



**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
NOVIEMBRE DE 2020



TABLA DE CONTENIDO

INTRODUCCIÓN	3
OBJETIVO	3
ALCANCE.....	3
DEFINICIONES Y ABREVIATURAS	4
RESPONSABILIDADES.....	4
ESTRATEGIA.....	4
DESARROLLO	4
DISTRIBUCIÓN PRESUPUESTAL	6
RIESGOS.....	8
INDICADORES	8
CRONOGRAMA.....	8

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

OBJETIVO

Actualizar metodología de riesgos de seguridad de la información de acuerdo a la guía para la administración de riesgos y el anexo 4 emitida por el DAFP.

Gestionar riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, de acuerdo con los contextos establecidos en la Entidad.

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



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

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.

ESTRATEGIA

La estrategia para el desarrollo del siguiente plan estará alienada y enfocada con la guía de administración de riesgos DAFP y Anexo 4 teniendo como mapa de ruta los siguientes pasos: establecimiento de contexto, identificación de riesgos, análisis, evaluación y monitoreo.

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

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



Nacional de Defensa Jurídica del Estado, 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.

Este documento presenta el mapa de ruta con el cual se identificarán los nuevos riesgos de seguridad de la información se priorizarán y se definirá el tratamiento a realizar.

De esta forma, se asegura la reducción de 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	Actualización Metodología de Riesgos de Privacidad y Seguridad de la Información	SGSI	Metodología de riesgos actualizada
2	Actualización matriz de riesgos existentes a la nueva metodología	SGSI	Matriz actualizada de Riesgos de seguridad de la información.
3	Identificación de nuevos riesgos de seguridad de la información alineados a la nueva metodología	SGSI	Matriz de riesgos de seguridad de la información con los nuevos riesgos identificados.
4	Informe riesgos y tratamiento riesgos de seguridad	SGSI	Informe de Riesgos de Seguridad y Privacidad de la Información

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
Adquirir Certificados de sitio seguro para las plataformas de comunicaciones unificadas Skype for business con una vigencia de un (1) Años	\$ 3.000.000
Adquirir Certificados de sitio seguro para las plataformas de páginas Web de la agencia (defensajuridica.gov.co) con una vigencia de tres (3) Años	\$ 13.000.000
Renovar licencias y actualización del uso de DLP, antivirus, encriptador, así como la prestación del servicio de	\$ 70.000.000



asistencia y soporte técnico de las mismas por doce (24) meses	
Adquirir Switches para servidores de apoyo, para renovación tecnológica por obsolescencia.	\$ 30.000.000

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



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

INDICADORES

de actividades del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información desarrolladas / total de actividades del plan a implementar *100

CRONOGRAMA

Incorporar un cronograma ejecución del plan, el cual debe contener como mínimo;

- Resultado esperado: describir los resultados esperados como consecución del plan.
- Entregables: enumerar los entregables (productos) a entregar asociado al resultado esperado del plan
- Responsables: establecer el responsable del entregable.
- Fechas de ejecución: establece la fecha de inicio y fin de entrega del entregable, estado de cumplimiento y observaciones
- Tipo de recurso; seleccionar que clase de recursos son necesarios para el cumplimiento del entregable; Humanos, Tecnológicos, Infraestructura, Financieros.

  CRONOGRAMA EJECUCIÓN PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN									
AÑO FORMULACIÓN									
FECHA DE CORTE									
RESULTADO ESPERADO	RESULTADOS / ENTREGABLES INTERMEDIOS	RESPONSABLE	EJECUCIÓN		FECHA DE CUMPLIMIENTO	ESTADO	TIPO DE RECURSO	RECURSOS \$	OBSERVACIONES
			Fecha Inicio	Fecha Final					
Actualización Metodología de Riesgos de Privacidad y Seguridad de la Información	Metodología de Riesgos Actualizada	SGSI	12-ene-21	31-mar-21			Humanos	N/A	Funcionarios de TI
Actualización matriz de riesgos existentes a la nueva metodología	Reuniones con los líderes de proceso Matriz Actualizada Actualización Micrositio Seguridad - Intranet	SGSI	1-abr-21	31-jul-21			Humanos	N/A	Funcionarios de TI Líderes y Enlaces de Procesos
Identificación de nuevos riesgos de seguridad de la información alineados a la nueva metodología	Reuniones con los líderes de proceso misionales Matriz actualizada con los nuevos riesgos de los procesos misionales Actualización Micrositio Seguridad - Intranet	SGSI	1-ago-21	30-sep-21		#REF!	Humanos	N/A	Funcionarios de TI Líderes y Enlaces de Procesos misionales
Informe riesgos y tratamiento riesgos de seguridad	Informe ejecutivo	SGSI	1-nov-21	31-dic-21			Humanos	N/A	Funcionarios de TI

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

Elaboró	Revisó	Aprobó
Nombre Cargo	Nombre Cargo	Nombre Cargo