GOBIERNO DE COLOMBIA

ARCHIVO GENERAL DE LA NACIÓN COLOMBIA

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2019

GOBIERNO DIGITAL

Grupo de Sistemas
Subdirección de tecnologías de la información archivística y documento electrónico
Archivo General de la Nación Jorge Palacios Preciado

1. PRESENTACIÓN

El presente documento se realiza con el fin de gestionar los riesgos de seguridad y privacidad de la información basado en los criterios de confidencialidad, integridad disponibilidad el cual se encuentra articulado con la metodología de riesgos del DAFP conforme a la guía para la gestión del riesgo y diseño de controles, en entidades públicas versión 4 y las disposiciones de la ley 1581 de 2012, decreto 1377 de 2013 y el decreto 886 de 2014.

2. ALCANCE

La vigencia del presente plan es 2019 y aplica para los 13 procesos que hacen parte del mapa de procesos definido en el sistema de gestión de calidad del Archivo General de la Nación, siendo un (1) proceso estratégico, siete (7) procesos de apoyo, cuatro (4) procesos misionales, un (1) proceso de evaluación independiente.

3. OBJETIVOS

3.1. Objetivo general

Elaborar el plan de tratamiento de riesgos de seguridad y privacidad de la información alineado con la guía metodológica para la gestión del riesgo del DAFP adoptada por el Archivo General de la Nación y las disposiciones del CONPES 3854 DEL 2016, la ley 1581 de 2012, decreto 1377 de 2013 y el decreto 886 de 2014.

3.2. Objetivos específicos

- Realizar el plan de trabajo específico vigencia 2019, conforme a los resultados obtenidos de las auditorías realizadas en la vigencia 2018 y de los mapas de riesgos institucionales.
- Alinear los procesos de información del Archivo General de la Nación con los de datos personales dando cumplimiento a la ley 1581 de 2012 y demás normas concordantes.
- Aportar avances al modelo integrado de planeación y gestión en sus políticas gobierno digital, seguridad digital, transparencia, acceso a la información pública y lucha contra la corrupción entre otras.
- Gestionar los riesgos de seguridad y privacidad de la información buscando la integración de la metodología del DAFP.

4. RECURSOS

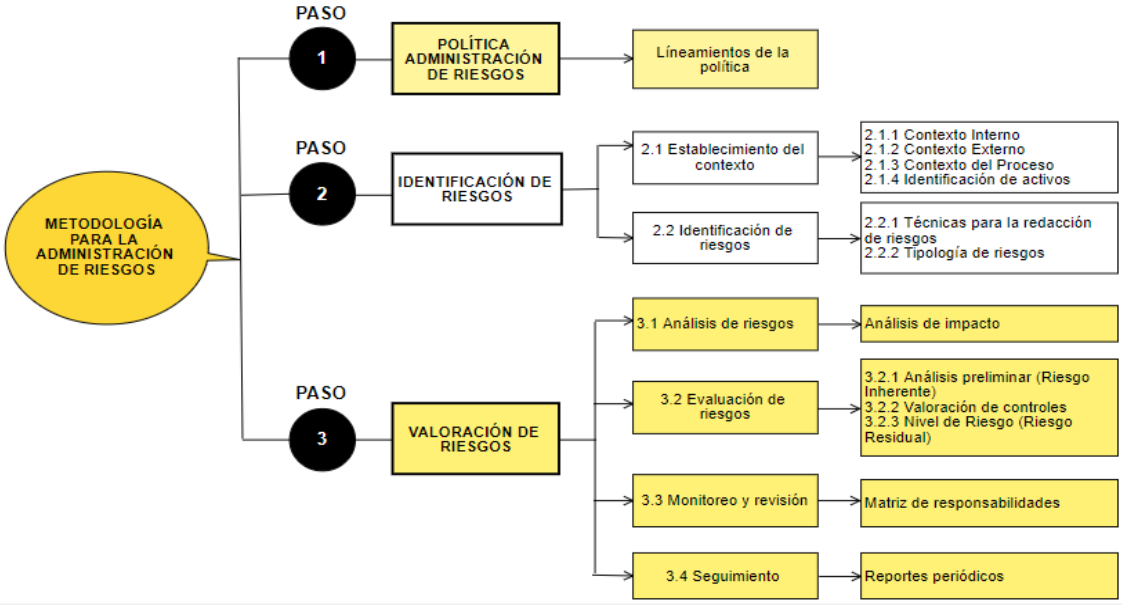
- **Humano:** La dirección general, comité de control interno, equipo MECI, oficina de control interno, los líderes de proceso, un profesional especializado en seguridad informática.
- **Físico:** Infraestructura tecnológica, controles de acceso físico.

