



PLAN DE TRATAMIENTO

DE RIESGOS DE SEGURIDAD
Y PRIVACIDAD DE LA INFORMACIÓN

| 2022

CONTENIDO

INTRODUCCIÓN	3
OBJETIVOS DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.	3
OBJETIVO GENERAL	3
OBJETIVOS ESPECÍFICOS	3
ALCANCE	4
ÁMBITO DE APLICACIÓN	4
TÉRMINOS Y DEFINICIONES	4
ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	7
ACCIONES DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2022	11
SEGUIMIENTO Y EVALUACIÓN AL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.	13
CONTROL DE CAMBIOS	13

INTRODUCCIÓN

El presente plan se elabora con el fin de dar a conocer las acciones e iniciativas que se realizan en el marco de la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información, en el contexto del Modelo Integrado de Planeación y Gestión, alineándose con la Política de Gobierno Digital y Seguridad Digital, teniendo en cuenta los cuatro principios de la seguridad informática: confidencialidad, integridad, disponibilidad y privacidad de la información de la UPME.

Todos los servidores públicos en cumplimiento de sus funciones, están expuestos a la materialización de riesgos que pueden afectar los procesos; por lo tanto, es necesario tomar medidas, para la mitigación de los riesgos identificados.

OBJETIVOS DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

OBJETIVO GENERAL

Establecer las acciones para gestionar de manera integral los riesgos de seguridad y privacidad de la información, a partir de la metodología de análisis de riesgo (identificación, análisis, valoración, manejo y monitoreo).

OBJETIVOS ESPECÍFICOS

- Identificar, analizar y valorar los riesgos de seguridad y privacidad de la información asociados a los procesos de la UPME.
- Realizar la divulgación y socialización de la gestión adecuada de los riesgos de seguridad y privacidad de la información, a los funcionarios, contratistas y partes interesadas de la UPME.

- Identificar e implementar controles y acciones encaminadas a prevenir y administrar los riesgos de seguridad y privacidad de la información asociados a los procesos de la UPME.
- Establecer las medidas preventivas y predictivas para minimizar la materialización de los riesgos de seguridad y privacidad de la información.

ALCANCE

Este plan establece las actividades definidas por la Entidad para la administración y gestión de los riesgos de seguridad y privacidad de la información, desde la definición del contexto estratégico, la identificación de los riesgos, su análisis, valoración y la formulación de acciones para la presente vigencia fiscal.

ÁMBITO DE APLICACIÓN

Los lineamientos definidos en este plan, aplican para la gestión de los Riesgos de Seguridad y Privacidad de la Información asociados a los procesos de la UPME.

TÉRMINOS Y DEFINICIONES

Los siguientes son términos y definiciones considerados importantes en el desarrollo del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información:

- **Aceptación de riesgo:** Decisión de asumir un riesgo.
- **Activo de Información:** En relación con la seguridad y la privacidad de la información, se refiere al activo que contiene o representa información pública que la entidad genere, obtenga, adquiera, transforme o controle.
- **Activo de Seguridad de la Información:** En el contexto de seguridad digital, son activos los elementos que utiliza la entidad para funcionar en el entorno digital tales como: aplicaciones, servicios web, redes, información física o digital, tecnologías de información -TI, tecnologías de operación -TO.
- **Análisis de Riesgo:** Uso sistemático de la información para identificar fuentes y para estimar el riesgo (Guía ISO/IEC 73:2002).

- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Disponibilidad:** Propiedad de la información, que sea accesible y utilizable por solicitud de un usuario.
- **Evaluación del Riesgo:** Proceso de comparar el riesgo estimado contra criterios dados, con el fin de determinar la importancia del riesgo.
- **Evento de seguridad de la información:** Situación u ocurrencia identificada en el estado de un sistema, servicio o red, indicando una posible violación de la seguridad de la información, política o falla en los controles, o una situación previamente desconocida que puede ser relevante para la seguridad de la entidad.
- **Gestión del riesgo:** Conjunto de componentes que brindan las bases y las disposiciones para identificar, evaluar y controlar los riesgos de la entidad. Esto incluye el análisis y valoración de los activos, la identificación de amenazas a dichos activos y la evaluación de su vulnerabilidad ante esas amenazas.
- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **Incidente de seguridad de la información:** Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos de la entidad.
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- **Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades.
- **Riesgo:** Es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso.
- **Riesgo Inherente:** Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.
- **Riesgo residual:** Nivel restante de riesgo después del tratamiento del riesgo.
- **Riesgos de Seguridad Digital:** Posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.
- **Seguridad de la Información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad. [NTC-ISO/IEC 17799:2006]
- **Sistema de gestión de la seguridad de la información SGSI:** Parte del sistema de gestión global, basado en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.
- **Tratamiento del riesgo:** Proceso de selección e implementación de acciones de mejora que permita gestionar el riesgo.
- **Valoración del riesgo:** Proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo.

ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El éxito de la administración y gestión de riesgos de Seguridad Digital depende del compromiso y la participación de la Alta dirección, funcionarios y contratistas de la entidad; por esto, es preciso identificar los actores que intervienen y sus responsabilidades de acuerdo con los lineamientos establecidos en el Modelo Integrado de Planeación y Gestión - MIPG, a partir de la estructuración de las líneas de defensa que se presentan a continuación:

	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO DE SEGURIDAD DIGITAL
LÍNEA ESTRATÉGICA	Comité Institucional de Coordinación de Control Interno	<ul style="list-style-type: none"> Definir y aprobar la política para la administración del riesgo. Analizar los riesgos y amenazas institucionales, que puedan afectar el cumplimiento del plan estratégico. Analizar los riesgos, vulnerabilidades y amenazas que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la entidad, gestión de los procesos y capacidades para prestar servicios. Monitorear el cumplimiento de la política de administración de riesgo de la entidad (Ver criterios diferenciales política de Control Interno - MIPG, componente evaluación de Riesgos).
	Comité Institucional de Gestión y Desempeño	<ul style="list-style-type: none"> Definir y hacer seguimiento a los niveles de aceptación (apetito al riesgo). Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles. Analizar la gestión del riesgo y aplicar las mejoras.
PRIMERA LÍNEA DE DEFENSA	Líderes de Proceso Secretaria General Subdirectores (as) Jefes (as) de Oficina Responsable de proyecto	<ul style="list-style-type: none"> Identificar, valorar, evaluar y actualizar cuando se requiera, los riesgos que pueden afectar los objetivos, programas, proyectos y planes asociados a los procesos. Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras para su gestión. Ejecutar y supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar. Informar a la Oficina Asesora de Planeación (segunda línea) o quien haga sus veces, sobre los

	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO DE SEGURIDAD DIGITAL
		<p>riesgos materializados en los objetivos, programas, proyectos y planes de los procesos a cargo.</p> <ul style="list-style-type: none"> • Reportar los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos.
SEGUNDA LÍNEA DE DEFENSA	Oficial de Seguridad de la Información	<ul style="list-style-type: none"> • Liderar y coordinar la implementación de las políticas de Seguridad de la Información, con la participación activa de las dependencias de la entidad. • Evaluar y coordinar la implementación de controles específicos de Seguridad de la Información para nuevos sistemas de información o servicios informáticos. • Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes. • Identificar las necesidades y recursos necesarios (tecnológicos, humanos, de capacitación, financieros, etc.) para el mantenimiento de la infraestructura de Seguridad de la Información. • Identificar las necesidades de formación (capacitación y entrenamiento) del Comité Institucional de Gestión y Desempeño, y establecer un plan de capacitación para formar y entrenar a sus integrantes. • Actuar como asesor en Seguridad de la Información para la entidad. • Hacer seguimiento al comportamiento de los indicadores de gestión de la Seguridad de la Información que adopte el Comité Institucional de Gestión y Desempeño. • Realizar la evaluación del desempeño del SGSI. • Realizar la revisión y supervisión del SGSI. • Establecer un programa periódico (por lo menos una vez al año) de revisión de vulnerabilidades de la plataforma tecnológica de la entidad y coordinar los respectivos aseguramientos conforme los resultados de las mencionadas pruebas. • Reportar al Comité Institucional de Gestión y Desempeño el estado de la investigación y monitoreo de los incidentes de Seguridad de la Información, los resultados de las auditorías periódicas, la revisión y supervisión del SGSI. • Presentar al Comité Institucional de Gestión y Desempeño iniciativas e informes periódicos del estado de Seguridad de la Información de la entidad. • Identificar los organismos externos que ejerzan autoridad en lo relacionado con los aspectos de Seguridad de la Información e identificar los mecanismos de contacto respectivos. Al menos se debe identificar el contacto con las siguientes autoridades: Grupo Investigativo Delitos Informáticos

