PRESIDENCIA DE LA REPÚBLICA

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

Bogotá D.C. Julio de 2018

TABLA DE CONTENIDO

1. OBJETIVO ---- 3
2. ALCANCE ---- 3
3. TERMINOS Y DEFINICIONES ---- 3
4. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN ---- 4
4.1 Definición de riesgos y oportunidades de Seguridad de la Información ---- 4
4.1.1 Creación de Nuevos riesgos de seguridad de la información ---- 4
4.1.2 Creación y documentación de Matriz de riesgos de seguridad de la información versus controles ---- 5
5. MARCO LEGAL ---- 6
6. REQUISITOS TÉCNICOS ---- 7
7. DOCUMENTOS ASOCIADOS ---- 7
8. RESPONSABLE DEL DOCUMENTO ---- 7

1. OBJETIVO

Definir el plan de tratamiento de riesgos que hacen parte del Sistema de Gestión de Seguridad de la Información, para así aplicar los controles con los cuales se buscan mitigar su materialización en el Departamento Administrativo de la Presidencia de la República.

De esta forma se busca que mediante el tratamiento de los riesgos y la mejora continua de la Seguridad y Privacidad de la Información, las partes interesadas tengan mayor confianza en el tratamiento de la información que se almacena y maneja en la Entidad.

2. ALCANCE

Se define el alcance del presente plan de tratamiento de riesgos, para los procesos del Departamento Administrativo de la Presidencia de la República, en concordancia con el alcance del Sistema de Gestión de Seguridad de la Información[1].

3. TERMINOS Y DEFINICIONES

Riesgo: Posibilidad de ocurrencia del evento que tiene un efecto positivo o negativo sobre el producto o servicio generado de un proceso o el cumplimiento de los objetivos institucionales.

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información*; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información.* Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera

También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.

Riesgo Positivo: Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.

Seguridad de la Información: Este principio busca crear condiciones de uso confiable V en el entorno digital, mediante un enfoque basado en la gestión de riesgos,

[1] Ver Manual del Sistema Integrado de Gestión de la Presidencia de la República SIGEPRE M-DE-02, sección: Alcance del Sistema de Gestión de Seguridad de la Información - SGSI.

preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.[2]

SIGEPRE: Es el sistema integrado de Gestión de la Presidencia de la República, que permite armonizar los procesos en búsqueda de una gestión eficiente, eficaz y trasparente, con el fin de aumentar la satisfacción de los clientes.

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

En el marco del Modelo de Seguridad y Privacidad de la Información y el Sistema de Gestión de Seguridad de la Información –SGSI del Departamento Administrativo de la Presidencia de la República, se busca prevenir los efectos no deseados que se puedan presentar en cuanto a seguridad de la información, por lo cual es importante controlar y establecer los riesgos de seguridad de la información.

De esta forma, se garantiza el tratamiento de los riesgos de seguridad de la información y la gestión de riesgo positivo u oportunidad, acorde con lo establecido en el **Lineamiento de Administración de Riesgos L-DE-01** y la **Guía para La Formulación, Seguimiento y Evaluación de Planes de Mejoramiento G-EM-01**.

4.1 Definición de riesgos y oportunidades de Seguridad de la Información

A continuación se da a conocer las actividades definidas con el fin de definir y realizar el proceso concerniente a los riesgos de seguridad de la información para la vigencia 2018, lo que permite una mejora continua del Sistema de Gestión de Seguridad de la Información de la Entidad:

4.1.1 Creación de Nuevos riesgos de seguridad de la información

Para la creación de nuevos riesgos de seguridad de la información, se desarrollan las siguientes actividades, las cuales se encuentran definidas en SIGEPRE, en la **OM-0422 TI - Creación de nuevos riesgos de seguridad de la información – SGSI.**

Nombre	Fecha Inicial planificada	Fecha final planificada	Responsable
1. Definición de etapa de identificación de riesgos de seguridad de la información.	25/06/2018 08:00	03/08/2018 23:59	Betty Yaneth Daza Sandoval

[2] Decreto 1008 de 14 de Junio de 2018, por el cual se establecen los lineamientos generales de la Política de Gobierno Digital.

