Defensa Jurídica del Estado

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

UNIDAD ADMINISTRATIVA ESPECIAL
AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO
ENERO DE 2025

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.

3. ALCANCE

La gestión de riesgos puede 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

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). (ISO/IEC 27000)

[1] chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://gobiernodigital.mintic.gov.co/692/articles-150517_Modelo_de_Seguridad_Privacidad.pdf

Confidencialidad: es la propiedad que garantiza que la información solo sea accesible para aquellas personas, entidades o procesos que están autorizados a acceder a ella. La confidencialidad protege la información sensible de accesos no autorizados, evitando su divulgación indebida.

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].

Disponibilidad: es la propiedad que garantiza que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo necesitan. Esto implica que los sistemas deben estar operativos y accesibles de manera confiable, minimizando tiempos de inactividad o fallos.

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

Integridad: es la propiedad que asegura que la información y sus métodos de procesamiento son completos y precisos, es decir, que no han sido alterados de manera no autorizada, ya sea accidental o intencionalmente. La integridad protege contra la modificación o destrucción de la información sin autorización.

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

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

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

5. RESPONSABILIDADES

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

[2] chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-162621_Modelo_de_Seguridad_y_Privacidad__MSPI.pdf

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 busca 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 2024 la implementación fase I de la estrategia para DRP basado en nube pública.

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

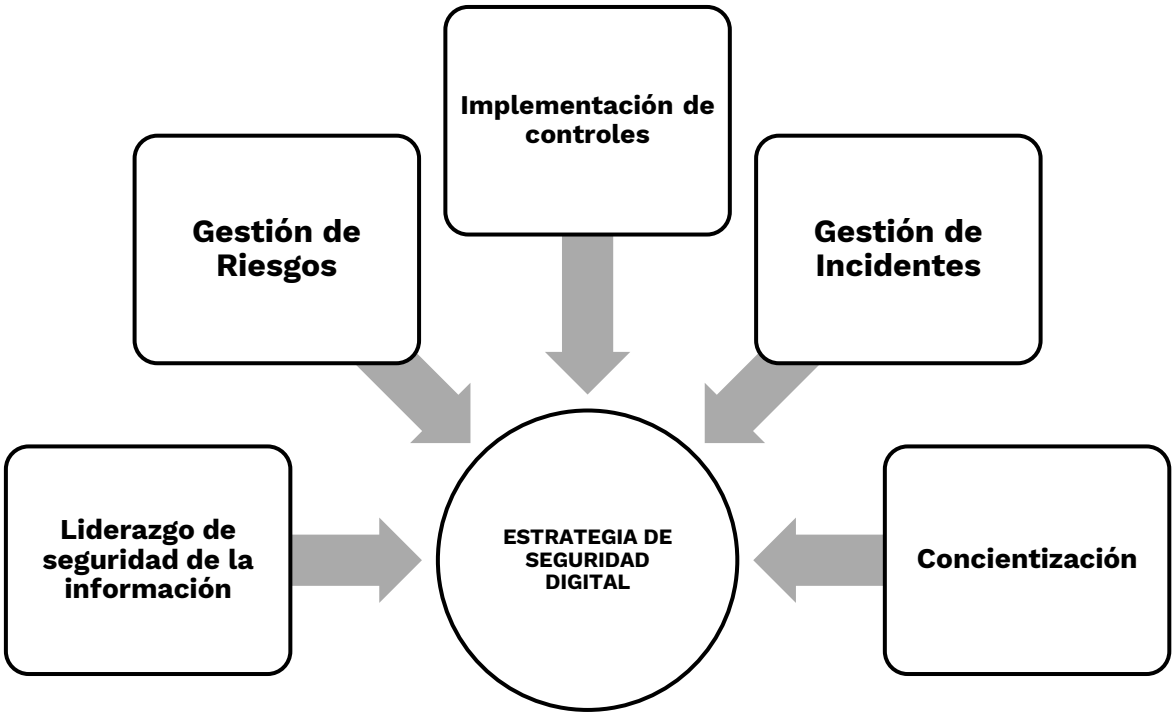
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	96	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	100	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	96	100	OPTIMIZADO
A.9	CONTROL DE ACCESO	99	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	100	100	OPTIMIZADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	99	100	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	97	100	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	95	100	OPTIMIZADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	86	100	OPTIMIZADO
A.15	RELACIONES CON LOS PROVEEDORES	100	100	OPTIMIZADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	97	100	OPTIMIZADO

A.18	CUMPLIMIENTO	100	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		**97**	100	100

6.2 Estrategia de seguridad digital[3]

La Agencia establece 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 en torno 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. Por tal motivo, la Agencia define las siguientes 5 estrategias específicas, que permiten establecer en su conjunto una estrategia general de la 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
Liderazgo de seguridad de la información	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.
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

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

	efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
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.

