Plan

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

GTE-PL-03-V7

Gestión Tecnológica
UNIDAD NACIONAL DE PROTECCIÓN
21-03-2024

COLOMBIA POTENCIA DE LA VIDA

Tabla de Contenido

1. OBJETIVO

Generar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información alineado a la metodología de Gestión del Riesgo de la Entidad, que permita a los responsables de los procesos de la UNP gestionar los riesgos que en materia de Seguridad y Privacidad de la Información, identificados a partir de los activos físicos y de información que hacen parte de la Entidad y valorados por sus dueños de acuerdo con el nivel de importancia respecto a su confidencialidad, integridad y disponibilidad.

2. ALCANCE

La gestión de Seguridad y Privacidad de la Información inicia con la identificación de los activos físicos y de información de la entidad y termina con el plan de tratamiento de los riesgos a los cuales están expuestos dichos activos, siguiendo las normas vigentes, la metodología definida por la entidad para la gestión del riesgo, las pautas y recomendaciones previstas en la ISO 31000 para su identificación, valoración, tratamiento y monitoreo enfocado al mantenimiento y mejoramiento continuo.

3. DEFINICIONES

ACTIVO: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, elementos de infraestructura física y computacional; servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital. (Norma ISO 9000).

ACTIVO DE INFORMACIÓN: Los activos de información son datos o información propietaria en medios electrónicos, impreso o entre otros medios, considerados sensitivos o críticos para los objetivos de la entidad o proceso. En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal. (Norma ISO 27000).

ADMINISTRACIÓN DEL RIESGO: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)

AMENAZA: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO 27000)

ANÁLISIS DE RIESGOS: Uso sistemático de la información para identificar las fuentes y estimar el riesgo. (ISO 27000)

APETITO AL RIESGO: magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)

CAUSA: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)

CONFIDENCIALIDAD: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. (ISO 27000)

CONSECUENCIA: Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas. Control: medida que modifica el riesgo (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)

CONTROL: Medida por la que se modifica el riesgo. Los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto. Los términos salvaguardan o contramedida son utilizados frecuentemente como sinónimos de control. (ISO 27000).

DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. (ISO 27000).

EVALUACIÓN DE RIESGOS: proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo. (ISO 27000).

EVITACIÓN DEL RIESGO. Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)

FACTORES DE RIESGO: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)

IDENTIFICACIÓN DEL RIESGO: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo. (ISO 27000).

IMPACTO. Cambio adverso en el nivel de los objetivos del negocio logrados. NTC-ISO 27005:2008. (ISO 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. (ISO 27000).

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Propiedad de la información relativa a su exactitud y completitud. (ISO 27000).

PROBABILIDAD: se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)

REDUCCIÓN DEL RIESGO: Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo. (ISO 27005).

RETENCIÓN DEL RIESGO: Aceptación de la pérdida o ganancia proveniente de un riesgo particular Fuente: (ISO 27005).

RIESGO DE CORRUPCIÓN: posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)

RIESGO DE SEGURIDAD DE LA INFORMACIÓN: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información. Seguridad de la información: preservación de la confidencialidad, integridad, y disponibilidad de la información. Fuente (NTC-ISO/IEC 27005).

RIESGO DE SEGURIDAD DIGITAL: combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como 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. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)

RIESGO INHERENTE: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)

RIESGO RESIDUAL: Nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)

RIESGO: En el contexto de los Sistemas de Gestión de Seguridad de la Información, los riesgos de Seguridad y Privacidad de la información pueden expresarse como un efecto de incertidumbre sobre los objetivos de seguridad de la información. El riesgo de Seguridad de la

Información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización. (ISO 27000).

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. (ISO 27000).

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI: parte del sistema de gestión global, basada 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. (ISO 27000).

TRATAMIENTO DEL RIESGO: Proceso para modificar el riesgo. (ISO 27000).

VALORACIÓN DEL RIESGO: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos. (ISO 27000).

VULNERABILIDAD: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO 27000).

4. MARCO LEGAL

I. Teniendo en cuenta lo dispuesto en el Decreto 612 de 2018 respecto a la integración de planes institucionales y estratégicos al plan de acción, el presente documento desarrolla la siguiente actividad descrita en el Plan de Acción "Adoptar las Guías del Sistema de Gestión de Seguridad y Privacidad de información - SGSI del modelo de seguridad y privacidad de la información - MSPI del Min-Tic en la UNP", del cual se presentará el producto "Documento informe de seguimiento de implementación del sistema de gestión de seguridad de la información.".
II. NTC / ISO 27001:2022 - Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
III. NTC / ISO 22301:2019 Sistemas de Gestión de la Continuidad del Negocio.
IV. NTC/ISO 10911:2018 Directrices para la auditoria de los Sistemas de Gestion/ Norma Tecnica Internacional.
V. NTC/ISO 31000:2018 ISO 31000 Gestión del Riesgo Principio y Directrices / Norma Tecnica Internacional.
VI. Modelo de Seguridad y Privacidad de la Información Cartilla No. 7 del Ministerio de Ciencia y Tecnología MinTIC.
VII. Cartilla del Departamento Administrativo de la Función Pública DAFP V6 – Noviembre de 2022.
VIII. Anexo 4 Modelo Nacional de Gestión de Riesgos en Seguridad de la Información en Entidades Públicas. - Ministerio de Tecnologías de la Información y las Comunicaciones - Octubre 2021.

