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

UNIDAD ADMINISTRATIVA ESPECIAL
AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO
ENERO DE 2024

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 y la Resolución 500 de 2021 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.

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.

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

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 Oficial 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. DESARROLLO

6.1 Estado actual de la entidad respecto al sistema de gestión de seguridad de la información

La Entidad ha venido fortaleciendo el modelo de seguridad y privacidad de la información desde el año 2016, desde un enfoque técnico y un enfoque estratégico, desde el nivel técnico se han adquirido herramientas para el monitoreo y correlación de eventos, contratación de servicios para análisis de vulnerabilidades, servicios de monitoreo de seguridad y revisión de marca. Desde el punto de vista estratégico se encaminó a fortalecer el Modelo de Seguridad y Privacidad de la Información (MSPI) y para ello se buscó actualizar las políticas de seguridad, la documentación procedimental, verificar los activos y riesgos de seguridad y documentar el plan de continuidad del negocio y plan de recuperación de desastres, resaltando para la vigencia 2023 la implementación del DRP.

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

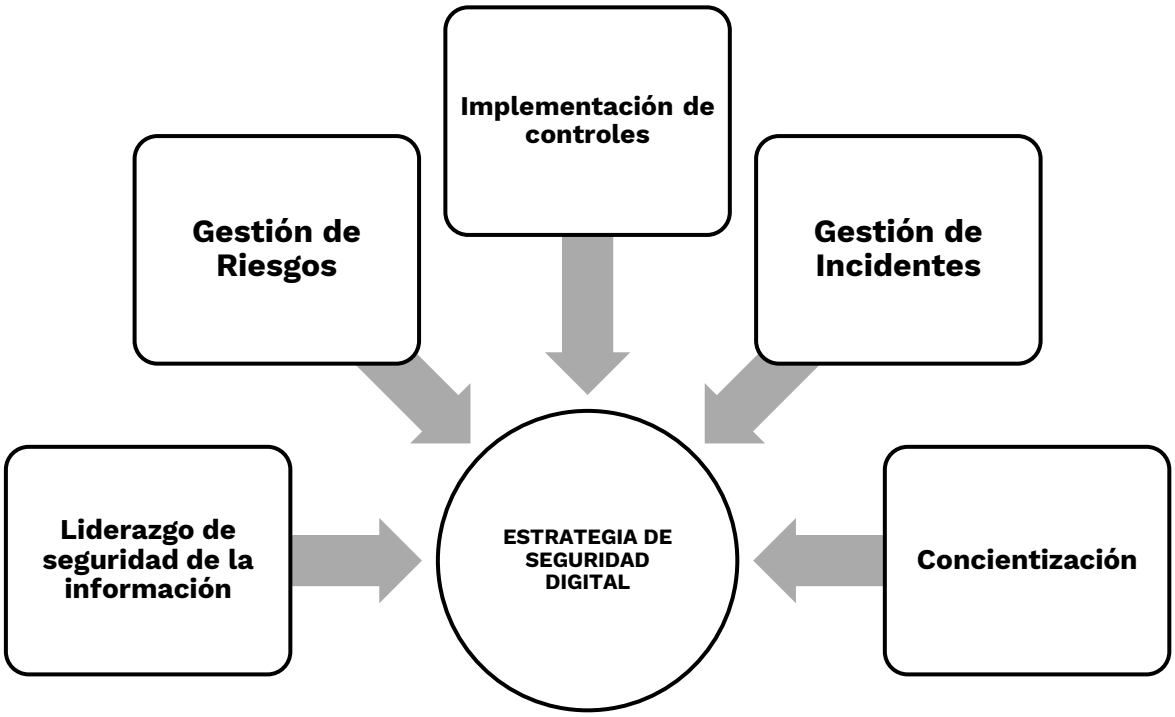
De este trabajo realizado a continuación, se copian los indicadores de implementación del MSPI tomando como base el instrumento de evaluación de MINTIC:

