PLAN TRATAMIENTO DE RIESGOS EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CÓDIGO: IM OC GTI PE 003
REVISIÓN: 4
FECHA DE LIBERACIÓN:

Documento firmado digitalmente:

REVISÓ	APROBÓ
_____ Nombre: Coronel (RA) Sonia Dolly Gutiérrez Carrillo Cargo: Gerente de Tecnologías de la Información _____ Nombre: **Leyda Nelcy Aguirre Martinez** Cargo: **Profesional Master GTI** _____ Nombre: **Sergio Alberto Villada Agudelo** Cargo: **Director de Transformación y Riesgos**	_____ Nombre: **CR (RA) Oscar Alberto Jaramillo Carrillo** Cargo: **Vicepresidente Corporativo** _____- Nombre: **Ronald Jamilton Moreno Samaniego** Cargo: **Jefe Oficina de Planeación**

Elaborado por:

Nombre: **Luisa Fernanda Pulido Paez**
Cargo: **Profesional GTI**

Tabla de contenido

PLAN TRATAMIENTO DE RIESGOS EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

La Industria Militar en procura de mejorar y transformar la gestión de calidad de la entidad adquiere una herramienta que busca transformar las actividades de la gestión de las personas, haciéndolas simples para conectarlas a una cultura de mejora continua.

La Gerencia de Tecnologías de la Información basada en los objetivos estratégicos de la Industria Militar y en la nueva herramienta diseña el plan de tratamiento de riesgos de Seguridad y Privacidad de la información con el fin de migrar datos reales y de esta manera mitigar los riesgos existentes, mediante este documento se establece un objetivo, alcance, medidas, y estrategias que buscan la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad que serán aplicadas durante el transcurso del 2023-2026.

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.

2. DEFINICIONES

- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

- **Riesgo de Seguridad de la Información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **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:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

- **Impacto:** consecuencias que puede ocasionar a la organización la materialización del riesgo.

- **Control o Medida:** Medida que permite reducir o mitigar un riesgo

3. OBJETIVO

Determinar una metodología para abordar y sintetizar los riesgos de seguridad y privacidad de la información mediante la caracterización, análisis, valoración y aplicación de los riesgos de pérdida de confidencialidad, disponibilidad e integridad de la información para prevenir su materialización y/o comprimir los impactos negativos en la gestión institucional.

3.1 OBJETIVOS ESPECÍFICOS

En beneficio del apoyo y cumplimiento al plan de tratamiento de riesgos en seguridad y privacidad de la información, se declaran los siguientes objetivos específicos:

- Analizar y seleccionar la metodología a operar dentro de la herramienta de Gestión de la calidad para la gestión del riesgo.

- Determinar las amenazas y vulnerabilidades por medio de entrevistas e incidentes de seguridad presentados en los activos de información encontrados para determinar el riesgo.

- Establecer los controles por medio de estándares para mitigar los riesgos de los activos identificados.

- Estimar el riesgo de manera cualitativa con el fin de considerar su impacto en caso de materializarse un riesgo.

- Optimizar continuamente los conocimientos del equipo de trabajo en materia de seguridad digital y prevención de riesgos.

4. ALCANCE DE DOCUMENTO

El presente plan tratamiento de riesgos en seguridad y privacidad de la información se orienta en todos aquellos activos de la información dentro del alcance del sistema de Seguridad de la Información.

5.MARCO DE REFERENCIA

5.1 Política de Administración de Riesgos

La Industria Militar se alinea sobre la política para la gestión de los riesgos y las oportunidades en la industria militar IM OC OFP CP 002 y para el análisis de riesgos de Seguridad de la Información toma como guía el PROCEDIMIENTO GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN IM OC GTI PR 015

5.2 Rol y responsabilidades

Para la Gestión de riesgos en el Informativo Roles y Responsabilidades del Modelo de Seguridad y Privacidad de la Información IM OC GTI IF 009, se define:

Rol Gestor de Riesgos

Propósito: Todos los colaboradores de la Industria Militar de Colombia son responsables de la identificación, evaluación y control de los Activos y riesgos de seguridad de la información. No obstante, la entidad asigna un responsable de la gestión, custodia y preservación lógica o física de los activos de información, de los riesgos de seguridad y privacidad de la información de cada proceso. Las principales responsabilidades de este rol incluyen, pero no se limitan a:

Capacitar y guiar al personal de la Industria Militar en la identificación y clasificación de Activos de Información.

Identificar, registrar y actualizar en conjunto con los líderes de proceso y/o jefes de dependencia los activos de información de la entidad.

Realizar la clasificación y valorización de los activos de información y revisarla como mínimo anualmente para garantizar que corresponde a los requisitos legales, normativos, contractuales y de la entidad.

