UNP

Plan

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

GTE-PL-03-V8

Gestión Tecnológica
UNIDAD NACIONAL DE PROTECCIÓN
31-01-2025

Tabla de Contenido

1. OBJETIVO 3
2. ALCANCE 3
3. DEFINICIONES 3
4. MARCO LEGAL 5
5. CONDICIONES GENERALES 10
6. CONTENIDO 10
6.1. Estrategia *10*
6.2. Metodología *10*
7. META ESTABLECIDA 14
8. INDICADOR: 14
9. Hoja de Ruta Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (Cronograma) 14
10. DOCUMENTOS RELACIONADOS 16
11. CONTROL DE CAMBIOS 16
12. CRÉDITOS 17

1. OBJETIVO

Fortalecer, definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) protegiendo y preservando la integridad, confidencialidad, disponibilidad, privacidad y autenticidad de la información en la UNP.

2. ALCANCE

El plan de tratamiento de riesgos aplica a toda la Unidad Nacional de Protección UNP, se enfocará en la gestión de todos los riesgos de seguridad de la información, en especial los que se presenten en la zona de riesgo Extremo, Alto o Moderado, se aplicará un adecuado tratamiento y gestión de los riesgos. El plan inicia con la identificación y gestión de riesgos y se finaliza con la constante participación activa de todos los procesos para realizar un continuó y efectivo seguimiento y monitoreo correspondiente a la Política Integral de Administración de Riesgos de la UNP.

3. DEFINICIONES

TÉRMINO	DEFINICIÓN
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)

TÉRMINO	DEFINICIÓN
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. (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).
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).
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

TÉRMINO	DEFINICIÓN
	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).
Seguridad Informática	La seguridad informática es una rama de la seguridad que se dedica a proteger los sistemas informáticos de amenazas externas e internas. Las amenazas externas son aquellas que provienen del entorno exterior en el que se encuentra el sistema como, por ejemplo: ataques informáticos, virus, robos de información https://www.grupocibernos.com/blog/que-es-la-seguridad-informatica-y-como-implementarla
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

Norma	Año	Descripción
Ley 2162	2021	Por medio de la cual se crea el Ministerio de Ciencia, Tecnología e Innovación y se dictan otras disposiciones
Ley 2052	2020	"Por medio de la cual se establecen disposiciones transversales a la rama ejecutiva del nivel nacional y territorial y a los particulares que cumplan funciones públicas y/o administrativas, en relación con la racionalización de trámites y se dictan otras disposiciones"
Ley 1955	2019	Articulo 147 Los siguientes principios orientarán los proyectos estratégicos de transformación digital:
Ley 1978	2019	Ley de Modernización del sector TIC
Ley 1712	2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Ley 1581	2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1474	2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

Norma	Año	Descripción
Ley 1437	2011	Por la cual se expide el Código de procedimiento Administrativo y de lo contencioso Administrativo.
Ley 1286	2009	Por la cual se modifica la Ley 29 de 1990, se transforma a Colciencias en Departamento Administrativo, se fortalece el Sistema Nacional de Ciencia, Tecnología e Innovación en Colombia y se dictan otras disposiciones.
Ley 1273	2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".
Ley 1341	2009	Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
Ley 1266	2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en base de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 594	2000	Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
Ley 599	2000	Por la cual se expide el Código Penal. En esta se mantuvo la estructura del tipo penal de violación ilícita de comunicaciones", se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el "Acceso abusivo a un sistema informático".
Ley 527	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.
Ley 39	1981	Sobre microfilmación y certificación de archivos.
Decreto 767	2022	Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

Norma	Año	Descripción
Decreto 088	2022	Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los articulas 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea.
Decreto 338	2022	Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones
Decreto 620	2020	Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 Y 64 de la Ley 1437 de 2011, los literales e, j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales
Decreto 1064	2020	Por el cual se modifica la estructura del ministerio de Tecnologías de la información y las comunicaciones
Decreto 756	2019	Creación de la Corporación Agencia Nacional de Gobierno Digital (AND)
Decreto 2106	2019	Se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública. CAPÍTULO II. Transformación Digital para una gestión pública efectiva
Decreto 1008	2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital en reemplazo de la Política de Gobierno en Línea
Decreto 612	2018	Integración de los planes institucionales y estratégicos al Plan de Acción
Decreto 1499	2017	“Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015” (MIPG)
Decreto 1413	2017	Establece lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
Decreto 1499	2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015
Decreto 415	2016	Definición y establecimiento del CIO en el sector publico