	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	**OPTIMIZADO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	84	100	**OPTIMIZADO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	98	100	**OPTIMIZADO**
A.8	GESTIÓN DE ACTIVOS	87	100	**OPTIMIZADO**
A.9	CONTROL DE ACCESO	98	100	**OPTIMIZADO**
A.10	CRIPTOGRAFÍA	90	100	**OPTIMIZADO**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	90	100	**OPTIMIZADO**
A.12	SEGURIDAD DE LAS OPERACIONES	90	100	**OPTIMIZADO**
A.13	SEGURIDAD DE LAS COMUNICACIONES	90	100	**OPTIMIZADO**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	78	100	**GESTIONADO**
A.15	RELACIONES CON LOS PROVEEDORES	100	100	**OPTIMIZADO**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	83	100	**OPTIMIZADO**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	90	100	**OPTIMIZADO**
A.18	CUMPLIMIENTO	86	100	**OPTIMIZADO**
PROMEDIO EVALUACIÓN DE CONTROLES		**90**	**100**	**OPTIMIZADO**

6.2 Estrategia de seguridad digital[3]

La Agencia establecerá una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira entorno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes que debe establecerse. Por tal motivo, LA ENTIDAD define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:

[3] PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN (PESI)-MINTIC



6.3 Descripción de las estrategias específicas (ejes)[4]

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Gestión de riesgos	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.

[4] PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN (PESI)-MINTIC

6.4 Portafolio de proyectos / actividades:

ESTRATEGIA / EJE	ACTIVIDADES	PRODUCTOS ESPERADOS
Gestión de riesgos	**ACTIVIDAD 1** Estandarizar riesgos de continuidad del negocio. **ACTIVIDAD 2** Seguimiento planes de tratamiento de riesgos de seguridad	**ACTIVIDAD 1** Matriz de riesgos de continuidad del negocio. **ACTIVIDAD 2** Informe seguimiento riesgos del proceso MC-F-18 FORMATO PARA ELABORAR EL INFORME SEGUIMIENTO A LOS RIESGOS
Implementación de controles	**ACTIVIDAD 1** Implementación DRP **ACTIVIDAD 2** Monitoreo seguridad **ACTIVIDAD 3** Análisis de vulnerabilidades **ACTIVIDAD 4** Análisis de Marca	**ACTIVIDAD 1** Infraestructura implementada **ACTIVIDAD 2** Servicio SOC **ACTIVIDAD 3** Informe resultados **ACTIVIDAD 4** Informe resultados
Gestión de incidentes	**ACTIVIDAD 1** Capacitar al personal en la gestión de incidentes de seguridad de la información.	**ACTIVIDAD 1** Sesiones de capacitación desarrolladas.

6.5 Distribución presupuestal

De acuerdo con 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
Profesional especializado responsable del Rol de Oficial de Seguridad de la Agencia para asegurar y mantener el Modelo de Seguridad y Privacidad de la Información.	$154.000.000
Servicio ciberseguridad para monitoreo de seguridad, monitoreo de red, análisis de vulnerabilidades y plan de recuperación de desastres.	$1.250.000.000

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 el cual esta soportado en PAA.

7. 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

8. INDICADORES

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

9. CRONOGRAMA

RESULTADO ESPERADO	PESO (%)	RESULTADOS / ENTREGABLES INTERMEDIOS	PESO (%)	RESPONSABLE	EJECUCIÓN	
					Fecha Inicio	Fecha Final
Gestión de riesgos	16%	Matriz riesgos continuidad del negocio.	100%	Oficial seguridad de la Información	15-jun-24	30-nov-24
Gestión de riesgos	16%	Informe seguimiento riesgos del proceso MC-F-18 FORMATO PARA ELABORAR EL INFORME SEGUIMIENTO A LOS RIESGOS	100%	Oficial seguridad de la Información	15-feb-24	30-nov-24
Implementación DRP	20%	Infraestructura implementada	100%	Oficial seguridad de la Información	15-feb-24	30-jun-24
Monitoreo seguridad	16%	Servicio SOC	100%	Oficial seguridad de la Información	15-feb-24	30-jun-24
Análisis de vulnerabilidades	16%	Informe resultados	100%	Oficial seguridad de la Información	30-jun-24	30-nov-24
Análisis de Marca	16%	Informe resultados	100%	Oficial seguridad de la Información	30-jun-24	30-nov-24

Elaboró	Revisó	Aprobó
Fredy Zea Rodriguez Gestor T1-14	**Oswaldo Useche Acevedo** Jefe Oficina	Comité Institucional de Gestión y Desempeño - CIGD