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

Versión: 6

Fecha: Bogotá D.C., enero de 2024

TABLA DE CONTENIDO

INDICE DE TABLAS

INTRODUCCIÓN

Este plan define el análisis, evaluación y tratamiento de los riesgos de seguridad y privacidad de la información, tomando como base la Guía para la Administración del Riesgo del Departamento Administrativo de la Función Pública (DAFP) y la "Guía de Gestión de Riesgos" del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), realizando la identificación, análisis, valoración, tratamiento de los riesgos e identificación de las vulnerabilidades y amenazas asociadas a los riesgos conforme a la norma ISO/IEC 27005:2011 Tecnologías de la información - Técnicas de Seguridad - Administración de riesgos de Seguridad de la Información.

1. OBJETIVOS

1.1 Objetivo general

Realizar el 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.

1.2 Objetivos específicos

- Realizar el plan de trabajo específico vigencia 2024.
- 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.

2. ALCANCE

La vigencia del presente plan es el año 2024 y aplica al proceso de Gestión de las Tecnologías de Información y el Gobierno Digital.

3. DEFINICIONES

Para la adecuada gestión del presente plan, se debe manejar con propiedad los siguientes términos:

- **Activo de información**: Todo aquel elemento de información, recibido, gestionado o producido, que posee valor para la entidad y, por lo tanto, debe protegerse para el logro de la misión. Serán activos de información críticos aquellos que son imprescindibles o su valor es clave para la operación de la entidad. Cuando se trate de activos informáticos, se entenderán como aquellos dispositivos tecnológicos que permiten la emisión, transmisión, procesamiento y recepción de información.

- **Cibernético.** Ciencia que estudia las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas.

- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. (ISO/IEC 27001).

- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. (ISO/IEC 27001).

- **Infraestructura:** Conjunto de activos o recursos técnicos, servicios o instalaciones que se consideran necesarios para el desarrollo normal de procesos o actividades.

- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos. (ISO/IEC 27001).

- **Privacidad:** 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, que genera la obligación de proteger dicha información en observancia del marco legal vigente.

- **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 residual:** Es un nivel de riesgo que permanece, luego de determinar y aplicar controles para su administración.

- **Valoración del riesgo:** Establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización.

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

- **Software:** Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

- **T.I. Tecnología de la Información:** Generalmente se conoce así al área o dependencia que administra la tecnología en una entidad. Para el presente documento, OTI o TI hacen referencia a la Oficina de Tecnología de la Información del AGN.

4. ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

El análisis del riesgo de seguridad de la información busca establecer la probabilidad de ocurrencia de este y sus consecuencias, evaluándolos con el fin de obtener información para calificar su nivel.

Para tener en cuenta en el análisis de los riesgos identificados, se han establecido dos aspectos: probabilidad e impacto.

Por probabilidad se entiende la posibilidad de ocurrencia del riesgo y puede ser medida con criterios de frecuencia si se ha materializado, o de factibilidad teniendo en cuenta la presencia de factores internos y externos, que pueden propiciarlo, aunque éste no se haya materializado.

El impacto se mide por las consecuencias que puede ocasionar a la Entidad la materialización del riesgo. Los pasos para el análisis de los riesgos son:

4.1 Calificación del riesgo.

Para la definición del impacto se debe tener en cuenta la clasificación del riesgo (estratégico, operativo, financieros, cumplimiento, tecnología, imagen) de acuerdo con la clase del riesgo y la magnitud del impacto se debe determinar el nivel en el que se encuentra.

4.2 Evaluación del riesgo.

Permite comparar los resultados de la calificación, con los criterios definidos para establecer el grado de exposición al riesgo; de esta forma, se define la zona de ubicación del riesgo inherente (antes de la definición de controles). La evaluación del riesgo se calcula con base en variables cuantitativas y cualitativas.

Con la evaluación del riesgo, previa a la formulación de controles, se obtiene la ubicación del riesgo en la matriz de evaluación; esto se denomina evaluación del riesgo inherente.

4.2.1 Desarrollo práctico – Análisis

Formato de Análisis de riesgos, el cual hace parte del proceso Administración del Sistema Integrado de Gestión de Calidad, donde se debe relacionar la siguiente información:

- Riesgo: Relacionar el riesgo redactado en el mapa de riesgos.
- Calificación de probabilidad: de acuerdo con la información cuantitativa y cualitativa generada por el análisis de los Riesgos.
- Calificación de impacto: de acuerdo con la información cuantitativa y cualitativa generada por el análisis de los Riesgos.
- Clasificación del riesgo: Ver componentes de la identificación del riesgo, en el apartado de clasificación de los riesgos.
- Evaluación: surge del cruce de los resultados cuantitativos de la calificación para probabilidad e impacto.

4.3 Valoración de los riesgos.

Es el producto de confrontar la evaluación del riesgo y los controles (preventivos o correctivos) de los procesos. La valoración del riesgo se realiza en tres momentos: primero, identificando los controles (preventivos o correctivos) que pueden disminuir la probabilidad de ocurrencia o el impacto del riesgo; luego, se deben evaluar los controles, y finalmente, con base en los resultados de la evaluación de los controles, determinar la evaluación del riesgo residual y definir la opción de manejo del riesgo. Lo anterior de acuerdo con los formatos Identificación y evaluación de controles y Valoración del riesgo.

4.4 Seguimiento de riesgos.

La administración de los riesgos de seguridad y privacidad de la información por proceso e institucionales será acompañada por el Oficial de Seguridad de la Información.

