, la cual desde ahora debe ser entendida como: el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital"

El DANE- FONDANE expidió la Resolución 0677 del 11 de junio de 2020, "Por la cual se conforma el Comité de Seguridad de la Información del Departamento Administrativo Nacional de Estadística — DANE y del Fondo Rotatorio del Departamento Administrativo Nacional de Estadística - FONDANE", en la cual se establecen funciones y organización del comité de seguridad de la Información de las referidas entidades.

El DANE-FONDANE expidió la Resolución 0602 del 31 de mayo de 2021, "Por el Departamento Administrativo Nacional de Estadística- DANE y el Fondo Rotatorio del cual el Departamento Administrativo Nacional de Estadística-FONDANE adoptan las políticas de Gobierno Digital y Seguridad Digital, se designa al Líder de Gobierno y Seguridad Digital y se dictan otras disposiciones", en la cual se designa al Subdirector o su delegado del nivel directivo o asesor como representante de la Alta Dirección para el desarrollo de las citadas políticas, como responsable de su implementación al Jefe de la Oficina de Sistemas en coordinación con la Oficina Asesora de Planeación y como instancia orientadora al Comité de Seguridad de la Información en lo relacionado con seguridad de la información.

Mediante documento CONPES 3854 de 2016 - Política Nacional de Seguridad Digital, se establece un marco institucional claro y preciso en torno a la seguridad digital.

Mediante Documento CONPES 3995 de 2020 - Política Nacional de Confianza y Seguridad Digital, se establecen medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías.

En la directiva presidencial 03 de 2021 emite lineamientos para el uso de servicios en nube, inteligencia artificial, gestión de datos y seguridad digital para entidades públicas de la rama ejecutiva de orden nacional e invita a su aplicación a entidades territoriales, así como a la rama legislativa y judicial.

El Ministerio de Tecnologías de la Información y las Comunicaciones expidió la Resolución 500 del 10 de marzo de 2021, "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital", en la cual establece los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establece los lineamientos y estándares para la estrategia de seguridad digital.

El DANE-FONDANE expidió la Resolución 644 del 20 de abril de 2022 "Por medio del cual se establecen niveles, roles y responsabilidades en materia de Seguridad de la Información y se designa al Oficial de Seguridad de la Información del Departamento Administrativo Nacional de Estadística- DANE y el Fondo Rotatorio del cual el Departamento Administrativo Nacional de Estadística-FONDANE".

## 3. Política general de seguridad de la información

La Política General de Seguridad de la información del DANE-FONDANE, comprende el compromiso de la alta dirección, los principios y la adopción de las políticas complementarias.

La Política General de Seguridad de la información de la DANE-FONDANE, se revisará y de ser necesario se actualizará cada dos años o antes, si ocurren cambios significativos, para asegurar su pertinencia, adecuación y mejora continua.

### 3.1. Objetivos

La presente política busca mediante su implementación el logro de los siguientes objetivos:

- Conservar, salvaguardar y proteger la información administrada por el DANE-FONDANE, para preservar la confidencialidad, integridad y disponibilidad de la información.

Este objetivo se mide a través de los siguientes indicadores que tienen el mismo peso ponderado:

(Indicador: controles implementados/controles a implementar).

(Indicador: actividades incluidas en el plan de sensibilización/ actividades ejecutadas).

(Indicador: eventos o incidentes atendidos/ eventos o incidentes reportados o detectados).

(Indicador: vulnerabilidades atendidas/vulnerabilidades detectadas).

- Asegurar el cumplimiento de los requerimientos legales y regulatorios vigentes en materia de seguridad de la información, para evitar sanciones, demandas y pérdida de imagen del DANE-FONDANE.
  (Indicador: resultado del autodiagnóstico del MSPI).
- Minimizar los riesgos de seguridad de la información, acorde con las necesidades institucionales, para asegurar que los activos cumplan con los atributos de integridad, confidencialidad y disponibilidad.
  (Indicador: riesgos materializados).

### 3.2. Alcance

La política general de seguridad de la información es de carácter transversal y abarca todos los procesos institucionales de la entidad.

Todos los servidores públicos, contratistas, terceros y partes interesadas deben cumplir con la presente política, las políticas complementarias, sus procedimientos y protocolos, cuando se recolecte, procese, almacene, recupere, intercambie, consulte

datos o información, en el desarrollo de la misión institucional y cumplimiento de sus objetivos estratégicos.