5. RESPONSABLES

- La dirección general
- Comité de control interno
- Equipo MECI
- Oficina de control interno
- Líderes de proceso
- Enlaces SIPG
- Equipo Sistema Integrado de planeación y gestión (SIPG)
- Profesional Especializado en seguridad informática

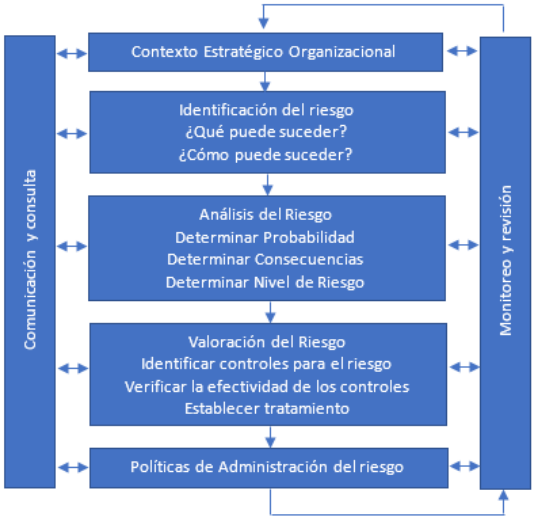
6. METODOLOGÍA DE IMPLEMENTACIÓN

De acuerdo con la guía metodológica para la administración del riesgo y el diseño de controles en entidades públicas, se deben aplicar tres (3) pasos básicos para el desarrollo y la definición e implementación de estrategias de comunicación transversales a toda la entidad.



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas – riesgos de gestión, corrupción y seguridad digital Función Pública octubre 2018.

Es por lo anterior que la implementación del plan de tratamiento de riesgos de seguridad y privacidad de la información consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento



Fuente: Cartilla de administración de riesgos del DAFP ISO 31000:2005

6.1. Actividades y entregables de las fases de la metodología de implementación Fuente: SIG-G-01_guia_metodologica_gestion_riesgo

Fase I – Caracterización de los sistemas de gestión y de los procesos de la Entidad

Dentro de esta fase se realizan las siguientes actividades:

- Listado Maestro de Registros en el SIG Actualizado
- Identificación de procedimientos actualizados
- Inventario de activos de información

Fase II – Identificación de riesgos

Dentro de esta fase se realizan las siguientes actividades:

- Identificación de causas
- Identificación de riesgo.
- Establecer las consecuencias.
- Tipificar y valorar el riesgo
- Determinar el impacto
- Determinar la probabilidad
- Determinar el nivel de riesgo inherente y residual

Fase III – Valoración de controles:

- Identificación del tipo de control
- Calificar el tipo de control.
- Valoración de la eficiencia del control.

Fase IV – Tratamiento de los riesgos

- Calculo estimado del riesgo residual
- Selección de la opción de tratamiento
- Determinar las acciones de mitigación del riesgo

Fase V – Seguimiento y Evaluación.

- Realizar seguimiento a la autoevaluación de la gestión por áreas
- Realizar monitoreo de los riesgos a través de la evaluación independiente que realiza la Entidad y el líder del sistema de gestión de seguridad y privacidad de la información.
- Determinar las alertas que se generen a partir de los resultados de las mediciones anteriores
- Aplicar acciones de mejora continua resultado de las auditorias, de los mapas de riesgos y planes de acción.
- Socialización de resultados

7. DESARROLLO DEL PLAN

El seguimiento del presente plan se realiza conforme a los informes y tiempos establecidos en el plan de acción por dependencia (PAD).

CONTROL DE CAMBIOS

FECHA	VERSIÓN	PROYECTÓ	REVISÓ	APROBÓ	DESCRIPCIÓN
23-05-2018	1.0	Heilin Guarnizo Rodriguez.	Manuel Gomez Patiño.	Erika Rangel Palencia	Versión inicial
20-02-2019	2.0	Heilin Guarnizo Rodriguez	Laura Ruiz Gomez	Laura Ruiz Gomez	Actualización