IX. Gobierno Digital Seguridad y Privacidad de la Información – Enero 2024.

5. CONDICIONES GENERALES

El presente documento está enmarcado en las pautas del Gobierno Nacional, específicamente en la Política Nacional de Seguridad Digital, en las directrices de manejo de riesgos de seguridad de la información y oportunidades establecidas por la Entidad, buscando determinar las acciones y mejores prácticas para tratar los posibles riesgos y oportunidades de seguridad y privacidad de la información.

6. CONTENIDO

6.1 Estrategias

La Unidad Nacional de Protección – UNP, mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información pretende proteger, preservar y administrar la Confidencialidad, Integridad y Disponibilidad de la Información, mediante una gestión integral de riesgos y la implementación de controles de Seguridad de la Información, con el fin de mitigar y reducir la probabilidad de ocurrencia de incidentes y cumplir con los requisitos legales y reglamentarios vigentes, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad y Privacidad de la Información.

Para lograr el cumplimiento del Plan se definen las siguientes estrategias:

1. Compromiso: es importante que la alta dirección promueva, apoye y asegure la disponibilidad de los recursos parala ejecución de los proyectos necesarios para la gestión integral de riesgos de Seguridad y Privacidad de la Información.
2. Integración de los riesgos de Seguridad y Privacidad de la Información al marco de gestión de riesgos de la UNP por parte de la Oficina Asesora de Planeación e Información.
3. Gestionar los riesgos de Seguridad y Privacidad de la Información.
4. Mitigar los impactos y reducir la probabilidad de ocurrencia de posibles incidentes de Seguridad y Privacidad de la Información, de forma efectiva, eficaz y eficiente.
5. Adopción de la cultura de Seguridad y Privacidad de la Información con un compromiso de todos los Servidores Públicos, Contratistas y Grupos de Interés de la UNP frente los riesgos de Seguridad y Privacidad de la Información y su tratamiento.

6.2 Gestión del Riesgo

6.2.1. Visión General la Gestión del Riesgo

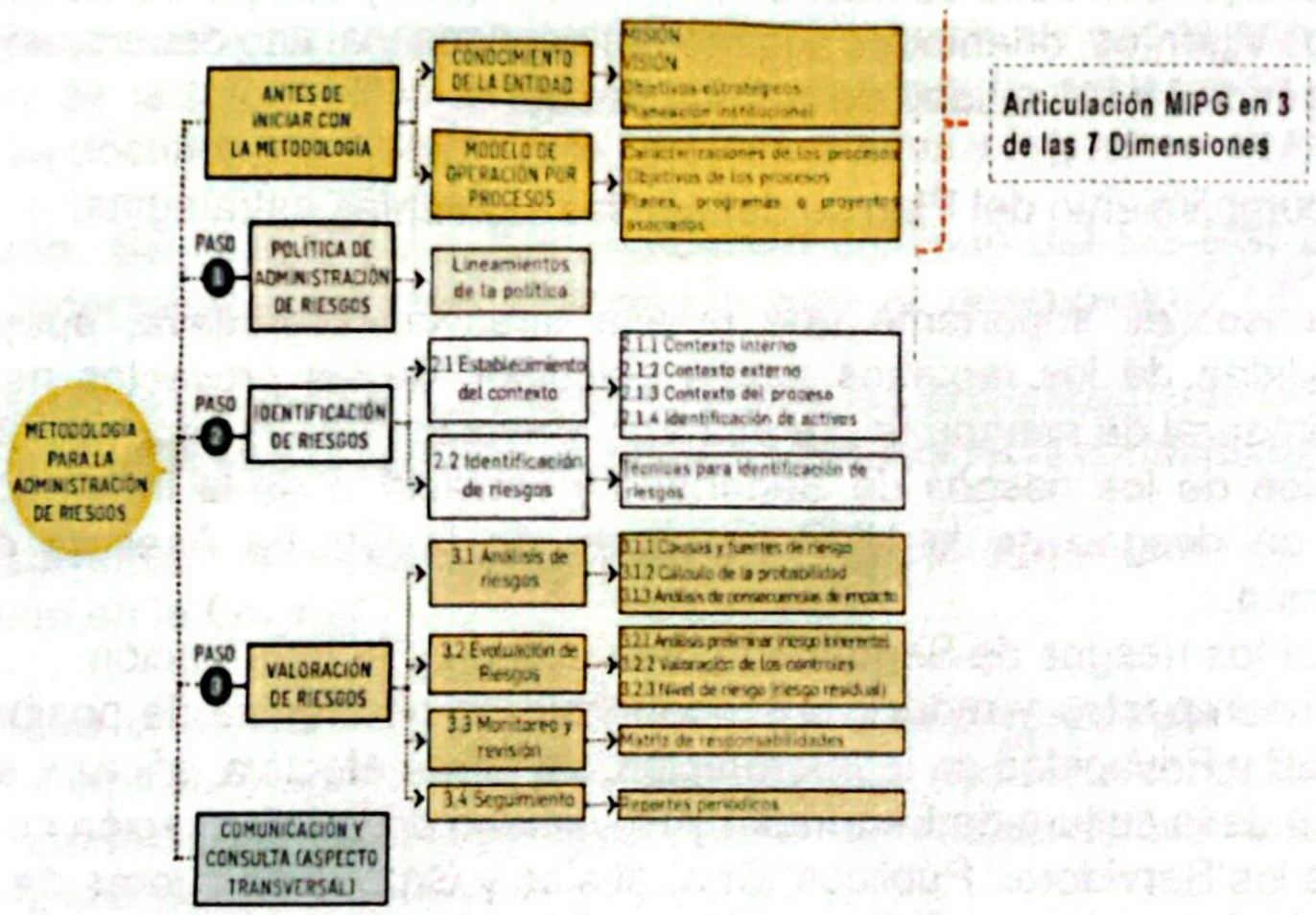
De acuerdo con la Guía de Gestión de Riesgos del DAFP – Departamento Administrativo de la Función Pública, las etapas generales para la Gestión de Riesgos adoptados por la UNP