Norma	Año	Descripción
Decreto 333	2014	Define el régimen de acreditación de las entidades de certificación, aplicable a personas jurídicas, públicas y privadas.
Decreto 2573	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.
Decreto 1078	2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1083	2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.
Decreto 1510	2013	Por el cual se reglamenta el Sistema de compras y contratación pública.
Decreto 2578	2012	Por el cual se reglamenta el Sistema Nacional de Archivos, se establece la Red Nacional de Archivos, se deroga el Decreto 4124 de 2004 y se dictan otras disposiciones relativas a la administración de los Archivos del Estado.
Decreto 235	2010	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas (Ley 2550 de 1995).
Decreto 4485	2009	Por medio de la cual se adopta la actualización de la Norma Técnica de Calidad en la Gestión Pública.
Decreto 1524	2002	Establecer las medidas técnicas y administrativas destinadas a prevenir el acceso a menores de edad a cualquier modalidad de información pornográfica contenida en Internet o en las distintas clases de redes informáticas a las cuales se tenga acceso mediante redes globales de información.
Decreto 2620	1993	Por medio del cual se reglamenta el procedimiento para la utilización de medios tecnológicos para conservar los archivos de los comerciantes.
Decreto 4065	2011	Por el cual se crea la Unidad Nacional de Protección (UNP), se establecen su objetivo y estructura.
Decreto 1066	2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector Administrativo del Interior
Resolución 500	2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital
Resolución 1519	2020	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
Resolución 0054	2024	Por medio de la cual se actualiza la Plataforma estratégica de la Unidad Nacional de Protección, UNP para periodo 2023 – 2026 y se deroga la resolución 0199 del 2 marzo de 2020

Norma	Año	Descripción
Resolución 0649	2024	Por medio de la cual se adopta la Política del Modelo Integrado de Planeación y Gestión. Sistema de Gestión de la Unidad Nacional de Protección
Resolución 1773	2024	Por medio de la cual se establece la Política Integral de Administración de Riesgos de la Unidad Nacional de Protección
Resolución 1774	2024	Por la cual se dictan lineamientos para la implementación del Modelo de seguridad y privacidad de la información de la Unidad Nacional de Protección, se actualiza la Política de Seguridad y Privacidad de la información y se deroga la Resolución 1847 de 2018
Resolución 1767	2024	Por la cual se organizas el Modelo Integrado de planeación y Gestión (MIPG-SIG) de la Unidad Nacional de Protección y se dictan otras disposiciones
Resolución 746	2022	Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No.500 de 2021.
Directiva Presidencial No. 02	2022	Directrices para garantizar la implementación segura de la Política de Gobierno Digital liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC
Directiva Presidencial No. 03	2021	Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos
Directiva Presidencial No. 02	2019	Simplificación de la interacción digital de los ciudadanos y el estado a través del portal único GOV.CO
Acuerdo 037	2002	Por el cual se establecen las especificaciones técnicas y los requisitos para la contratación de los servicios de depósitos, custodia, organización, reprografía y conservación de documentos de archivo en desarrollo de los artículos 13 y 14 y sus Parágrafos 1 y 3 de la ley General de Archivos 594 de 2000.
Acuerdo 047	2000	Por el cual se desarrolla el artículo 43 del capítulo V Acceso a los documentos de archivo", del Reglamento general de archivos sobre "Restricciones por razones de conservación".
Acuerdo 50	2000	Por el cual se desarrolla el artículo 64 del título VII conservación de documento", del Reglamento general de archivos sobre "Prevención de deterioro de los documentos de archivo y situaciones de riesgo".
Acuerdo 11	1996	Por el cual se establecen criterios de conservación y organización de documentos.
CONPES 3995	2020	Política Nacional de Confianza y Seguridad Digital Este documento CONPES, formula una política nacional que tiene como objetivo establecer medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital
CONPES 3975	2019	“Política nacional para la Transformación digital e inteligencia artificial”

