



Plan

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GTE-PL-03-V6

Gestión Tecnológica
UNIDAD NACIONAL DE PROTECCIÓN
30-01-2024



Tabla de Contenido

1. OBJETIVO	3
2. ALCANCE	3
3. DEFINICIONES	3
4. MARCO LEGAL	6
5. CONDICIONES GENERALES	7
6. CONTENIDO	7
6.1 Estrategias	7
6.2 Gestión del Riesgo	8
6.2.1. Visión General la Gestión del Riesgo	8
6.2.3 Etapas para la Gestión del Riesgo	13
6.2.3.1 Identificación de Riesgos	13
6.2.3.1.1. Acciones para la Identificación de Riesgos	13
6.2.3.1.2 Análisis de Riesgos	14
6.2.3.2 Evaluación (Valoración del Riesgo)	14
6.2.3.3 Tratamiento del Riesgo	15
6.2.3.4 Monitoreo del Riesgo	16
7. INDICADOR	17
8. DOCUMENTOS RELACIONADOS	18
9. ANEXOS	18
10. CONTROL DE CAMBIOS	18
11. CRÉDITOS	19



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 de información que hacen parte del respectivo registro 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 riesgos de seguridad y privacidad de la información inicia con la identificación de los activos 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 seguimiento, monitoreo y evaluación enfocado al cumplimiento 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 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 2019: “Adoptar las guías del sistema de gestión de seguridad 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. Decreto 1078 de 2015 - Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- III. CONPES 3854 de 2016 - Política Nacional de Seguridad Digital
- IV. NTC / ISO 27001:2022 - Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
- V. NTC/ISO 31000:2018 - Gestión del Riesgo. Principios y directrices
- VI. NTC/ISO 27001:2006 – 27001:2013 Sistema de gestión de seguridad de la información reemplazarla por la versión 2022
- VII. NTC/ ISO 22301 DE 2012 sistemas de gestión de la continuidad del negocio reemplazarla por la versión 2019.
- VIII. NTC/ ISO 27002:2007-27002:2015 Seguridad de la información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información – reemplazarla por la última versión del año 2022



- IX. NTC/ISO 27002:2007-27005:2009 Tecnologías de la información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la información. Reemplazarla por la última versión del año 2022 Seguridad de la información, ciberseguridad y protección de la privacidad: directrices para la gestión de riesgos de seguridad de la información.
- X. NTC/ISO 10911:2018 Directrices para la auditoria de los Sistemas de Gestion/ Norma Tecnica Internacional.
- XI. NTC/ISO 31000:2018 ISO 31000 Gestión del Riesgo Principio y Directrices / Norma Tecnica Internacional.
- XII.
- XIII. Modelo de Seguridad y Privacidad de la Información V.3.0.2 – MPSI de la Estrategia de Gobierno en Línea – GEL hoy Gobierno Digital.
- XIV. Decreto 103 de 2015, Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
- XV. Decreto 1494 de 2015, Por el cual se corrigen yerros en la Ley 1712 de 2014
- XVI. Constitución Política de Colombia art 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar.
- XVII. Ley 527 de 1999, Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- XVIII. Decreto 2573 de 2014, Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
- XIX. Política de Seguridad de la Información de la Entidad.
- XX. Guía de Gestión de Riesgos para Seguridad y Privacidad de la Información Guía No. 7 de Mintic https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

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 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, enmarcado en el Sistema de Gestión de Seguridad de la Información – SGSI, 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, reduciendo la probabilidad de incidentes y cumpliendo los requisitos legales y reglamentarios, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información.

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

1. Compromiso: es importante que la alta gerencia para promueva, apoye y financie la realización de los proyectos asociados a la gestión 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 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