contemplan el compromiso de la dirección de la Entidad, el equipo interdisciplinario encargado de la administración del modelo de gestión de riesgos y las capacitaciones de la metodología, lo cual está a cargo de la Oficina Asesora de Planeación e Información.

En lo que respecta a la Seguridad y Privacidad de la Información, se integrara a la Gestión de Riesgos adoptada por la UNP con la norma técnica NTC-ISO 31000:2018 Principios y directrices de la Gestión del Riesgo que brinda soporte a los conceptos generales que se especifican en la norma NTC-ISO 27001:2022 y está diseñada para facilitar la implementación satisfactoria de la seguridad y privacidad de la información con base en la gestión de Riesgos y oportunidades asociados a los activos de información.

La guía Metodológica para la Administración del Riesgo (Ilustración 1) del Departamento Administrativo de la función Pública es la carta de navegabilidad para la administración del Riesgo en las Entidades Públicas, la cual actúa en concordancia con el componente de Administración del Riesgo establecido en el Manual Estándar de control Interno para el Estado Colombiano en la Identificación, Valoración, Análisis y Seguimiento y Monitoreo de los mismo en una entidad.

Ilustración 1 Metodología para la Administración de Riesgos



Fuente: *DAFP (2020)*

6.2.2 Actualizar acorde con ISO 27001:2022 y describir las etapas.

La norma ISO 27001:2022 establece un conjunto de requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI), a continuación, se describen las etapas del proceso de

implementación de un SGSI según la norma ISO 27001:2022, fundamentado en una estructura de Riesgos:

1. **Inicio del proyecto:** Esta etapa implica la definición del alcance del SGSI, la identificación de los activos físicos y de información críticos de acuerdo con la valoración de estos, la comprensión de las necesidades y expectativas de las partes interesadas y la asignación de roles y responsabilidades.

2. **Análisis de riesgos:** En esta etapa se lleva a cabo una evaluación sistemática de los posibles riesgos de Seguridad de la Información con el fin de identificar las amenazas, vulnerabilidades y posibles impactos en los activos críticos identificados dentro de la organización, y finaliza con la determinación de las acciones de tratamiento necesarias para mitigar los riesgos identificados.

3. **Planificación:** Se elabora un plan de Gestión de Seguridad y Privacidad de la Información, donde se establecen los objetivos y metas del SG-PSI, se identifican las medidas de seguridad necesarias, se establece un cronograma de implementación y se asignan los recursos necesarios.

4. **Implementación:** En esta etapa se implementan las medidas de seguridad definidas en la etapa anterior, se realizan controles que estarán alineados con las políticas de seguridad de la información definidos en la entidad, la declaración de aplicabilidad (SOA) y se documentan los procesos, procedimientos y reglas necesarias.

5. **Evaluación:** Se lleva a cabo una evaluación continua del SG-PSI para verificar su eficacia, detectar posibles desviaciones y mejorar el desempeño.