Norma	Año	Descripción
CONPES 3920	2018	“Política nacional de explotación de datos (BIG DATA)”.
CONPES 3854	2017	Política nacional de seguridad digital
CONPES 3701	2011	Lineamientos de Política para Ciberseguridad y Ciber defensa.
CONPES 3670	2010	Lineamientos de Política para la continuidad de los programas de acceso y servicio universal a las Tecnologías de la Información y las Comunicaciones.
Norma Técnica ISO 27001	2022	Norma Técnica ISO 27001 de 2022 Norma técnica de Seguridad de la Información.

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. Estrategia

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 de la Información.

6.2. Metodología

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

6.2.1. Identificación de Riesgos:

La identificación de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Seguridad Informática de la Unidad Nacional de Protección – UNP, se fundamenta en la afectación a los activos de seguridad de la información identificados en cada proceso de la Entidad, la falta de apropiación en temas referentes a la seguridad y privacidad de la información o la ausencia y/o ineficacia de controles que puede ser aprovechada por

amenazas causando la materialización de riesgos, por lo que es preciso identificar los activos de seguridad de la información afectados, el impacto de la triada de los activos (Confidencialidad, Integridad, Disponibilidad), el dueño del riesgo, así como las causas o eventos asociados; para determinar los activos afectados, es necesario validarlos dentro del inventario de activos de seguridad de la información del proceso en donde en su valoración se estableció la criticidad a partir de la valoración del CID, la clasificación de la información y otros atributos importantes a tener en cuenta en la identificación de riesgos, estas actividades se encuentran descritas dentro de la Guía Identificación y Valoración de Riesgos de Seguridad y Privacidad de la Información GTE-GU-04 y el formato Identificación y Valoración de Riesgos de Seguridad y Privacidad de la Información GTE-FT-39.

6.2.2. Valoración del riesgo:

La valoración de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Seguridad Informática de la Unidad Nacional de Protección – UNP, se realizará de acuerdo con la metodología para la administración de riesgos mencionada en la Guía Identificación y valoración de Riesgos de Seguridad y Privacidad de la Información GTE-GU-04 implementada y aprobada en la Entidad.

Siguiendo esta metodología, en las diferentes mesas de trabajo que se desarrollan con los procesos se analizan aquellas cuestiones internas o externas que impactan directamente, la relación del activo critico valorado preliminarmente por medio de la metodología establecida, se identifican los riesgos teniendo en cuenta los activos críticos y se realiza la valoración teniendo en cuenta la probabilidad de ocurrencia e impacto como valoración preliminar para identificar el nivel del riesgo inherente, asociando las posibles causas que lo genera, vulnerabilidades y consecuencias potenciales en caso de una materialización.
Las tablas de valoración en cuanto a la probabilidad e impacto se encuentran descritas dentro de la Guía de identificación y valoración de riesgos de seguridad y privacidad de la información GTE-GU-04. Asi mismo, se encuentran definidos los niveles de riesgos inherentes resultantes de la valoración de probabilidad x impacto.

Es importante tener en cuenta que, al momento de realizar la valoración del activo de seguridad de la información de acuerdo con la triada del SGSI (Confidencialidad-Integridad y Disponibilidad), cada proceso identificará sus riesgos de seguridad de la información únicamente con aquellos activos que tienen un nivel de criticidad ALTO. Esto quiere decir, que son los activos a los que se le debe tener un mayor manejo debido a que son los que podrían ocasionar un impacto significativo en los procesos. Por lo tanto, al momento de estar en la fase de identificación, valoración, tratamiento y monitoreo de riesgos en el formato vigente, se visualizará el inventario de aquellos activos críticos (Nivel Alto) identificados.

6.2.3. 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 opciones 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 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.

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, y los responsables de aprobar e implementar acciones residuales con las actividades propuestas, con el fin de que estas se encuentren relacionadas con las causas que generan los posibles riesgos identificados, 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 residuales y se comparan las actividades de control propios de cada proceso con los Controles propuestos por el anexo A de la ISO/IEC 27001:2022 y verificar que no se ha omitido ningún control necesario, estos controles se encuentran establecidos de acuerdo con GTE-FT-46 Declaración Aplicabilidad-SOA identificada en la UNP.