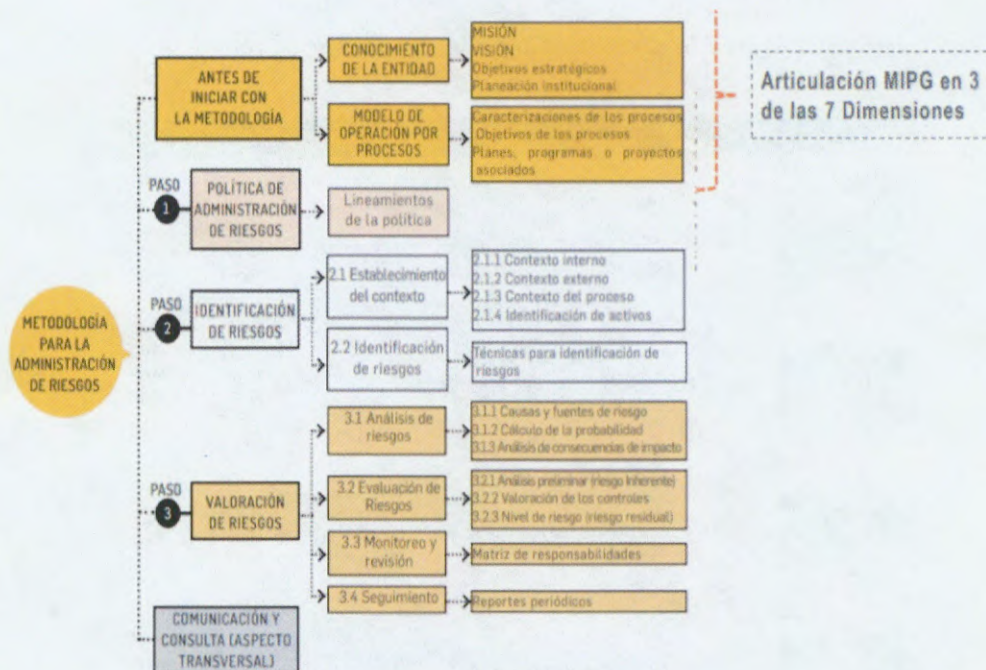
De acuerdo con la Guía de Gestión de Riesgos del DAFP – Departamento Administrativo de la Función Pública, las etapas generales para la gestión de riesgos adoptados por la UNP contemplan el compromiso de la dirección de la Entidad, el equipo interdisciplinario encargado de la administración del modelo 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

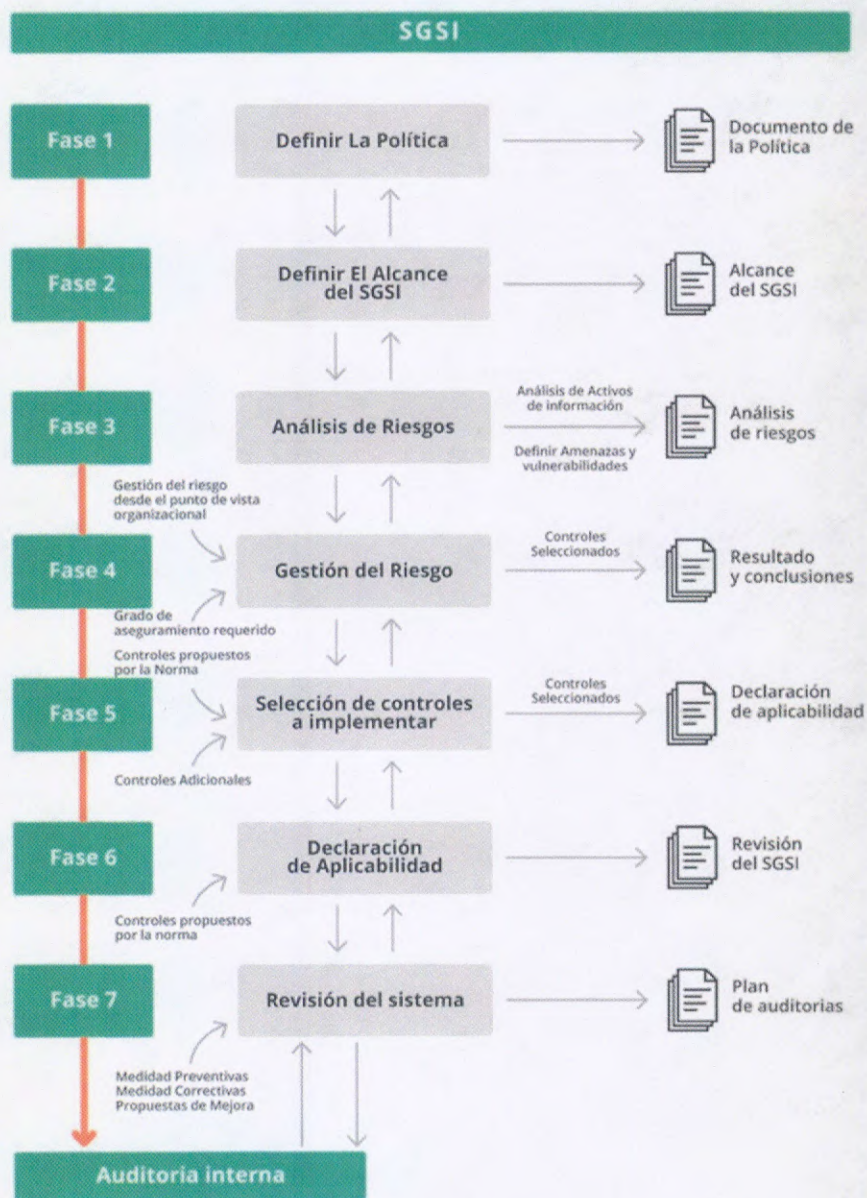


Fuente: DAFP (2020)