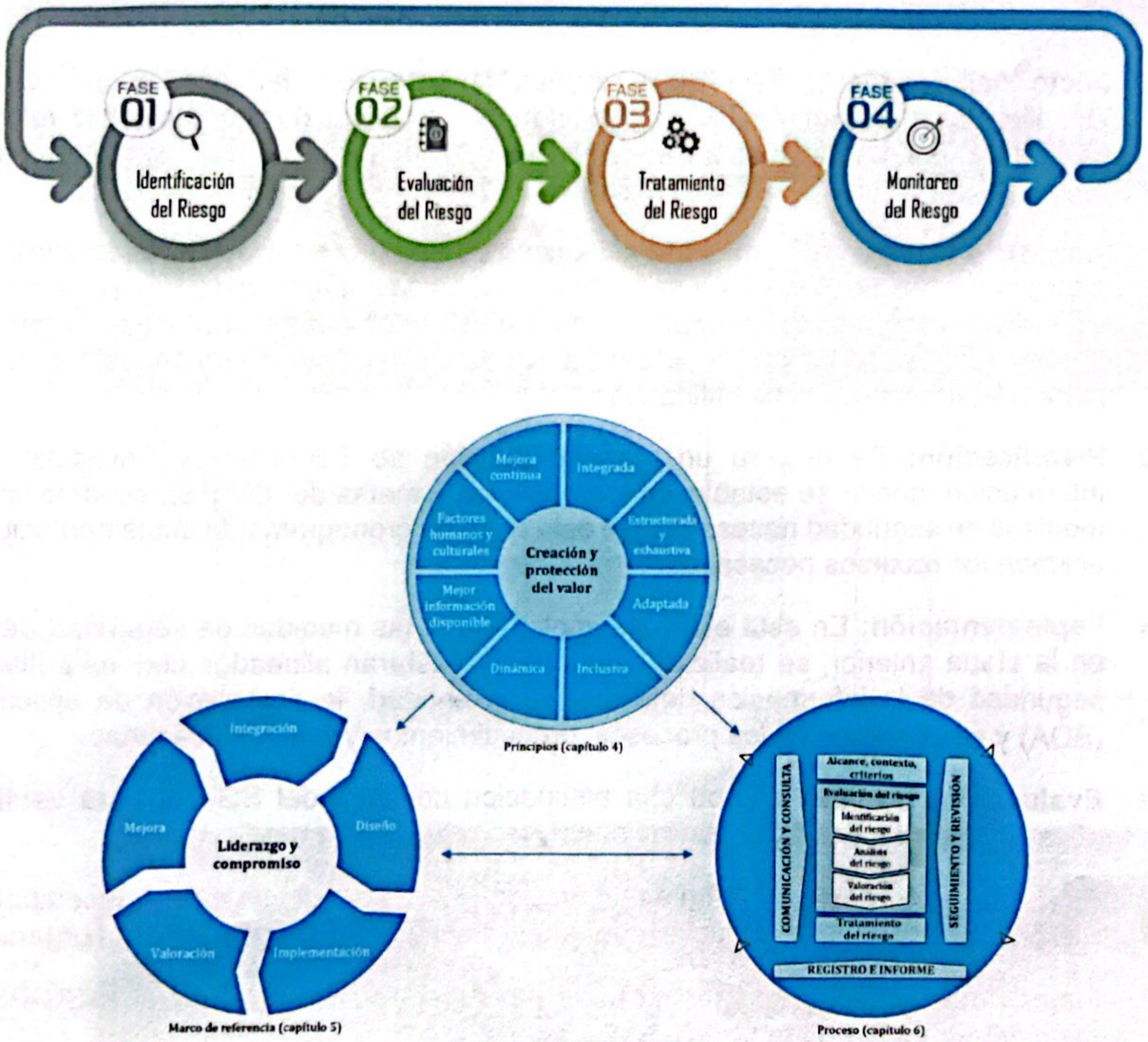
6. **Revisión por la Dirección:** La alta dirección revisa periódicamente el desempeño SG-PSI para asegurar su adecuación, idoneidad y eficacia en el contexto de la organización.

7. **Mejora continua:** Se toman acciones para mejorar continuamente el SG-PSI y su desempeño en la Entidad.

Cabe destacar que la norma ISO 27001:2022 sigue una metodología de mejora continua conocida como Planificar-Hacer-Verificar-Actuar (PHVA), también conocida como ciclo de Deming. Esta metodología se aplica en cada una de las etapas mencionadas anteriormente para garantizar la efectividad del SG-PSI.

La ilustración 3 muestra que, el proceso de Gestión del Riesgo es un proceso cíclico en sus diversas actividades y se puede implementar tan detalladamente como se requiera el tratamiento.

Ilustración 3 Proceso de gestión del riesgo en la seguridad de la información



Fuente: ISO 31000:2018

6.2.3 Etapas para la Gestión del Riesgo

6.2.3.1 Identificación y Valoración de Riesgos

De acuerdo con la guía del Departamento Administrativo de la Función Pública DAFP V6, la norma ISO 27001:2022 en sus numerales (6.1.2 y 8.2) de Seguridad de la Información y la asociación Activo – Riesgo - Control, en esta etapa se identifican los riesgos que están bajo el control de la Entidad, teniendo en cuenta las cuestiones internas y externas, la comprensión de las necesidades y expectativas , y la caracterización de cada proceso que pueden generar riesgos que afecten el cumplimiento de los objetivos en SI, estas actividades se encuentran

descritas dentro de la GTE-GU-04 Guía Identificación y Valoración de Riesgos de Seguridad y Privacidad de la Información y el formato GTE-FT-36 Identificación y Valoración de Riesgos de Seguridad y Privacidad de la Información.

Tabla 1. Acciones Proceso de Gestión de Riesgos de Seguridad y Privacidad de la Información

IDENTIFICACIÓN							
PROCESO	TIPO DE RIESGO	DUEÑO DEL RIESGO	RIESGO	Principio de SI			CAUSAS O EVENTOS (Activos Asociados)
				Conf.	Integr.	Disp.	