	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO DE SEGURIDAD DIGITAL
		<p>(DEINF) de la DIJIN, Unidad de delitos Informáticos de la Fiscalía General de la Nación, Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT), Comando Conjunto Cibernético (CCOC), Centro Cibernético Policial (CCP), Equipo de respuesta a incidentes de seguridad informática Gobierno (CSIRT).</p> <ul style="list-style-type: none"> • Identificar comunidades y grupos de interés relacionados con Seguridad de la Información que le permitan mantenerse actualizado y en contacto con expertos en los temas de Seguridad de la Información. • Definir el procedimiento para la Identificación y Valoración de Activos. • Adoptar o adecuar el procedimiento formal para la gestión de riesgos de Seguridad Digital (Identificación, Análisis, Evaluación y Tratamiento). • Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de Seguridad Digital y en la recomendación de controles para mitigar los riesgos. • Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos. • Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de Seguridad Digital.
<p>SEGUNDA LÍNEA DE DEFENSA</p>	<p>Coordinadores GIT: Administrativa, Financiera, Servicio al Ciudadano, Gestión Documental, Talento Humano Responsable del proyecto</p> <p>Supervisores</p> <p>Comité de contratación</p> <p>Delegados de Riesgos en cada proceso</p>	<ul style="list-style-type: none"> • Acompañar a los líderes de procesos en la identificación, análisis, valoración, evaluación del riesgo, la definición de controles bajo su responsabilidad y los temas a su cargo. • Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. • Realizar el seguimiento al mapa de riesgos de su proceso. • Reportar los avances de la gestión del riesgo. • Proponer las acciones de mejora a que haya lugar posterior al análisis, valoración, evaluación o tratamiento del riesgo. • Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su proceso o responsabilidad. • Identificar, analizar, valorar y evaluar los riesgos y controles asociados a su gestión con enfoque en la prevención del daño antijurídico bajo responsabilidad del Jefe de la Oficina Jurídica o quien haga sus veces • Comunicar al equipo de trabajo a su cargo la responsabilidad y resultados de la gestión del riesgo.

	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO DE SEGURIDAD DIGITAL
TERCERA LÍNEA DE DEFENSA	Oficina de Control Interno o quien haga sus veces	<ul style="list-style-type: none"> ● Brindar asesoría, orientación técnica, evaluación y seguimiento a la gestión del riesgo. ● Brindar asesoría a los responsables y ejecutores de los procesos y proyectos (primera línea de defensa), respecto a metodologías y herramientas para la identificación, análisis y evaluación de riesgos, como complemento a la labor de acompañamiento que deben desarrollar las oficinas de planeación (segunda línea de defensa). ● Asesorar a la primera línea de defensa de forma coordinada con el Grupo Interno de Planeación, en la identificación de los riesgos y diseño de controles. ● Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos. ● Pronunciarse sobre la pertinencia y efectividad de los controles. ● Recomendar mejoras a la política de operación para la administración del riesgo. ● Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa. ● Señalar aquellos aspectos que consideren una amenaza para el cumplimiento de los objetivos de los procesos, de los objetivos y metas institucionales, en el marco de la evaluación independiente. ● Identificar y alertar al Comité de Coordinación de Control Interno posibles cambios que pueden afectar la evaluación y el tratamiento del riesgo. ((Ver criterios diferenciales política de Control Interno - MIPG, componente evaluación de Riesgos).

De igual manera, el GIT de Planeación o quien haga sus veces, realizará acompañamiento metodológico para la gestión de Riesgos de Seguridad y Privacidad de la Información de la UPME.

Por su parte, los líderes de proceso tienen la responsabilidad de delegar el (los) profesional(es) que se encargará(n) del monitoreo, reporte y socialización de los riesgos asociados con Seguridad y Privacidad de la Información en la Entidad.

Todos los servidores, serán responsables de ejecutar controles operativos en el día a día.