La Ilustración 2 indica el proceso para la implementación de un sistema de Gestión de Seguridad de la información.

Ilustración 2 Metodología para la Administración de Riesgos



Fuente: ISO 27001:2022



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:

1. Inicio del proyecto: Esta etapa implica la definición del alcance del SGSI, la identificación de los activos de información críticos, la identificación 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 riesgos de seguridad de la información para identificar las amenazas, vulnerabilidades y posibles impactos en los activos críticos de la organización. Se seleccionan las medidas de seguridad necesarias para mitigar los riesgos identificados.
3. Planificación: Se elabora un plan de gestión de seguridad de la información, donde se establecen los objetivos y metas del SGSI, 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 y se documentan los procesos y procedimientos necesarios.
5. Evaluación: Se lleva a cabo una evaluación continua del SGSI para verificar su eficacia, detectar posibles desviaciones y mejorar el desempeño.
6. Revisión por la dirección: La alta dirección revisa periódicamente el SGSI para asegurar su adecuación, idoneidad y eficacia en el contexto de la organización.
7. Mejora continua: Se toman acciones para mejorar continuamente el SGSI y su desempeño en la organización.

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

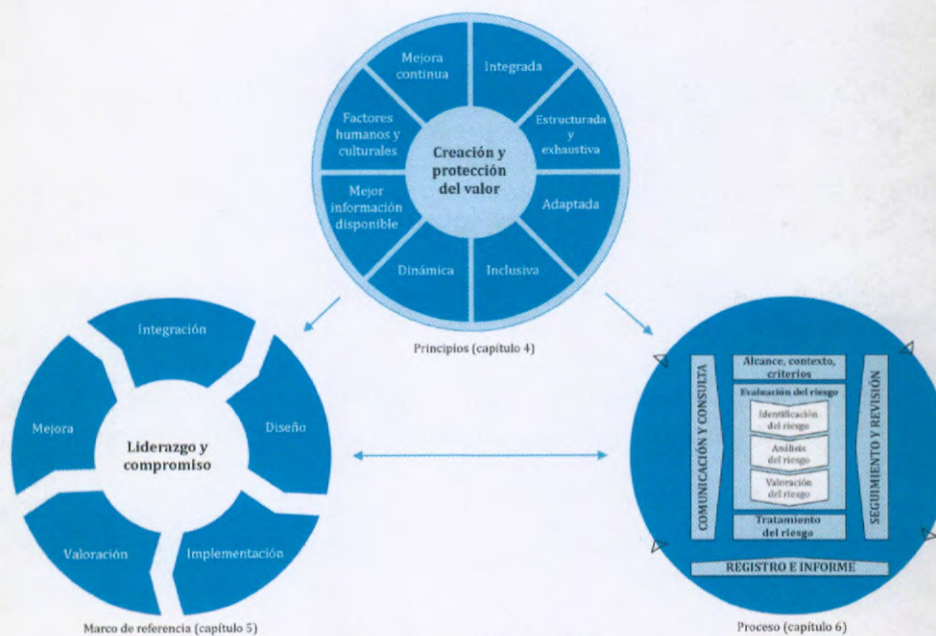


Deming. Esta metodología se aplica en cada una de las etapas mencionadas anteriormente para garantizar la efectividad del SGSI.

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 de Riesgos

De acuerdo con la Guía de Gestión de Riesgos para Seguridad y Privacidad de la Información Guía No. 7 de Mintic, la norma ISO 27001:2022 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 el Contexto, la caracterización de cada proceso y los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos en SI.

6.2.3.1.1. Acciones para la Identificación de Riesgos

Las acciones listadas en la Tabla 2, son las requeridas para dar cumplimiento a los objetivos de Gestión de riesgos de seguridad de la información en la Entidad, donde se definen metas, productos y responsables, consolidando el cronograma de ejecución de actividades.

