Agencia Nacional de Defensa Jurídica del Estado

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

UNIDAD ADMINISTRATIVA ESPECIAL
AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO
ENERO DE 2022

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el Entorno TIC para el Desarrollo Digital, ciudadanos y hogares empoderados del Entorno Digital, Transformación Digital Sectorial y Territorial e Inclusión Social Digital.
Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001:2013, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el DAFP. [1]

2. OBJETIVO

Hacer seguimiento a los tratamientos de riesgos de Seguridad y Privacidad de la información e identificar los riesgos de Continuidad de la Operación de TI de acuerdo con los contextos establecidos en la Entidad.

3. ALCANCE

La gestión de riesgos podrá ser aplicada sobre cualquier proceso de la Agencia, a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información, que permitan y faciliten el desarrollo de las etapas de identificación del contexto, del riesgo, análisis, evaluación y opciones de tratamiento, además las pautas para su seguimiento, monitoreo y evaluación.

[1] https://www.mintic.gov.co/portal/604/articles-100251_plan_tratamiento_seguridad_2020.pdf

4. DEFINICIONES Y ABREVIATURAS

Riesgo: es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

Amenaza: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

Vulnerabilidad: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

Probabilidad: es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.

Impacto: son las consecuencias que genera un riesgo una vez se materialice.

Control o Medida: acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.[2]

5. RESPONSABILIDADES

El líder de seguridad de la información o en su ausencia el líder del proceso de Gestión de Tecnologías de la Información será el encargado de dar continuidad a las actividades descritas en este plan.

6. ESTRATEGIA

La estrategia para el desarrollo del siguiente plan estará alienada con la guía de administración de riesgos DAFP y Anexo 4 teniendo como mapa de ruta el monitoreo de los tratamientos de los riesgos y la identificación de riesgos de continuidad de la operación de TI

7. DESARROLLO

En el marco del Modelo de Seguridad y Privacidad de la Información y el Sistema de Gestión de Seguridad de la Información – SGSI de la Agencia Nacional de Defensa Jurídica del Estado, busca prevenir los efectos no deseados que se

[2] https://www.mintic.gov.co/portal/604/articles-100251_plan_tratamiento_seguridad_2020.pdf

puedan presentar en cuanto a seguridad de la información, por lo cual es importante controlar y establecer los riesgos de seguridad de la información.

Este documento presenta el mapa de ruta con el cual se realizará el monitoreo a los tratamientos de los riesgos de seguridad e identificar los riesgos de Continuidad de la Operación de TI.

De esta forma, se asegura la mitigación de los riesgos de seguridad de la información, acorde con la guía MC-G-02 GUÍA ADMINISTRACIÓN DE RIESGOS y la formulación, seguimiento y evaluación de planes de mejoramiento.

NÚMERO	ACTIVIDAD	RESPONSABLE	PRODUCTO O RESULTADO ESPERADO
1	Migración riesgos de seguridad información a la herramienta DARUMA	SGSI	Riesgos migrados
2	Seguimiento plan de tratamiento de Riesgos de Seguridad procesos que tienen riesgos en zona ALTA	SGSI	Informe seguimiento riesgos del proceso MC-F-18 FORMATO PARA ELABORAR EL INFORME SEGUIMIENTO A LOS RIESGOS
3	Identificación riesgos de continuidad del negocio	SGSI	Matriz de riesgos de continuidad del negocio.
4	Informe riesgos y tratamiento riesgos de seguridad	SGSI	Informe 2022 riesgos y tratamientos seguridad digital realizado

8. DISTRIBUCIÓN PRESUPUESTAL

De acuerdo a la proyección PAA las siguientes adquisiciones hacen parte de los controles para fortalecer la infraestructura técnica y prevenir la mitigación de riesgos de seguridad de la información.

OBJETO	VALOR ESTIMADO EN LA VIGENCIA ACTUAL
Contratar "ANÁLISIS DE VULNERABILIDADES Y EXPLOTACIÓN". (ETHICAL HACKING) Contempla: Tiempos de Contratación y Ejecución del Servicio	$492.660.000
Contratar "CENTRO OPERACIONES DE SEGURIDAD (SOC)" diagnóstico de Sistemas e Infraestructura a administrar, monitorear, pruebas e implementación.	

Nota: El seguimiento de los proyectos que implican presupuesto será reportado en el seguimiento de del plan implementación y seguimiento del mapa de ruta

de los proyectos e iniciativas de tecnología de información -PETI 2021-2024 el cual esta soportado en PAA

9. RIESGOS

CLASIFICACIÓN DEL RIESGO	DESCRIPCIÓN DEL RIESGO	CAUSAS	CONSECUENCIAS	CONTROLES
Estratégico	Incumplimiento de metas propuestas para los planes de acción institucional de TI.	Insuficiente de asignación de tiempos y recursos Disminución de presupuesto	Incumplimientos legales y llamados de atención	Planificación y entrega del PAA a Financiera

10. INDICADORES

Porcentaje de verificación Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

11. CRONOGRAMA

Ver formato Cronograma ejecución plan DE-F-31 CRONOGRAMA EJECUCION PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

RESULTADO ESPERADO	RESULTADOS / ENTREGABLES INTERMEDIOS	RESPONSABLE	EJECUCIÓN	
			Fecha Inicio	Fecha Final
Migración 42 riesgos de seguridad información a la herramienta DARUMA	Parametrización Herramienta Cargue de datos	Fredy Zea- Gestor T1-14	15-ene-22	30-abr-22

Informe seguimiento riesgos de los procesos (MC-F-18 FORMATO PARA ELABORAR EL INFORME SEGUIMIENTO A LOS RIESGOS)	Matriz plan de tratamiento de Riesgos de Seguridad procesos que tienen riesgos en zona ALTA	Fredy Zea-Gestor T1-14	30-mar-22	15-dic-22
Matriz con riesgos de continuidad del negocio de Gestión de Tecnologías de la Información	Guía de Riesgos actualizada Riesgos de continuidad del negocio transversales a la entidad con enfoque de TI	Fredy Zea-Gestor T1-14	1-may-22	30-oct-22
Informe riesgos y tratamiento riesgos de seguridad	Matriz Riesgos de Seguridad Matriz Riesgos de Continuidad de TI	Fredy Zea-Gestor T1-14	1-dic-22	31-dic-22

Elaboró	Revisó	Aprobó
Fredy Zea Rodriguez Gestor T1-14	**Rosse Mary Villamil** Gestor T1-16	**Rosse Mary Villamil** Gestor T1-16