6.2.3.1. Definición y aprobación de mapas de riesgos y planes de tratamiento:

Una vez concluidas las tres etapas anteriores y se obtenga la valoración residual de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Seguridad Informática de la Unidad Nacional de Protección – UNP, los responsables de proceso apoyados por los enlaces MIPG-SIG, deberán realizar a través del desarrollo de Memorando Interno la aprobación del Mapa de Riesgos con la aceptación del riesgo residual y la aprobación del plan de tratamiento de riesgos detallando las actividades requeridas que permitan mantener los niveles de riesgo residuales y madurar los controles establecidos en el Sistema de Gestión en Seguridad y Privacidad de la Información.

Es importante tener en cuenta que el proceso de aprobación de mapas de riesgos de seguridad de la información debe ser revisados y aprobados por cada responsable de proceso ante el Comité Institucional de Gestión y Desempeño-CIGD quien tiene la facultad de orientar y articular la implementación y operación del MIPG.

6.2.4. 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 de estos a todos los procesos de la entidad.

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.

6.2.4.1. Materialización de Riesgos SG-SPI:

Una vez terminado el monitoreo del riesgo y desarrollada la descripción de la acción ejecutada soportada con evidencias objetivas, en el caso de materializarse un riesgo, este debe ser reportado al Sistema de Gestión en Seguridad y Privacidad de la Información con la solicitud del desarrollo de acciones correctivas, siguiendo lo establecido en el Manual Integral de Gestión de Riesgos GIN-MA-03 y la Guía Directrices y GIN-PR-01 Procedimiento Gestión de Mejora, así mismo se deberá analizar el riesgo y validar en qué nivel queda posterior a la materialización registrando los cambios respectivos en el mapa de riesgos.

En caso de que se materialice un riesgo que no esté identificado, deberá ser reportado al Sistema de Gestión en Seguridad y Privacidad de la Información con la solicitud del desarrollo de la gestión del cambio en el Procedimiento Planificación y Gestión del Cambio GIN-PR-10.

6.2.4.2. Oportunidad de Mejora en el SG-SPI:

La Unidad Nacional de Protección – UNP no sólo deberá centrarse en los riesgos identificados sino que los análisis o apreciaciones del riesgo en sus cuatro etapas serán las bases para la identificación y desarrollo de oportunidades: la primera en el seguimiento del tratamiento de riesgos y la segunda por los resultados obtenidos en el monitoreo de riesgos, siguiendo lo establecido en el Manual Integral de Gestión de Riesgos GIN-MA-03 y la Guía Directrices, los Lineamientos para la Implementación de ACOM y Métodos de Análisis de Causas GIN-GU-02 y el Procedimiento Planificación y gestión del cambio GIN-PR-10, esto permitirá que los procesos alcancen un mejor desempeño y se contribuya a la maduración de los controles implementados en Seguridad y privacidad de la Información en la Entidad.

7. META ESTABLECIDA

La meta para el Plan Tratamiento de Riesgos de Seguridad y Privacidad de la Información será de 100% de cumplimiento para el periodo 2025.

8. INDICADOR:

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

Indicador = ((Fases ejecutadas durante el trimestre) / (fases programadas durante el trimestre)) * 100

Nombre del indicador	Objetivo	Fórmula	Meta Trimestral
Cumplimiento del Plan tratamiento de riesgos de seguridad y privacidad de la información	Medir el porcentaje de cumplimiento de las fases definidas en el Plan tratamiento de riesgos de seguridad y privacidad de la información	((Fases ejecutadas durante el trimestre) / (fases programadas durante el trimestre)) * 100	100%

La meta se desglosándola trimestralmente de la siguiente manera:

Tabla . Ponderación y meta del indicador

Trimestre	Ponderación fases del trimestre	Meta Anual
I Trimestre	25%	100%
II Trimestre	25%	
III Trimestre	25%	
IV Trimestre	25%	

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.