- Determinar los privilegios de acceso y criterios de respaldo para los activos de información.
- Aprobar la divulgación de información que este bajo su proceso.
- Comunicar violaciones de seguridad o incidentes sobre los activos de información de su proceso.
- Velar que la información que le ha sido confiada sea protegida durante su ciclo de vida (creación, almacenamiento, distribución, transporte y destrucción segura) de modificaciones y usos no autorizados.
- Liderar y brindar acompañamiento a los procesos de la entidad en la gestión de riesgos de seguridad y privacidad de la información, así como los controles correspondientes para su mitigación y seguimiento al plan de tratamiento de riesgos, de acuerdo con las disposiciones y metodologías en la materia.
- Identificar, valorar y gestionar los riesgos del Sistema de Gestión de Seguridad de la Información.
- Analizar, actualizar y valorar las vulnerabilidades y amenazas que afectan los activos de información. La versión vigente y controlada de este documento, solo podrá ser consultada a través del Gestor Documental INDUDARUMA La copia o impresión diferentes a la publicada, será considerada como documento no controlado y su uso indebido no es responsabilidad del Grupo Administrador de Documentos de la Industria Militar
- Revisar y gestionar para que los controles de seguridad sean implementados de acuerdo al nivel de clasificación de la información de su proceso.
- Identificar, actualizar y guiar la definición de planes de acción para tratar los riesgos.
- Contribuir al desarrollo de los manuales de normas y procedimientos.

6.METODOLOGÍA DE GESTIÓN DE RIESGOS

La Industria Militar, En cumplimiento a la política de seguridad digital y el modelo de seguridad y privacidad de la información (MSPI), se identifica, analiza, evalúa y trata el riesgo de los activos de información con el fin de establecer las amenazas, vulnerabilidades, e impacto de situaciones adversas que puedan afectar la operación y funcionamiento normal de los activos de información de la organización.

Dentro de Marco de Seguridad del Modelo de Seguridad y Privacidad de la información (en adelante MSPI), un tema decisivo, es la Gestión de riesgos la cual es utilizada para la toma de decisiones. Por otra parte, Teniendo en cuenta que el contexto organizacional, son las entidades del Estado, la metodología en la cual se basa La Industria Militar es la “Guía de Riesgos” del DAFP, buscando que haya una integración a lo que se ha desarrollado dentro de la Entidad para otros modelos de Gestión, y de éste modo aprovechar el trabajo adelantado en la identificación de Riesgos para ser complementados con los Riesgos de Seguridad. Es así como alineando los Objetivos estratégicos de la Entidad, al desarrollo del MSPI se logra una integración con lo establecido a través de la guía de Riesgos del DAFP, así como con lo determinado en otros modelos de Gestión

Es importante resaltar que para la evaluación de riesgos en seguridad de la información un insumo vital es la clasificación de activos de información ya que una buena práctica es realizar gestión de riesgos a los activos de información que se consideren con nivel de clasificación ALTA dependiendo de los criterios de clasificación; es decir que en los criterios de Confidencialidad, Integridad y Disponibilidad tengan la siguiente calificación:

El proceso de Gestión de Riesgos en la seguridad de la información consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento.

- Proceso para la administración del riesgo:

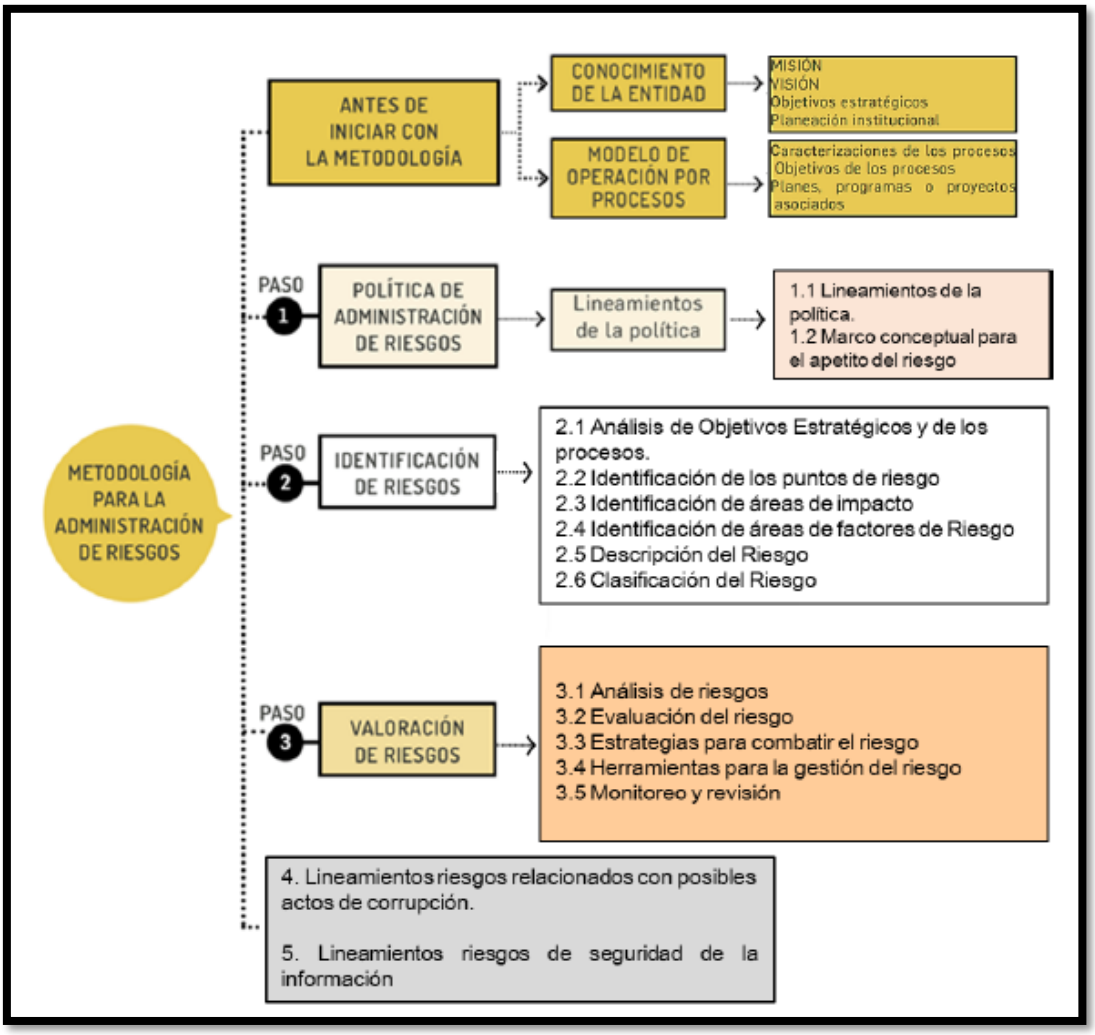

Imagen 1. Tomado de la Cartilla de Administración de Riesgos del DAFP

- Proceso para la administración del riesgo en seguridad de la información

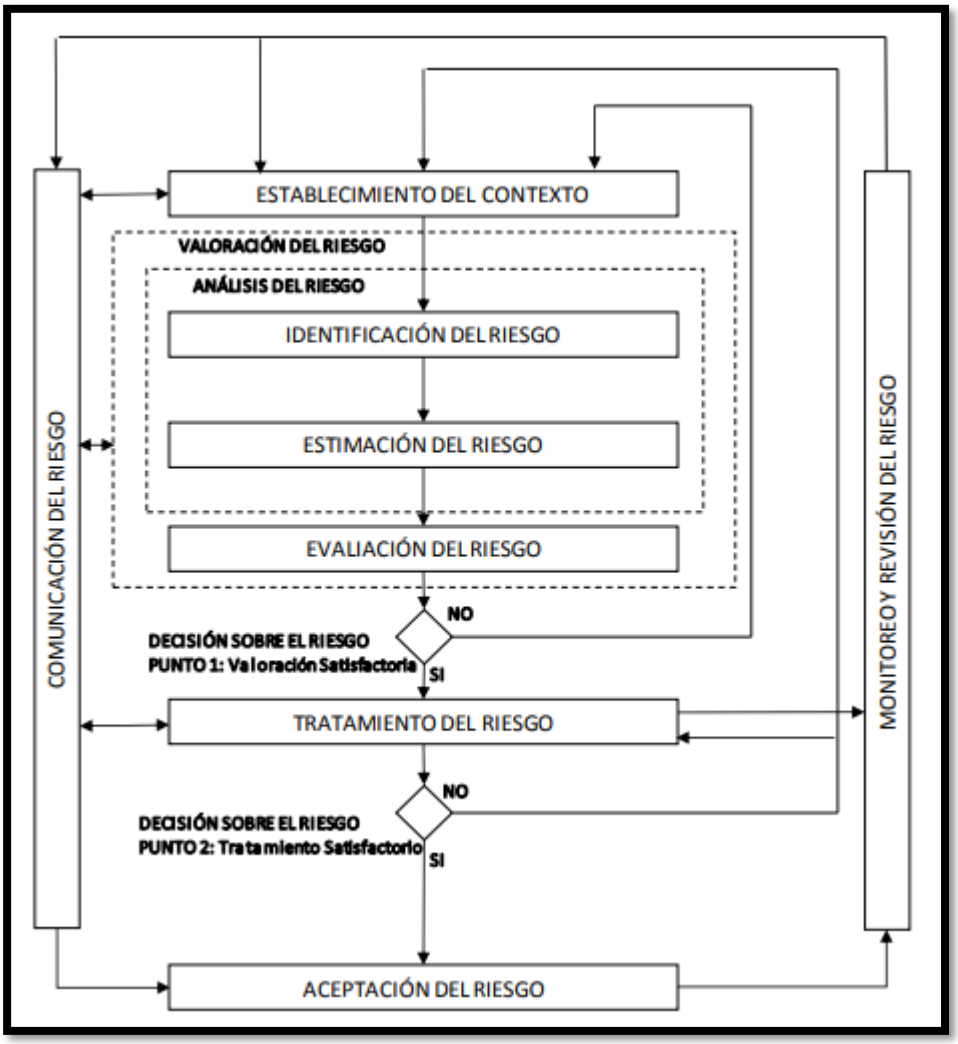

Imagen 2. Tomado de la NTC-ISO/IEC 27005

Así como lo ilustra la imagen 2 el proceso de gestión del riesgo en la seguridad de la información puede ser iterativo para las actividades de valoración del riesgo y/o el tratamiento del mismo. Un enfoque iterativo para realizar la valoración del riesgo puede incrementar la profundidad y el detalle de la valoración en cada iteración

El contexto se establece como primera medida, luego se realiza la valoración del riesgo y si esta suministra información suficiente para determinar de manera eficaz las acciones que se necesitan para modificar los riesgos a un nivel aceptable entonces la labor está terminada y sigue el tratamiento del riesgo. Si la información no es suficiente, se llevará a cabo otra iteración de la valoración del riego con un contexto revisado (por ejemplo, los

criterios de evaluación del riesgo los criterios para aceptar el riesgo o los criterios de impacto).

La eficacia del tratamiento de tratamiento del riesgo depende de los resultados de la valoración del riesgo. Es posible que el tratamiento del riesgo no produzca inmediatamente un nivel aceptable de riesgo residual en esta situación, si es necesaria, se puede requerir otra iteración de la valoración del riesgo con cambios en los parámetros del contexto (por ejemplo, criterios para la valoración del riesgo, de aceptación o de impacto del riesgo).

La actividad de aceptación del riesgo debe asegurar que los riesgos residuales son aceptados explícitamente por los directores de la entidad. Esto es especialmente importante en una situación en la que la implementación de los controles se omite o se pospone, por ejemplo, por costos. La siguiente tabla resume las actividades de gestión del riesgo en la seguridad de la información que son pertinentes para las cuatro fases del proceso del MSPI