2. Realizar etapa de análisis de riesgos de seguridad de la información.	25/06/2018 08:00	03/08/2018 23:59	Betty Yaneth Daza Sandoval
3. Efectuar etapa de valoración de riesgos de seguridad de la información.	25/06/2018 08:00	03/08/2018 23:59	Betty Yaneth Daza Sandoval
4. Generar la etapa de manejo de los riesgos de seguridad de la información.	25/06/2018 08:00	03/08/2018 23:59	Betty Yaneth Daza Sandoval
5. Definir la fecha de monitoreo de la aplicación de los controles definidos en la etapa de valoración.	25/06/2018 08:00	03/08/2018 23:59	Betty Yaneth Daza Sandoval
6. Realizar comunicación con las dependencias del DAPRE con el fin de conocer los posibles riesgos de seguridad de la información que se puedan originar en cada una de las dependencias.	25/06/2018 08:00	03/08/2018 23:59	Betty Yaneth Daza Sandoval

4.1.2 Creación y documentación de Matriz de riesgos de seguridad de la información versus controles

Se define oportunidad de mejora que permite la documentación de matriz de riesgos de seguridad de la información versus controles, basados en la norma ISO 27001:2013, a continuación se dan a conocer las actividades desarrolladas, las cuales se encuentran descritas en la **OM-0421 TI - Creación y documentación de Matriz de riesgos de seguridad de la información versus controles - SGSI**:

Nombre	Fecha Inicial planificada	Fecha final planificada	Responsable
1. Documentación de matriz de riesgos versus objetivos de control de Políticas de la seguridad de la información.	25/06/2018 08:54	03/08/2018 23:59	Ana Rocio Castro Paez
2. Documentación de matriz de riesgos versus objetivos de control de Organización de la seguridad de la información.	25/06/2018 11:58	03/08/2018 23:59	Ana Rocio Castro Paez
3. Documentación de matriz de riesgos versus objetivos de control de Seguridad de los recursos humanos.	25/06/2018 11:59	03/08/2018 23:59	Ana Rocio Castro Paez
4. Documentación de matriz de riesgos versus objetivos de control de Gestión de activos.	25/06/2018 11:59	03/08/2018 23:59	Ana Rocio Castro Paez

5. Documentación de matriz de riesgos versus objetivos de control de control de acceso.	25/06/2018 11:59	03/08/2018 23:59	Ana Rocio Castro Paez
6. Documentación de matriz de riesgos versus objetivos de control de Criptografía.	25/06/2018 12:00	03/08/2018 12:59	Ana Rocio Castro Paez
7. Documentación de matriz de riesgos versus objetivos de control de Seguridad física y del entorno.	25/06/2018 11:55	03/08/2018 23:59	Ana Rocio Castro Paez
8. Documentación de matriz de riesgos versus objetivos de control de seguridad de las operaciones.	25/06/2018 11:55	03/08/2018 23:59	Ana Rocio Castro Paez
9. Documentación de matriz de riesgos versus objetivos de control de Seguridad de las comunicaciones.	25/06/2018 11:56	03/08/2018 23:59	Ana Rocio Castro Paez
10. Documentación de matriz de riesgos versus objetivos de control de adquisición, desarrollo y mantenimiento de sistemas.	25/06/2018 11:56	03/08/2018 23:59	Ana Rocio Castro Paez
11. Documentación de matriz de riesgos versus objetivos de control de relaciones con los proveedores.	25/06/2018 11:56	03/08/2018 23:59	Ana Rocio Castro Paez
12. Documentación de matriz de riesgos versus objetivos de control de gestión de incidentes de seguridad de la información.	25/06/2018 11:57	03/08/2018 23:59	Ana Rocio Castro Paez
13. Documentación de matriz de riesgos versus objetivos de control de aspectos de seguridad de la información de la gestión de continuidad del negocio.	25/06/2018 11:57	03/08/2018 23:59	Ana Rocio Castro Paez
14. Documentación de matriz de riesgos versus objetivos de control de cumplimiento.	25/06/2018 11:58	03/08/2018 23:59	Ana Rocio Castro Paez

5. MARCO LEGAL

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.

- Decreto 612 de 4 de Abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.
- Decreto 1008 de 14 de Junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.

6. REQUISITOS TÉCNICOS

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.

7. DOCUMENTOS ASOCIADOS

- L-DE-01 Lineamientos para la Administración del Riesgo.
- G-EM-01 Guía Para La Formulación, Seguimiento y Evaluación De Planes De Mejoramiento.
- M-TI-01 Manual de Políticas de Seguridad de la Información.

8. RESPONSABLE DEL DOCUMENTO

Jefe Área de Tecnologías y Sistemas de Información.