

Departamento Administrativo
Nacional de Estadística



OFICINA DE SISTEMAS


**POLÍTICA GENERAL DE SEGURIDAD
DE LA INFORMACIÓN**

Noviembre 2017

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 2 PÁGINA: 1
ELABORÓ: Profesional Oficina de Sistemas	REVISÓ: Coordinador Grupo de Plataforma Tecnológica y Sistemas de Información	APROBÓ: Jefe Oficina Sistemas

TABLA DE CONTENIDO

INTRODUCCIÓN.....	2
1. OBJETIVO	3
2. ALCANCE.....	3
3. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACION	3
4. LINEAMIENTOS	4
5. DESCRIPCIÓN DE TAREAS	4
6. DEFINICIONES.....	5
7. BIBLIOGRAFÍA	6

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 2 PÁGINA: 2
ELABORÓ: Profesional Oficina de Sistemas	REVISÓ: Coordinador Grupo de Plataforma Tecnológica y Sistemas de Información	APROBÓ: Jefe Oficina Sistemas


INTRODUCCIÓN

El Departamento Administrativo Nacional de Estadística - DANE, como ente rector de la información estadística, debe garantizar su producción, disponibilidad, confiabilidad, integridad y calidad. Por tal razón, propone una Política de seguridad de la información de carácter estratégica con el fin de reconocer su importancia.

El DANE reconoce la información y en especial los datos utilizados para producir estadísticas, como los activos más importantes de la entidad; por lo tanto, se compromete a proteger la privacidad, seguridad y gestión de su ciclo de vida, cumpliendo con los mandatos de la constitución y la ley de reserva estadística y promoviendo la confianza y cooperación de los ciudadanos.

Es importante que la seguridad de la información sea un requisito inherente a las actividades y procesos de la entidad, y nunca deberá ser una función adicional o no prioritaria.

El DANE establecerá los mecanismos para difundir, revisar, actualizar y consolidar la política, los lineamientos, y los demás componentes del Sistema de Gestión de la Seguridad de la Información y alinearlos de forma efectiva con los demás sistemas de gestión institucionales.

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 2 PÁGINA: 3
ELABORÓ: Profesional Oficina de Sistemas	REVISÓ: Coordinador Grupo de Plataforma Tecnológica y Sistemas de Información	APROBÓ: Jefe Oficina Sistemas

1. OBJETIVO

Este documento permite establecer la política y lineamientos sobre las cuales se debe direccionar el desarrollo de la seguridad de información del DANE, y los principios de actuación de todo el personal que tenga acceso o responsabilidades sobre la información en la entidad.

Mantener la Política de Seguridad de la Información actualizada, vigente y operativa dentro del marco determinado por los riesgos globales identificados en la Entidad.

2. ALCANCE

La política del Sistema de Gestión de seguridad de la información aplica a toda la Entidad, a terceros del DANE y a la ciudadanía en general.

La política de seguridad es el fundamento del Sistema de Gestión de Seguridad de la Información (SGSI), apoya el cumplimiento del control de la norma ISO/IEC 27001:2013 Política de Seguridad (control anexo A).

5 Políticas de seguridad de la información

5.1 Directrices establecidas por la dirección para la seguridad de la información

5.1.1 Políticas para la seguridad de la información.

5.1.2 Revisión de las políticas para seguridad de la información.


3. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACION

El DANE considera que la seguridad es indispensable para proteger los activos de la información de las amenazas, por ende, propenderá por la continuidad de la operación, minimizando el riesgo de daño o pérdida de la información.

Para apoyar el cumplimiento de los objetivos estratégicos, la Entidad contempla la seguridad de la información como uno de los factores críticos de éxito; debido a esto, esta debe disponer de la debida protección, con el fin de mantener la confianza de los usuarios internos y externos, en los procesos, en los trámites y en los servicios. Por consiguiente, la Entidad definirá la política y lineamientos para la gestión de la seguridad de la información.

Política:

La Entidad implementará controles, procedimientos, protocolos y métodos para gestionar de manera eficiente los activos de información y fomentará una cultura de seguridad de la información, mitigando los riesgos que afecten su integridad, disponibilidad y confidencialidad, dentro de un marco orientado a la mejora continua, cumpliendo con la ley de reserva estadística y promoviendo la confianza y cooperación de los usuarios.