### 3.3. Compromiso de la Alta Dirección

La Alta Dirección[3] del DANE-FONDANE está comprometida con la adopción e implementación del Modelo de Seguridad y Privacidad de la Información, para proteger, preservar y administrar la confidencialidad, integridad y disponibilidad de los activos de información en los procesos institucionales. Así como, la seguridad digital y la gestión de la continuidad de la operación, orientados a la mejora continua y el alto desempeño, con la finalidad de contribuir a la producción, disponibilidad y calidad de la información estadística estratégica, y dirigir, planear, ejecutar, coordinar, regular y evaluar la producción y difusión de información oficial básica. Lo anterior, mediante la administración de los riesgos de seguridad de la información, previniendo y mitigando el impacto de incidentes y dando cumplimiento a los requisitos legales y reglamentarios con la implementación de controles establecidos en el estándar internacional ISO 27001 Anexo A.

### 3.4. Principios

Los principios que se describen a continuación están orientados a cumplir con los tres atributos de la seguridad de la información como son: la integridad, la disponibilidad y la confidencialidad.

- Usar apropiado de los activos para los fines previstos y para cumplir con los objetivos institucionales.
- Proteger la información generada, transmitida, procesada y resguardada, en los procesos de negocio y su infraestructura tecnológica, de los riesgos que se puedan generan por los accesos otorgados o el uso indebido de la información. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

3 La Alta Dirección en el DANE es el Director, Subdirector y Representante legal de FONDANE. Decreto Ley 770 de 2015 Por el cual se establece el sistema de funciones y de requisitos generales para los empleos públicos correspondientes a los niveles jerárquicos pertenecientes a los organismos y entidades del Orden Nacional.

- Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos, mediante la implementación de controles de acceso a la información, sistemas y recursos de red.
- Controlar la operación de los procesos de negocio, garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- Garantizar que la seguridad sea parte integral de los procesos, mediante la aplicación de políticas, análisis de riesgos y buenas prácticas en temas de seguridad de la información.
- Promover la gestión adecuada de incidentes, eventos y debilidades de seguridad para lograr el mejoramiento continuo del modelo de seguridad.
- Asegurar la disponibilidad de los procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos e incidentes de seguridad.
- Cumplir las obligaciones legales, regulatorias y contractuales establecidas.

### 3.5. Políticas complementarias de seguridad de la información

La Alta Dirección4 DANE-FONDANE define las políticas complementarias de seguridad de la información; el detalle de cada una se incluirá en el manual de políticas de seguridad.

## 4. Roles y responsabilidades

Los roles y responsabilidades se encuentran definidos por Resolución.

## 5. Cumplimiento

Todos los servidores públicos, contratistas, terceros y partes interesadas del DANE-FONDANE, que en el ejercicio de sus actividades utilicen información y servicios TI de las citadas entidades deben cumplir con la presente política, políticas

4 La Alta Dirección en el DANE es el Director, Subdirector y Representante legal de FONDANE. Decreto Ley 770 de 2015 Por el cual se establece el sistema de funciones y de requisitos generales para los empleos públicos correspondientes a los niveles jerárquicos pertenecientes a los organismos y entidades del Orden Nacional.

complementarias, sus procedimientos y protocolos. Su incumplimiento, traerá consigo las consecuencias legales previstas en la normativa vigente.

## 6. Glosario

Activo: Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 2016, pág. 56).

Amenaza: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización. (ISO/IEC 27000:2016).

Control: Medida que modifica el riesgo. (NTC ISO 31000:2011). Medios para gestionar el riesgo e incluye políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal. (MGRSD 2018).

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad. (DAFP 2018).

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Infraestructura crítica cibernética nacional: Aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública. (CONPES 3854, pág. 29).

Integridad: Propiedad de exactitud y completitud. (DAFP 2018).

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Privacidad: Por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente. (MSPI).

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).

Riesgo de seguridad de la información: 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).

Riesgo de seguridad digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas. (DAFP 2018).

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

Seguridad digital: Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país. (CONPES 3854 2016, pág. 29).

Sistema de Gestión de Seguridad de la Información- SGSI: 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).

Partes interesadas: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad. (MSPI).

Vulnerabilidad: Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas. (Basado en DAFP 2018).

## 7. Referentes nacionales e internacionales

- Modelo de Seguridad y Privacidad de la Información establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones (2021).

## 8. Bibliografía

Departamento Administrativo de la Función Pública (2022). Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Recuperado de https://www.funcionpublica.gov.co/documents/28587410/34299967/Guia_administracion_riesgos_capitulo_riesgo_fiscal.pdf/50bff85a-70c6-dd15-68f5-6cd2ea2a8707?t=1677003002032

Ministerio de Tecnologías de la Información y las Comunicaciones (2021). Modelo de Seguridad y Privacidad de la Información versión 4. Recuperado de https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_1.pdf