Tabla 2. 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.	Integ.	Disp.	
	Tecnológico						

Fuente: Elaboración propia.

El propósito de la identificación del riesgo es encontrar, reconocer y describir los riesgos y oportunidades que pueden ayudar o impedir a una organización lograr sus objetivos, en la Identificación del riesgo y oportunidad se determina el Dueño del Riesgo, la afectación a los principios de SI y los Activos asociados al riesgo y oportunidad en análisis dentro de la UNP.

En la UNP se utiliza un rango de técnicas para identificar incertidumbres que pueden afectar a uno o varios objetivos, considerando factores como las fuentes de riesgo tangibles e intangibles, las causas y los eventos, las amenazas y las oportunidades, las vulnerabilidades



y las capacidades, los cambios en los contextos externo e interno, los indicadores de riesgos emergentes, la naturaleza y el valor de los activos y los recursos, las consecuencias y sus impactos en los objetivos, las limitaciones de conocimiento y la confiabilidad de la información, los factores relacionados con el tiempo y los sesgos, los supuestos y las creencias de las personas involucradas.

En la UNP se considera que puede haber más de un tipo de resultado, que puede dar lugar a una variedad de consecuencias tangibles o intangibles.

6.2.3.1.2 Análisis de Riesgos

El propósito del análisis del riesgo es comprender la naturaleza del riesgo y sus características incluyendo, cuando sea apropiado, el nivel del riesgo, el análisis del riesgo implica una consideración detallada de incertidumbres, fuentes de riesgo, consecuencias, probabilidades, eventos, escenarios, controles y su eficacia. Un evento puede tener múltiples causas y consecuencias y puede afectar a múltiples objetivos.

El análisis del riesgo se puede realizar con diferentes grados de detalle y complejidad, dependiendo del propósito del análisis, la disponibilidad y la confiabilidad de la información y los recursos disponibles.

Según las circunstancias y el uso previsto, las técnicas de análisis pueden ser cualitativas, cuantitativas o una combinación de estas, el análisis del riesgo debería considerar factores como: la probabilidad de los eventos y de las consecuencias, la naturaleza y la magnitud de las consecuencias, la complejidad y la interconexión, los relacionados con el tiempo y la volatilidad, la eficacia de los controles y los niveles de sensibilidad y confianza.

La identificación y análisis de riesgos se consignan dentro de la Tabla 2 Acciones Proceso de Gestión de Riesgos de Seguridad y Privacidad de la Información, en la Sección de "Identificación".

6.2.3.2 Evaluación (Valoración del Riesgo)

El propósito de la valoración del riesgo es apoyar a la toma de decisiones, la valoración del riesgo en la UNP implica comparar los resultados del análisis del riesgo con los criterios del riesgo establecidos para determinar cuándo se requiere una acción adicional. Esto puede conducir a una decisión de no hacer nada más, considerar opciones para el tratamiento del riesgo, realizar un análisis adicional para comprender mejor el riesgo, mantener los controles existentes o reconsiderar los objetivos.

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 2, son las requeridas para dar cumplimiento a la Evaluación 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

Tabla Evaluacion

EVALUACIÓN						
PROBABILIDAD ESCALA	IMPACTO ESCALA	EVALUACION RIESGO INHERENTE (PROBABILIDAD X IMPACTO)	NIVEL DE RIESGO INHERENTE (RIESGOS PROPIOS DEL PROceso O ACTIVIDAD)	CONTROLES ISO/IEC 27001 (DETALLE CONTROLES SI27001)	CONTROLES EXISTENTES (DETALLE CONTROLES SI-UNP)	CONTROLES ISO/IEC 27001 (DETALLE CONTROLES SI27001)
RARA = 1 IMPROBABLE = 2 POSIBLE = 3 PROBABLE = 4 CRISIS/SEGURO = 5	INCONSIDERABLE = 1 MENOR = 6 MODERADO = 9 MAYOR = 12 CATASTROFICO = 15					
3	12	36	ALTO			

Fuente: Elaboración propia.

6.2.3.3 Tratamiento del Riesgo

El propósito del tratamiento del riesgo es seleccionar e implementar opciones 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 Economía 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 2, 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.