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 2 PÁGINA: 4
ELABORÓ: Profesional Oficina de Sistemas	REVISÓ: Coordinador Grupo de Plataforma Tecnológica y Sistemas de Información	APROBÓ: Jefe Oficina Sistemas

4. LINEAMIENTOS


A continuación, se establecen los lineamientos y objetivos que soportan el SGSI del DANE.

- Tener como responsabilidad; garantizar la confidencialidad, integridad y disponibilidad de los activos de información.
- Las responsabilidades frente a la seguridad de la información, serán definidas, socializadas, difundidas y deberán ser aceptadas por cada uno de los funcionarios, contratistas y terceros.
- El DANE protegerá la información generada, procesada o resguardada por los procesos de la entidad y los activos de información que hacen parte de los mismos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de ésta. Para ello, es fundamental la aplicación de controles de acuerdo con la clasificación de la información, su propiedad o custodia.
- El DANE protegerá las instalaciones físicas y la infraestructura tecnológica que soporta los procesos misionales, administrativos y de soporte.
- El DANE controlará la operación de sus procesos, garantizando la seguridad de los recursos.
- El DANE controlará el acceso a las instalaciones físicas, información, sistemas y recursos de red.
- El DANE adoptará la seguridad como parte integral del ciclo de vida de los sistemas de información.
- El DANE a través de una adecuada gestión de los eventos de seguridad, propenderá por una mejora continua de su modelo de seguridad.
- El DANE gestionará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas. El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional en esta materia.
- El DANE a través de la Oficina de Sistemas, definirá los encargados de la gestión de seguridad de la información en la Entidad.
- El DANE restringirá la instalación de cualquier tipo de software o hardware en los equipos de cómputo. Esto es responsabilidad del equipo de TI, y por tanto son los únicos autorizados para el uso de claves para la administración de servidores y estaciones de trabajo y por ningún motivo serán compartidas con los usuarios.

5. DESCRIPCIÓN DE TAREAS

Las siguientes tareas se derivan de la implementación de la Política de Seguridad de la información del DANE y constituyen parte fundamental del SGSI:

1. Proteger los activos de información del DANE, de acuerdo con lo establecido en los procesos institucionales y acorde con la regulación existente.

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 2 PÁGINA: 5
ELABORÓ: Profesional Oficina de Sistemas	REVISÓ: Coordinador Grupo de Plataforma Tecnológica y Sistemas de Información	APROBÓ: Jefe Oficina Sistemas

2. Adoptar una metodología para la administración de riesgos del Sistema de información de Gestión institucional del DANE.
3. Definir y ejecutar campañas de socialización de la seguridad de la información.
4. Hacer seguimiento al cumplimiento de la política de seguridad de la información.
5. Mantener actualizada la documentación que fundamenta el Sistema de Gestión de Seguridad de la Información.
6. Establecer y comunicar, apoyado con sensibilizaciones a los usuarios, sobre su responsabilidad en el uso de los activos de información.
7. Proteger la imagen, los intereses y el buen nombre del DANE.
8. Propender por el debido cumplimiento de las normas de propiedad intelectual.
9. Adoptar soluciones tecnológicas y controles, encaminados al tratamiento de los riesgos y la seguridad de la información.

6. DEFINICIONES

Activos: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la entidad.

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la entidad.

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría.

Control: Herramienta de la gestión del riesgo, incluyendo políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal.


Confidencialidad: Propiedad que determina que la información está disponible y es revelada a individuos, entidades, organizaciones o procesos autorizados.

Disponibilidad: Propiedad que determina que la información sea accesible y utilizable por solicitud de una entidad, organización, individuo o procesos autorizado.

Integridad: Propiedad de salvaguarda la exactitud y estado completo de los activos

Política: Dirección general y forma expresada por la gerencia

Riesgo: Combinación de la probabilidad de un evento y sus consecuencias.

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 2 PÁGINA: 6
ELABORÓ: Profesional Oficina de Sistemas	REVISÓ: Coordinador Grupo de Plataforma Tecnológica y Sistemas de Información	APROBÓ: Jefe Oficina Sistemas

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 entidad 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.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

7. BIBLIOGRAFÍA

<http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html>

APROBACION: La actualización de la política general de seguridad de la información y los lineamientos, fueron Aprobados mediante Comité de Desarrollo Administrativo de 9 de Noviembre del 2017.