Fuente: Elaboración propia / GTE-GU-04 GIVRSPI

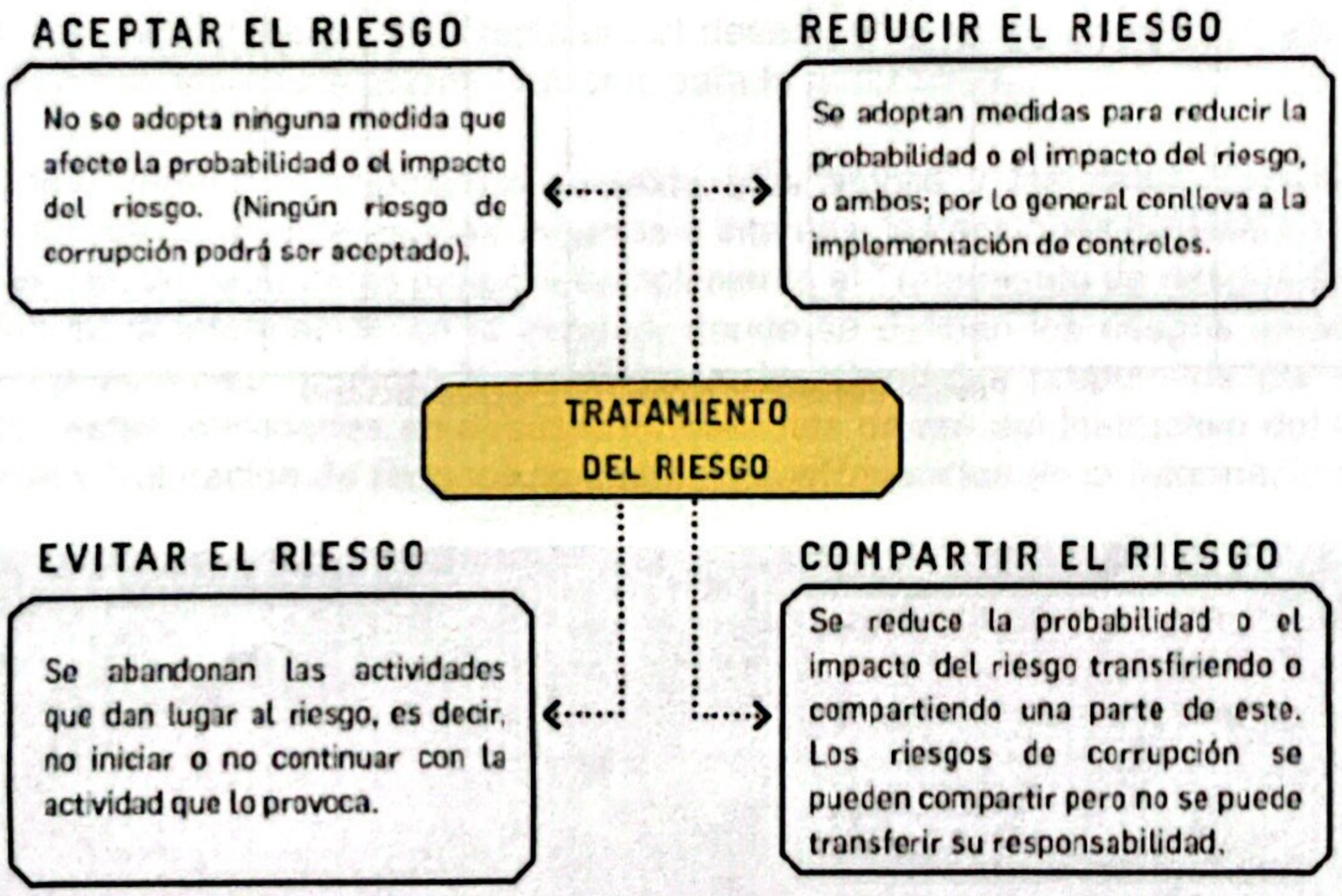
Tabla 2 valoración

VALORACIÓN				
PROBABILIDAD (INHERENTE) ESCALA	IMPACTO (INHERENTE) ESCALA	EVALUACION RIESGO INHERENTE (Probabilidad x Impacto)	NIVEL DE RIESGO INHERENTE (Riesgos propios del Proceso)	OPCIÓN DE TRATAMIENTO (Mitigar Asumir Evitar Transferir)
RARA VEZ = 1 IMPROBABLE = 2 POSIBLE = 3 PROBABLE = 4 CASI SEGURO = 5	INSIGNIFICANTE = 3 MENOR = 6 MODERADO = 9 MAYOR = 12 CATASTROFICO = 15			
0	0	#N/D	#N/D	

Fuente: Elaboración propia / GTE-GU-04 GIVRSPI

6.2.3.2 Tratamiento del Riesgo

¿Qué es tratamiento del riesgo?
Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción. A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, y partiendo de lo que establezca la política integral del riesgo, los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento. Pero en caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables para la dirección se deberá volver a analizar y revisar dicho tratamiento. El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:



Fuente: DAFP guía de administración de riesgos V6

El propósito del tratamiento del riesgo es seleccionar e implementar acciones para abordar el riesgo, en la UNP el tratamiento del riesgo implica un proceso iterativo de formular y seleccionar opciones para el tratamiento del riesgo, planificar e implementar el tratamiento del riesgo, evaluar la eficacia de ese tratamiento, decidir si el riesgo residual es aceptable y si no es aceptable, efectuar tratamiento adicional.

Las opciones de tratamiento del riesgo no necesariamente son mutuamente excluyentes o apropiadas en todas las circunstancias, en las acciones inherentes para tratar el riesgo se pueden implicar una o más de las siguientes actividades: evitar el riesgo decidiendo no iniciar

o continuar con la actividad que genera el riesgo, aceptar o aumentar el riesgo en busca de una oportunidad, eliminar la fuente de riesgo, modificar la probabilidad, modificar las consecuencias, compartir el riesgo o retener el riesgo con base en una decisión informada.

La justificación para el tratamiento del riesgo es más amplia que las simples consideraciones económicas y debería considerar todas las obligaciones de la organización, los compromisos voluntarios y los puntos de vista de las partes interesadas, la selección de las opciones para tratar el riesgo debería realizarse según los objetivos de la organización, los criterios del riesgo y los recursos disponibles.