ACCIONES DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2022

Para el año 2022 dentro de la identificación, análisis y valoración de los riesgos de Seguridad y Privacidad de la Información y acciones de tratamiento, se adelantarán las siguientes actividades:

ID	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	META	PRODUCTO	FECHA	
						INICIO	FIN
1	Actualización y adopción del contexto normativo aplicable al Sistema de Gestión de Riesgos de Seguridad Digital de la UPME	<ul style="list-style-type: none"> Revisión de la normatividad interna y externa de Seguridad y Privacidad de la información. Actualización y/o definición de instrumentos para la implementación de la Política para la Gestión Integral del Riesgo de la UPME en lo relacionado con Riesgos de Seguridad Digital (seguridad y privacidad de la información) de la entidad. Socialización a los funcionarios, contratistas y 	<ul style="list-style-type: none"> Oficial de Seguridad de la Información. Líder del Dominio Seguridad de la AE 	100%	Instrumentos para la implementación de la Política para la Gestión Integral del Riesgo de la UPME en lo relacionado con Riesgos de Seguridad Digital (seguridad y privacidad de la información) de la entidad.	01/02/21	30/11/21

		partes interesadas de los instrumentos para la Implementación de la Política para la Gestión Integral del Riesgo de la UPME específicamente en Riesgos de Seguridad y Privacidad de la Información de la entidad.					
2	Análisis de Riesgos de Seguridad Digital.	Realizar el Análisis de riesgos de Seguridad y Privacidad de la Información a los diferentes procesos de la entidad de acuerdo con la metodología adoptada por la UPME	Todas las áreas de la UPME Oficial de Seguridad de la Información.	100%	Matriz de Riesgos de Seguridad Digital de la UPME.	01/02/22	30/11/22
3	Monitoreo y revisión de la Gestión de Riesgos de Seguridad Digital.	Definición de indicadores para el monitoreo de la Gestión de riesgos de seguridad y privacidad de la información. Aprobación y seguimiento de indicadores para el monitoreo de la Gestión de riesgos de seguridad y	Oficial de Seguridad Jefe OGI	100%	Informes de monitoreo	01/02/22 15/06/22	15/06/22 30/11/22

		privacidad de la información.					
--	--	-------------------------------	--	--	--	--	--

SEGUIMIENTO Y EVALUACIÓN AL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Para el seguimiento y evaluación del Plan de Tratamiento de Riesgos de seguridad y privacidad de la información, se aplicarán instrumentos que permitan la generación de reportes cualitativos y cuantitativos con una periodicidad trimestral, para ser socializados ante el Comité institucional de gestión y desempeño de manera semestral.

CONTROL DE CAMBIOS

Fecha	Versión	No. Comité de Gestión y Desempeño de Aprobación	Observación o Motivo del Cambio
31/01/2021	1	Comité. No 3 del 27/01/2021	Actualización
16/06/2021	2	Comité. No.07 del 16/06/2021	<p>Identificación de mejora acorde con la metodología de riesgos emitida por Función Pública y lineamientos gubernamentales emitidos por MINTIC.</p> <ul style="list-style-type: none"> • Replanteamiento de los Objetivos del Documento. • Ajustes a las definiciones • Roles y Responsabilidades Replanteamiento de los roles que intervienen en la gestión de Riesgos de Seguridad Digital de la entidad y sus responsabilidades de acuerdo con los lineamientos establecidos en MIPG, se incluyó la estructuración de las líneas de defensa. <p>Eliminación punto 7.1 Procedimiento para la gestión de riesgos en la UPME, se generará documento (Procedimiento o Metodología para la Gestión de Riesgos de Seguridad Digital en la entidad)</p> <ul style="list-style-type: none"> • Acciones del Plan. • Actividad No.1 Replanteamiento de descripción, responsables y entregables de la Política de Gestión de Riesgos de Seguridad y Privacidad de la Información. • Actividad No.2 Consolidación de actividades No.2 y No.3, dejando Actividad general: Análisis de Riesgos de Seguridad Digital. • Actividad No.3 Redefinición de la actividad No.4 Monitoreo y revisión de la Gestión de Riesgos de Seguridad Digital. • Seguimiento y evaluación al plan de tratamiento de riesgos de seguridad y privacidad de la información. Se modificó el siguiente ítem: • Adopción de la Política de Gestión de Riesgos de Seguridad Digital (Seguridad y Privacidad de la Información) de la UPME Inclusión de los siguientes ítems: - Seguimiento al Plan con una periodicidad trimestral Presentación de los avances en el Comité institucional de Gestión y Desempeño con una periodicidad semestral.
31/01/2022	1	Comité. No 2 del 31/01/2022	<p>Actualización 2022</p> <p>Inclusión de acciones a ejecutar en la presente vigencia</p>

PLAN DE TRATAMIENTO

DE RIESGOS DE SEGURIDAD
Y PRIVACIDAD DE LA INFORMACIÓN



www.upme.gov.co