Tabla Tratamiento

TRATAMIENTO					
OPCIÓN DE TRATAMIENTO (DETALLAR: ASUMIR / EVITAR / TRANSFERIR)	ACCIONES INHERENTES (CONTROL EFECTIVO FUTURO A IMPLEMENTAR) (DETALLAR PLAN DE ACCIÓN EN TÉRMINOS DEL CECI-PINA)	PROBABILIDAD ESCALA	IMPACTO ESCALA	NIVEL DE RIESGO RESIDUAL ESCALA	ACCIONES RESIDUALES (CONTROL EFECTIVO FUTURO A IMPLEMENTAR) (DETALLAR PLAN DE ACCIÓN EN TÉRMINOS DEL CECI-PINA)
		IMPOSIBLE = 1 POSIBLE = 2 PROBABLE = 3 CASI SEGURO = 4	PEQUEÑO = 1 MENOR = 2 MODERADO = 3 MAJOR = 4 GRANDE = 5	EXTREMO ALTO MODERADO BAJO	
Mitigar el Riesgo	Divulgación de las políticas de seguridad al interior de la entidad Cumplimiento de las políticas de seguridad de la información	3	12	36	Divulgación de las políticas de seguridad al interior de la entidad Cumplimiento de las políticas de seguridad de la información

Fuente: Elaboración propia.

6.2.3.4 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 2, son las requeridas para dar cumplimiento al Monitoreo 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.



Tabla Monitoreo

MONITOREO					
CRONOGRAMA DE SEGUIMIENTO		INDICADOR DE EFECTIVIDAD (DEFINIDO POR EL DUEÑO DEL RIESGO QUE DA CUENTA AL PLAN DE ACCIÓN EN EL CICLO PRIVA)		% AVANCE FORMULA= (NUMERADOR / DENOMINADOR)*100	DESCRIPCION DE LA ACCION EJECUTADA (EVIDENCIAS O SOPORTE)
FECHA INICIO (dd/mm/aaaa)	FECHA FIN (dd/mm/aaaa)	FORMULA= (NUMERADOR / DENOMINADOR) NUMERADOR = ACCIONES EJECUTADAS DENOMINADOR = ACCIONES PROGRAMADAS			
		NUMERO ACCIONES PROGRAMADAS	NUMERO ACCIONES EJECUTADAS		

7. INDICADOR

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

$$\text{Indicador} = ((\text{Actividades ejecutadas trimestral}) / (\text{actividades programadas trimestral})) * 100$$

Se define meta de 85% anual del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para el periodo 2023.

La meta es acumulativa, desglosándola trimestralmente de la siguiente manera:

Tabla 3. Ponderación y meta del indicador

TRIMESTRE	PONDERACIÓN DEL TRIMESTRE	META MINIMA DE CUMPLIMIENTO POR TRIMESTRE	META ANUAL
I TRIMESTRE	25%	20%	85%
II TRIMESTRE	25%	40%	
III TRIMESTRE	25%	60%	
IV TRIMESTRE	25%	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 de la Información

9. ANEXOS

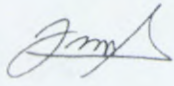
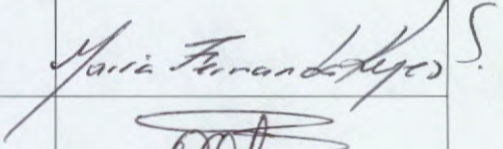
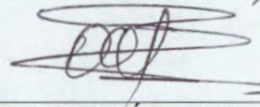
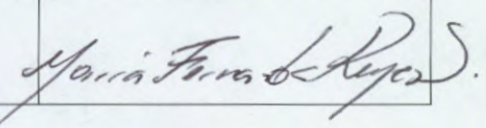
- Cronograma del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

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 incluyen 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



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
30-01-2024



Cronograma Plan de Tratamiento de Riesgos de seguridad y privacidad de la Información 2023

Capítulo	Actividad	Producto	Responsable	Fecha de inicio	Fecha de cumplimiento	Seguimiento
Establecer el contexto	Planificación y preparación del plan	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	09/02/2024	I trimestre de 2024
	Identificación de activos críticos	Lista de Activos Identificados	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	Identificación de Riesgos y Oportunidades	Riesgos SGSI - 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
	Evaluación de impacto y probabilidad	Riesgos SGSI - Valoración de Riesgos	Jefe Oficina Asesora de Planeación e Información, Contratistas de Seguridad, Auditor SI	09/02/2024	29/03/2024	I trimestre de 2024
Análisis de riesgos	Análisis y cálculo de nivel de riesgo	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, Contratistas de Seguridad, Auditor SI	16/05/2024	28/06/2024	II trimestre de 2024
Tratamiento de riesgos	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
	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
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