La información proporcionada por las acciones inherentes a la UNP permite reevaluar el riesgo y proporcionar una nueva medición denominada riesgo residual, que permite a la UNP establecer la base de la selección de las opciones para el tratamiento, incluyendo los beneficios esperados, las personas que rinden cuentas y las responsables de aprobar e implementar acciones residuales con las acciones propuestas, los recursos necesarios, incluyendo las contingencias, las medidas del desempeño, las restricciones, los informes y seguimiento requeridos y los plazos previstos para la realización.

Las decisiones tienen en cuenta un contexto más amplio y las consecuencias reales y percibidas por las partes interesadas externas e internas, las acciones listadas en la Tabla de Tratamiento, son las requeridas para dar cumplimiento al Tratamiento de riesgos de seguridad y privacidad de la información en la Entidad, donde se definen los riesgos inherentes y se comparan los controles propios de la UNP con los Controles propuestos por la ISO/IEC 27001:2022. estas actividades se encuentran descritas dentro del Instructivo del GTE-FT-36 Identificación y Valoración de Riesgos de Seguridad y Privacidad de la Información.

Tabla 3 Tratamiento

TRATAMIENTO							
ACCIONES INHERENTES (Control efectivo futuro a implementar)	CONTROLES EXISTENTES (Detalle Controles Propios del Proceso - UNP)	CONTROLES ISO/IEC 27001 (Detalle Controles SG-SI)	CONTROLES ISO/IEC 27001 (Comparativo Controles UNP - SG/SI)	PROBABILIDAD RESIDUAL ESCALA RARA VEZ = 1 IMPROBABLE = 2 POSIBLE = 3 PROBABLE = 4 CASI SEGURO = 5	IMPACTO RESIDUAL ESCALA INSIGNIFICANTE = 3 MENOR = 6 MODERADO = 9 MAYOR = 12 CATASTROFICO = 15	NIVEL RIESGO RESIDUAL EXTREMO ALTO MODERADO BAJO	ACCIONES RESIDUALES (Control efectivo futuro a implementar)
Divulgación de las políticas de seguridad al interior de la entidad: xx/xx/xxxx Cumplimiento de las políticas de seguridad de la información: xx/xx/xxxx			Autenticación Digital	0	0	BAJO	Divulgación de las políticas de seguridad al interior de la entidad: xx/xx/xxxx Cumplimiento de las políticas de seguridad de la información: xx/xx/xxxx

Fuente: Elaboración propia / GTE-GU-04 GIVRSPI

6.2.3.3 Monitoreo del Riesgo

El propósito del seguimiento y la revisión es asegurar y mejorar la calidad y la eficacia del diseño, la implementación y los resultados del proceso, en la UNP el seguimiento continuo y la revisión periódica del proceso de la gestión del riesgo y sus resultados debería ser una parte planificada del proceso de la gestión del riesgo, con responsabilidades claramente definidas.

El seguimiento y la revisión tienen lugar en todas etapas del proceso, el seguimiento y la revisión incluyen planificar, recopilar y analizar información, registrar resultados y proporcionar retroalimentación, los resultados del seguimiento y la revisión deberían incorporarse a todas las actividades de la gestión del desempeño, de medición y de informe de la organización.

Las decisiones tienen en cuenta un contexto más amplio y las consecuencias reales y percibidas por las partes interesadas externas e internas, las acciones listadas en la Tabla de Monitoreo, son las requeridas para dar cumplimiento al Monitoreo de riesgos de Seguridad y Privacidad de la Información en la Entidad, (La fórmula de medición puesta en la Tabla es una de las muchas formas de medir el riesgo en cada proceso), donde se definen las mediciones y el análisis de datos por las mediciones desarrolladas, cada dueño de riesgo tiene la oportunidad de medir sus riesgos de acuerdo a la naturaleza y complejidad de las actividades que tenga a cargo, estas actividades se encuentran descritas dentro del Instructivo del GTE-FT-36 Identificación, valoración y tratamiento de Riesgos de Seguridad y Privacidad de la Información; el Monitoreo se cumplirá siguiendo la función de la oficina de Control Interno teniendo en cuenta su rol de tercera línea de defensa, ya que es quién evalúa la eficacia de los controles que se definen en las matrices de riesgos del SG-SPI de los procesos de forma cuatrimestral.

MONITOREO					
CRONOGRAMA DE SEGUIMIENTO		INDICADOR DE EFECTIVIDAD Formula= (Numerador / Denominador)		PORCENTAJE DE AVANCE	DESCRIPCION DE LA ACCION EJECUTADA (Evidencias o Soporte)
FECHA INICIO (dd/mm/aaaa)	FECHA FIN (dd/mm/aaaa)	NUMERADOR: Numero Acciones Programadas	DENOMINADOR: Numero Acciones Ejecutadas		

Fuente: Elaboración propia / GTE-GU-04 GIVRSPI

7. INDICADOR

El indicador del plan es el seguimiento al cumplimiento de la eficacia de las actividades y se formula de la siguiente manera:

Indicador = ((Actividades ejecutadas durante el trimestre) / (actividades programadas durante el trimestre)) * 100

Se define meta de 85% anual del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para el periodo 2024.