La calificación y evaluación de los riesgos del sistema de seguridad de la información se realiza por parte del dueño del proceso.

La efectividad de los controles y cumplimiento de las acciones de mitigación de riesgos se realiza por parte de la Oficina de Control Interno.

Los resultados de la evaluación y las observaciones de Control Interno serán presentados al Oficial de Seguridad y a la Dirección General, en el momento que lo considere pertinente, para que se tomen las decisiones necesarias que garanticen la sostenibilidad de la Administración de estos riesgos en el AGN.

5. MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

El Archivo General de la Nación en su mapa de riesgos tiene definidos los riesgos tecnológicos y de seguridad digital, los cuales serán el objeto de tratamiento para mantener la integridad y confidencialidad de la información.

Tabla 1. Mapa de Riesgos

Identificación del riesgo						Análisis del riesgo inherente							
Referencia	Descripción del Riesgo	Causa Inmediata	Causa Raíz	Clasificación del Riesgo	Tipo de Riesgo	Probabilidad	%	Criterios de impacto	Impacto	%	% Zona de riesgo	% Zona de riesgo	Zona de Riesgo
1	Posibilidad de vulnerabilidades de los sistemas de información por ataque a los servidores de la entidad debido al incumplimiento de parte de los usuarios de las políticas establecidas sobre seguridad informática.		Incumplimiento de parte de los usuarios de las políticas establecidas sobre seguridad informática		OPERATIVO	**POSIBLE**	60%	Un ataque cibernético a los servidores de la entidad causaría un impacto mayor a la operación de la entidad en la medida que podría generar perdidas de información y afectar las vulnerabilidades.	**MAYOR**	80%	70%	70%	**ALTO**
2	Posibilidad de pérdida de la Disponibilidad, confidencialidad e integridad de la Información por tener software obsoleto debido a que no está actualizado y que no tenga soporte técnico de parte del proveedor de servicios informáticos.		No tener software actualizado que garantice un soporte adecuado de parte del proveedor de servicios informáticos.		SEGURIDAD DIGITAL	**IMPROBABLE**	40%	Perder disponibilidad, confidencialidad e integridad de la información tiene consecuencias de perdida reputacional de la entidad y genera desconfianza en cuanto a la seguridad de los datos de los usuarios de los sistemas de la entidad.	**MODERADO**	60%	50%	50%	**MODERADO**
3	Pérdida de los activos de información por no tener controles debido a un deficiente uso de los sistemas de información, bases de datos y aplicativos de la entidad		No disponer de políticas, procedimientos y controles de fuga de información en los sistemas de información, bases de datos y aplicativos.		SEGURIDAD DIGITAL	**PROBABLE**	80%	Fuga de información de la entidad puede tener impacto en Daño de la marca o del buen nombre de la Entidad o interrupción de la continuidad del negocio.	**MAYOR**	80%	80%	80%	**ALTO**

Fuente: Matriz de Riesgos Institucionales AGN 2023

6. DESARROLLO DEL PLAN

Para la vigencia 2024 se establecen las actividades de acuerdo con el enfoque en Riesgos, realizando el respectivo cruce entre lo establecido en el Modelo de Seguridad y Privacidad de la Información, la Política de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, la matriz de autodiagnóstico del Modelo Integrado de Planeación y Gestión – MIPG del Departamento

Administrativo de la Función Pública – DAFP y las buenas prácticas aplicables. De igual manera se tiene en cuenta los siguientes recursos disponibles:

- Humanos:
  - Oficial de Seguridad de la Información.
  - Grupo de Tecnologías de la Información: Infraestructura tecnológica y redes.
  - Líderes y gestores de los procesos
  - Grupo Interno de Trabajo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
  - CSIRT de Gobierno

- Técnicos:
  - Guía para la administración del riesgo y el diseño de controles en entidades públicas – Riesgos de gestión, corrupción y seguridad digital del DAFP
  - Matriz de riesgos Sistema de Gestión de Seguridad de la Información - SGSI

- Logísticos: Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.

Con base en lo anterior, se cuenta con recursos para plasmar acciones de mejora que permitan enfocar a la entidad hacia la meta establecida, considerando actividades concretas, medibles y alcanzables, que admitan la mejora continua.

7. HOJA DE RUTA

Se establece la siguiente hoja de ruta, detallando en el plan de trabajo las acciones y el plazo de ejecución.

Tabla 2. Hoja de Ruta

Proyectos	2024											
	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
Actualización de la metodología de riesgos: cuando se requiera la actualización de la política, metodología y lineamientos de la gestión de riesgos												
Sensibilización: Socialización de lineamientos de la Gestión de Riesgos de Seguridad y privacidad de la Información.												
Identificación de Riesgos de Seguridad de la Información y Seguridad Digital.												
Actualización del mapa de riesgos, controles y sus planes de tratamiento												
Seguimiento Fase de Tratamiento												

Fuente: Elaboración propia

8. CONTROL DE CAMBIOS

VERSIÓN	FECHA APROBACIÓN	RESPONSABLE	DESCRIPCIÓN
1	23-05-2018	Manuel Gómez Patiño.	Versión inicial
2	18-02-2019	Laura Ruiz Gómez.	Actualización
3	30/03/2021	Omar Villarreal Osorio	Actualización
4	23/12/2021	Omar Villarreal Osorio	Actualización
5	20/12/2022	Omar Villarreal Osorio	Actualización
6		Martha Patricia Vargas Rodríguez	Actualización