ETAPAS DEL MSPI	PROCESO DE GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACION
Planear	Establecer Contexto Valoración del Riesgo Planificación del Tratamiento del Riesgo Aceptación del Riesgo
Implementar	Implementación del Plan de Tratamiento de Riesgo.
Gestionar	Monitoreo y Revisión Continuo de los Riesgos.
Mejora Continua	Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información.

Tabla 1. Etapas de la Gestión del Riesgo a lo Largo del MSPI

7.PROCESO DE DESARROLLO (PENDIENTE)

7.1 Identificación y Valoración del Riesgo

7.2 Tratamiento de Riesgos de Seguridad de la Información

7.3 Seguimiento y Control

8.CRONOGRAMA

9.RECURSOS

La estimación y asignación de los recursos para el plan de tratamiento de riesgos de Seguridad de la información identificados en la entidad, corresponderá al dueño del riesgo, quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos en el plan de tratamiento. Si el establecimiento de los controles implica la adquisición de herramientas tecnológicas bajo la responsabilidad de la Gerencia de Tecnologías de la Información.

10.INDICADORES

La medición se realiza con un indicador de gestión que está orientado principalmente a disminuir el número de riesgos identificados con nivel alto y externo a través de la implementación y evaluación de controles. El número de riesgos identificados como no aceptables no debe ser superior al 20% del total de riesgos identificados.

La Gerencia de Tecnologías de la Información asesora a las áreas en el proceso de identificación y valoración de los riesgos de seguridad de información y seguridad digital, asimismo apoyará a los responsables de las áreas en la definición de los controles y hará seguimiento a su implementación, con el fin, de evidenciar en el siguiente ciclo la efectividad de los controles implementados y en consecuencia la disminución del riesgo No aceptable. Así mismo, si se llegan a presentar incidentes de seguridad se validarán los riesgos identificados para determinar si obedece a un riesgo identificado y proceder a valorar, recalificar e implementar nuevos controles.