La meta no es acumulativa, desglosándola trimestralmente de la siguiente manera:

Tabla 3. Ponderación y meta del indicador

TRIMESTRE	PONDERACIÓN ACTIVIDADES DEL TRIMESTRE	META MINIMA DE CUMPLIMIENTO DE ACTIVIDADES POR TRIMESTRE	META ANUAL
I TRIMESTRE	85%	85%	85%
II TRIMESTRE	85%	85%	
III TRIMESTRE	85%	85%	
IV TRIMESTRE	85%	85%	

Fuente: Elaboración Propia

El cumplimiento del Indicador se desarrolla de acuerdo con el contenido del Cronograma de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, anexo a este Documento.

8. DOCUMENTOS RELACIONADOS

- GDT-FT-23 Acta de Reunión
- GTE-GU-04 Guía Identificación y Valoración de Riesgos de Seguridad y Privacidad de la Información.
- GIN-MA-03 Manual Integral de Gestión de Riesgos.
- GTE-FT-36 Identificación, valoración y tratamiento de Riesgos de Seguridad y Privacidad de la Información.
- GTE-MA-02 Manual de Políticas de Seguridad y Privacidad de la Información.
- GTE-GU-05 Guía Identificación y valoración de Activos de Información.
- Anexo Declaración de Aplicabilidad SGSI – UNP 2023.

9. ANEXOS

- Cronograma del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

10. CONTROL DE CAMBIOS

VERSIÓN INICIAL	DESCRIPCIÓN DE LA CREACIÓN O CAMBIO DEL DOCUMENTO	FECHA	VERSIÓN FINAL
00	Creación del Plan de Tratamiento de riesgos de Seguridad y Privacidad de la Información	31/01/2019	01
01	Actualización del Plan de Tratamiento de riesgos de Seguridad y Privacidad de la Información para la vigencia 2020	31/01/2020	02
02	Actualización del Plan de Tratamiento de riesgos de Seguridad y Privacidad de la Información para la vigencia 2021	20/01/2021	03
03	Actualización del Plan de Tratamiento de riesgos de Seguridad y Privacidad de la Información para la vigencia 2022	20/01/2022	04
04	Actualización de las fechas propuestas en el cronograma de actividades del plan de Tratamiento de riesgos de Seguridad y Privacidad de la Información y desglose de la meta propuesta en el indicador, por valores acumulativos de porcentaje en cada uno de los semestres.	17/05/2022	05
05	Actualización del Plan de Tratamiento de riesgos de Seguridad y Privacidad de la Información para la vigencia 2024, se incluye el tratamiento de riesgos siguiendo la Guía de Gestión de Riesgos para Seguridad y Privacidad de la Información Guía No. 7 de Mintic, se inluyen las actividades completas de Gestión de Riesgos en sus cuatro parámetros: Identificación, Valoración, Tratamiento y Monitoreo de Riesgo, se agrega el Anexo: 2 ANEXO2-GTE-PL-03-Matriz de Riesgos de Seguridad y Privacidad de la Información.	30/01/2024	06
06	Actualización del Plan de Tratamiento de riesgos de Seguridad y Privacidad de la Información para la vigencia 2024, se incluye el tratamiento de riesgos siguiendo la Guía de Gestión de Riesgos para Seguridad y Privacidad de la Información Guía No. 7 de Mintic, guiadel Departamento Administrativo de la Función Pública DAFP V6, Anexo 4 Modelo Nacional de Gestión de Riesgos en Seguridad de la Información en Entidades Públicas y Gobierno Digital Seguridad y Privacidad de la Información se inluyen las actividades completas de Gestión de Riesgos en sus cuatro parámetros: Identificación, Valoración, Tratamiento y Monitoreo de Riesgo. Se cambia el tipo de meta de acumulativa a no acumulativa dejandola para los 4 periodos en 85%	21/03/2024	07

11. CRÉDITOS

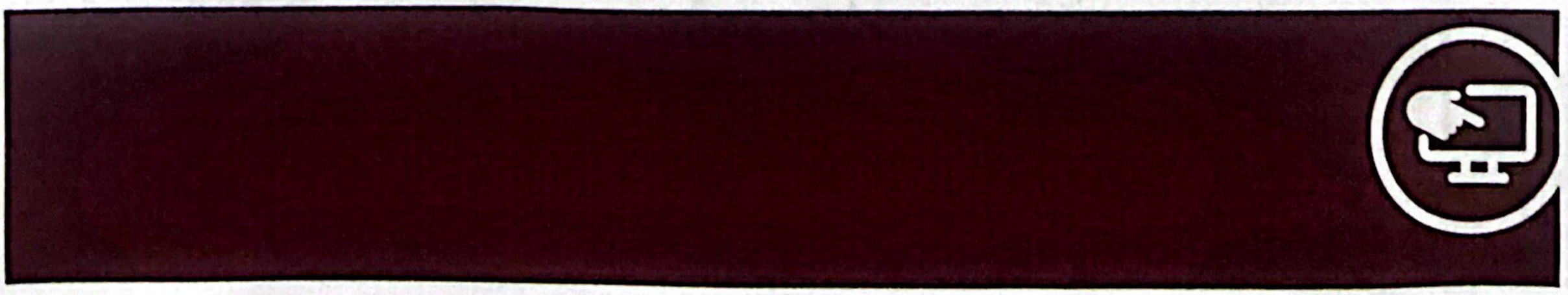
FIRMAS DE ELABORACIÓN, REVISIÓN Y APROBACIÓN DEL DOCUMENTO	
Elaboró Nombre: Javier Herrera Cargo y/o Vinculación/dependencia: Contratista-Oficial de Seguridad CISO - Proceso Gestión tecnológica / Oficina Asesora de Planeación e Información	
Revisó: Nombre: Maria Fernanda Reyes Sarmiento Cargo: Jefe de la Oficina Asesora de Planeación e Información	
Aprobó: Nombre: Augusto Rodríguez Ballesteros Cargo: director general	
FIRMA DE OFICIALIZACIÓN DEL DOCUMENTO- SISTEMA INTEGRADO DE GESTIÓN MIPG -SIG	
Oficializó: Nombre: Maria Fernanda Reyes Sarmiento Cargo: Jefe de la Oficina Asesora de Planeación e Información	