6.4 Portafolio de proyectos / actividades:

ESTRATEGIA / EJE	ACTIVIDADES	PRODUCTOS ESPERADOS
Gestión de riesgos	**ACTIVIDAD 1** Incorporar los riesgos asociados a continuidad del negocio a la Matriz de Riesgos de la Agencia. **ACTIVIDAD 2** Realizar seguimiento al Plan de Tratamiento de Riesgos de Seguridad.	**ACTIVIDAD 1** Publicar en Daruma la 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** Realizar rediseño e implementación DRP. **ACTIVIDAD 2** Mantener el servicio de Monitoreo de Seguridad. **ACTIVIDAD 3** Realizar Análisis de vulnerabilidades.	**ACTIVIDAD 1** Infraestructura implementada de acuerdo con el alcance definido. **ACTIVIDAD 2** Informes del Servicio SOC. **ACTIVIDAD 3** Informe de resultados de los análisis realizados.

	ACTIVIDAD 4 Realizar Análisis de Marca **ACTIVIDAD 5** Revisar y actualizar los controles implementados de seguridad y privacidad de la información	**ACTIVIDAD 4** Informe de resultados del análisis de marca **ACTIVIDAD 5** Matriz de controles actualizada.
Gestión de incidentes	**ACTIVIDAD 1** Gestión de incidentes de Seguridad de la Información.	**ACTIVIDAD 1** Registro del indicador de incidentes en el sistema Daruma.

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.	$100.000.000
Servicio de ciberseguridad para monitoreo de seguridad, monitoreo de red, análisis de vulnerabilidades, marca y afinamiento e implementación de estrategia de recuperación ante desastres en nube hibrida.	$819.249.762

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 asignación de tiempos y recursos Disminución de presupuesto	Incumplimientos legales y llamados de atención	Planificación y entrega del PAA a Financiera

8. INDICADORES

(A) (Actividades ejecutadas / Actividades programadas) *100

9. CRONOGRAMA

RESULTADO ESPERADO	PESO (%)	RESULTADOS / ENTREGABLES INTERMEDIOS	PESO (%)	RESPONSABLE	EJECUCIÓN	
					Fecha Inicio	Fecha Final
Identificar Riesgos de Continuidad del Negocio	10,00%	Incorporar riesgos asociados a continuidad del negocio a la Matriz de Riesgos de la Agencia.	100%	Oficial seguridad de la Información	1-jun-25	30-ago-25
Gestionar de Riesgos de Seguridad de la Información	10,00%	Seguimiento planes de tratamiento de riesgos de seguridad	100%	Oficial seguridad de la Información	15-feb-25	30-nov-25
Realizar rediseño e implementación DRP	25,00%	Infraestructura implementada de acuerdo con el alcance definido	100%	Oficial seguridad de la Información	15-feb-25	30-jul-25
Mantener el servicio de Monitoreo de Seguridad	15,00%	Informes Servicio SOC	100%	Oficial seguridad de la Información	15-feb-25	30-nov-25
Análisis de vulnerabilidades y marca	13,00%	Informe de resultados	100%	Oficial seguridad de la Información	15-feb-25	30-nov-25
Revisar y actualizar controles del MSPI	10,00%	Matriz de controles	100%	Oficial seguridad de la Información	15-feb-25	30-nov-25
Gestión de incidentes de Seguridad de la Información	17,00%	Registro del indicador de incidentes en el sistema Daruma	100%	Oficial seguridad de la Información	15-feb-25	30-nov-25

Elaboró	Revisó	Aprobó
Fredy Zea Rodriguez Contratista	**Oswaldo Useche** Jefe T.I **Carlos Adolfo Rangel** Gestor T1-14	Comité Institucional de Gestión y Desempeño - CIGD