9. Hoja de Ruta Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (Cronograma)

PLAN DE TRATAMIENTO DE RIESGOS		PROGRAMACIÓN 2025											
Plan	**Fases**	**En**	**Feb**	**Mar**	**Abr**	**May**	**Jun**	**Jul**	**Ag**	**Sep**	**Oct**	**Nov**	**Dic**
Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Realizar una sensibilización de la Metodología de Identificación de Activos de Seguridad de la Información	**25%**											
	Identificación y valoración de los activos de Información, aplica a los 18 procesos												
	Actualización de la metodología de Gestión de Riesgos en el SGSI												
	Formalización de la metodología de Gestión de Riesgos en el SGSI				**25%**								
	Sensibilización a todos los procesos de la metodología e identificación matriz de riesgos para la identificación de los activos de seguridad de la información.												
	Informe de monitoreo SGSI vulnerabilidades												
	Actualizar un documento del SIG							**25%**					
	Realizar una mesa de trabajo para el manejo de los nuevos riesgos y activos de información												
	Actualización del formato de Matriz de Riesgos de Seguridad de la Información												
	Sensibilización a todos los procesos del formato de matriz de riesgos												
	Identificación, valoración y tratamiento de riesgo inherentes en la matriz de riesgo										**25%**		
	Revisión e identificación de los controles en la matriz de riesgos												
	Informe de monitoreo SGSI vulnerabilidades												
	Informe de resultados de Revisión por la Dirección												

10. DOCUMENTOS RELACIONADOS

- GIN-MA-03 Manual Integral de Gestión de Riesgos.
- GIN-PR-10 Procedimiento Planificación y gestión del cambio.
- GTE-GU-04 Guía Identificación y Valoración de Riesgos de Seguridad y Privacidad de la Información.
- GIN-GU-02 Lineamientos para la Implementación de ACOM y Métodos de Análisis de Causas.
- GTE-FT-39 Identificación, valoración y tratamiento de Riesgos de Seguridad y Privacidad de la Información.
- Resolución 1773 de 2024

11. 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	21/03/2024	07

VERSIÓN INICIAL	DESCRIPCIÓN DE LA CREACIÓN O CAMBIO DEL DOCUMENTO	FECHA	VERSIÓN FINAL
	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.		
07	Actualización del Plan de Tratamiento de riesgos de Seguridad y Privacidad de la Información para la vigencia 2025, se incluyen las actividades de Definición y aprobación de mapas de riesgos y planes de tratamiento, Oportunidad de Mejora en el SG-SPI, el uso del Procedimiento Planificación y gestión del cambio y la Guía Lineamientos para la Implementación de ACOM y Métodos de Análisis de Causas. Inclusión de la Hoja de Ruta Plan de Tratamiento de Seguridad y Privacidad de la Información	31/01/2025	08

12. CRÉDITOS

FIRMAS DE ELABORACIÓN, REVISIÓN Y APROBACIÓN DEL DOCUMENTO	
Elaboró Nombre: Elsa Marlen Baracaldo Huertas Cargo y/o Vinculación/dependencia: Contratista- Proceso Gestión tecnológica / Oficina Asesora de Planeación e Información	
Revisó: Nombre: John Anderson Hernandez Correa Cargo: Contratista Grupo de Gestión de las Tecnologías (GGT) – Oficina Asesora de Planeación e Información	
Revisó: Nombre: Maria Teresa Suescun Perdomo Cargo y/o Vinculación/dependencia: Contratista / Oficina Asesora de Planeación e Información	
Revisó: Nombre: Javier Francisco Rodríguez Moreno Cargo: jefe Oficina Asesora de Planeación e Información (E)	
Aprobó: Nombre: Miguel Ángel Quiroga Ruíz Cargo: Director General (E)	
FIRMA DE OFICIALIZACIÓN DEL DOCUMENTO- SISTEMA INTEGRADO DE GESTIÓN MIPG -SIG	
Oficializó: Nombre: Javier Francisco Rodríguez Moreno Cargo: jefe Oficina Asesora de Planeación e Información (E)	

ORIGINAL FIRMADO
UNIDAD NACIONAL DE PROTECCIÓN