Anexos

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

Gestión Tecnológica
UNIDAD NACIONAL DE PROTECCIÓN
21-03-2024

COLOMBIA POTENCIA DE LA VIDA



Cronograma Plan de Tratamiento de Riegos de seguridad y privacidad de la Información 2024

Capítulo	Actividad	Producto	Responsable	Fecha de inicio	Fecha de cumplimiento	Seguimiento
Corresponden a los resultados de la Guía GTE-GU-04 Identificación y Valoración de Riesgos Seguridad y Privacidad de la Información						
Establecer el contexto	Planificación y preparación del plan 5 procesos iniciales	Análisis de Contexto con elementos de afectación a capacidad de cumplimiento	Jefe Oficina Asesora de Planeación e Información, Contratistas de Seguridad, Auditor SI	09/01/2024	29/03/2024	I trimestre de 2024
	Planificación y preparación del plan 13 procesos finales	Análisis de Contexto con elementos de afectación a capacidad de cumplimiento	Jefe Oficina Asesora de Planeación e Información, Contratistas de Seguridad, Auditor SI	01/04/2024	15/05/2024	II trimestre de 2024
Identificación de riesgos	Identificación de Activos de Información críticos 5 procesos iniciales	Lista de Activos de Información Identificados en cada proceso	Jefe Oficina Asesora de Planeación e Información, Contratistas de Seguridad, Auditor SI	09/02/2024	29/03/2024	I trimestre de 2024
	Identificación de Activos de Información críticos 13 procesos finales	Lista de Activos de Información Identificados en cada proceso	Jefe Oficina Asesora de Planeación e Información, Contratistas de Seguridad, Auditor SI	01/04/2024	15/05/2024	II trimestre de 2024
	Identificación de Riesgos 5 procesos iniciales	Riesgos SG-SPI Identificación de Riesgos	Jefe Oficina Asesora de Planeación e Información, Contratistas de Seguridad, Auditor SI	09/02/2024	29/03/2024	I trimestre de 2024
	Identificación de Riesgos y Oportunidades 13 procesos finales	Riesgos SG-SPI Identificación de Riesgos	Jefe Oficina Asesora de Planeación e Información, Contratistas de Seguridad, Auditor SI	01/04/2024	15/05/2024	II trimestre de 2024
Análisis de riesgos	Análisis y cálculo de nivel de riesgo 5 procesos iniciales	Riesgos SGSI - Niveles de Riesgo	Jefe Oficina Asesora de Planeación e Información, Contratistas de Seguridad, Auditor SI	09/01/2024	29/03/2024	I trimestre de 2024
	Análisis y cálculo de nivel de riesgo 13 procesos finales	Riesgos SGSI - Niveles de Riesgo	Jefe Oficina Asesora de Planeación e Información, Contratistas de Seguridad, Auditor SI	01/04/2024	15/05/2024	II trimestre de 2024
	Priorización de riesgos	Riesgos SGSI - Niveles de Riesgo	Jefe Oficina Asesora de Planeación e Información,	09/01/2024	29/03/2024	I trimestre de 2024

Capítulo	Actividad	Producto	Responsable	Fecha de inicio	Fecha de cumplimiento	Seguimiento
Corresponden a los resultados de la Guía GTE-GU-04 Identificación y Valoración de Riesgos Seguridad y Privacidad de la Información						
	5 procesos iniciales		Contratistas de Seguridad, Auditor SI			
	Priorización de riesgos 13 procesos finales	Riesgos SGSI - Niveles de Riesgo	Jefe Oficina Asesora de Planeación e Información, Contratistas de Seguridad, Auditor SI	01/04/2024	15/05/2024	II trimestre de 2024
Corresponden a los resultados del GTE-PL-03 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información						
Tratamiento de riesgos	Implementación de controles	Lista de Controles Implementados	Jefe Oficina Asesora de Planeación e Información, Contratistas de Seguridad, Auditor SI	16/08/2024	30/09/2024	III trimestre de 2024
	Desarrollo de estrategias de tratamiento	Plan de Tratamiento de Riesgos	Jefe Oficina Asesora de Planeación e Información, Contratistas de Seguridad, Auditor SI	01/07/2024	15/08/2024	III trimestre de 2024
Monitoreo y seguimiento	Monitoreo de cumplimiento de KPIs	Informes de Monitoreo	Jefe Oficina Asesora de Planeación e Información, Contratistas de Seguridad, Auditor SI	01/10/2024	15/11/2024	IV trimestre de 2024
	Revisión y actualización del plan	Plan de Tratamiento de Riesgos Actualizado	Jefe Oficina Asesora de Planeación e Información, Contratistas de Seguridad, Auditor SI	18/11/2024	04/12/2024	IV trimestre de 2024

Fuente: Elaboración Propia