Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Secretaría TIC, Innovación y Gobierno Abierto
Gobernación de Nariño

2026 | Versión 1

PROCESO ASOCIADO:	DEPENDENCIA ASOCIADA:
GESTIÓN DE TECNOLOGÍA	SECRETARIA TIC, INNOVACIÓN Y GOBIERNO ABIERTO

Tabla de contenido

Introducción 2
1. Objetivo 3
2. Alcance 3
3. Marcos 4
3.1. Marco conceptual 4
3.2. Marco normativo 5
4.1. Establecer el contexto 7
4.2. Identificación de riesgos 7
4.3. Valoración de riesgos 7
4.4. Definición del Plan de tratamiento. 7
4.5. Materialización 8
4.6. Oportunidad de mejora. 8
4.7. Medición 8
5. Matriz operativa del plan institucional. 9
6. Monitoreo y seguimiento. 11
7. Revisión, aprobación y verificación. 11

Introducción

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información constituye un componente esencial para salvaguardar la integridad, confidencialidad y disponibilidad de los activos de información de la Gobernación de Nariño. Este plan se creó con el propósito de planificar acciones específicas que minimicen la ocurrencia de riesgos o incidentes de seguridad, así como también la aplicación de controles para mitigar el impacto en la entidad en caso de que los riesgos se materialicen.

Su enfoque no solo se limita a la reacción ante incidentes, sino que busca desarrollar estrategias robustas para la identificación, análisis, tratamiento, evaluación y monitoreo de los riesgos de seguridad digital con una mayor objetividad.

En el contexto actual, Colombia enfrenta un incremento significativo de amenazas digitales que afectan tanto al sector público como al privado, tales como ataques de ransomware, phishing, ingeniería social, robo de información, accesos no autorizados, indisponibilidad de servicios y vulneraciones a datos personales. Estas amenazas se ven potenciadas por la creciente digitalización de los servicios públicos, el uso de plataformas en la nube, el trabajo remoto y la interconexión de sistemas, lo que exige para la Entidad fortalecer sus capacidades de prevención, detección y respuesta ante incidentes de seguridad y privacidad de la información.

Este plan hace parte integral del Modelo de Seguridad y Privacidad de la Información (MSPI) y busca reducir los riesgos a niveles aceptables para la entidad.

1. Objetivo

Identificar y gestionar los riesgos de seguridad digital sobre los activos de información de la Gobernación de Nariño, con el fin de minimizar y mitigar su materialización, asegurando el cumplimiento normativo, la continuidad de los servicios institucionales y la confianza de los ciudadanos.

2. Alcance

Aplica a todos los activos de información de gestión tecnológica identificados y valorados bajo responsabilidad de la Gobernación de Nariño, tanto en medios físicos como digitales, locales o en la nube.

3. Marcos

3.1. Marco conceptual

Activo de información: toda información, elementos, servicios o personas, relacionados con la producción o tratamiento de información, que tengan valor para la entidad, y por lo tanto se deben administrar y proteger.

Amenaza: causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Análisis de riesgos: utilización sistemática de la información disponible, para identificar amenazas y vulnerabilidades sobre activos de información.

Confidencialidad: propiedad que determina que la información no esté disponible ni sea revela-da a individuos, entidades o procesos no autorizados.

Control: acción que permite reducir o mitigar un riesgo.

Impacto: es el estado resultante después de la ocurrencia o materialización de un riesgo.

Indicadores: son métricas, unidades o mecanismos que permite evaluar el desempeño y ejecución de los procedimiento y controles de seguridad y privacidad de la información.

Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos.

Disponibilidad: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Minimizar la ocurrencia de riesgos: implementar medidas proactivas y controles para reducir tanto la probabilidad de que un evento negativo suceda como la magnitud de su impacto si ocurre, buscando que el riesgo sea manejable o aceptable, y no necesariamente eliminarlo por completo, lo que se logra mediante prevención y protección.

Mitigar riesgos: implementar acciones y estrategias para reducir la probabilidad de que ocurra un evento negativo o, si ocurre, disminuir significativamente su impacto en un proyecto, negocio o vida personal, sin necesariamente eliminarlo por completo, sino gestionándolo a niveles tolerables. Se trata de un proceso proactivo dentro de la gestión de riesgos, que busca minimizar pérdidas, contratiempos y daños.

Probabilidad: posibilidad de que ocurra o se materialice un riesgo.

Riesgo: es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o de los procesos. Se expresa en términos de probabilidad y consecuencias.

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 institucional y los intereses nacionales, incluye aspectos relacionados con el aspecto físico, digital y las personas.

Seguridad digital: preservación de la confidencialidad, integridad y disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.

Vulnerabilidad: representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

3.2. Marco normativo

En este marco se incluye la normatividad vigente y aplicable que está directamente relacionada con el plan institucional.

Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1712 de 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.
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1083 de 2015	Por medio del cual se expide el Decreto único Reglamentario del Sector de Función Pública, el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de Gobierno Digital, antes Gobierno en Línea y Seguridad Digital.
Decreto 612 de 2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
Decreto 767 de 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
Resolución 500 de	Por la cual se establecen los lineamientos y estándares

2021	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 de 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 746 de 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.
CONPES 3701 de 2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa.
CONPES 3854 de 2017	Política Nacional de Seguridad digital.
CONPES 3995 de 2020	Confianza y Seguridad Digital
CONPES 4069 de 2022	Política Nacional de Ciencia, tecnología e innovación 2022 – 2031.
Modelo de Seguridad y Privacidad de la información MSPI V5 de 2025 MinTIC	Documento Maestro del Modelo de Seguridad y Privacidad de la Información dirigida a las entidades del Estado
ISO/IEC 27001:2022	Estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información.
ISO/IEC 27005:2009	Gestión del riesgos de seguridad de información.

4. Descripción del desarrollo del plan

4.1. Establecer el contexto

La definición del contexto es una base para la identificación de los riesgos, este se encuentra definido en la matriz de identificación y valoración de Riesgos de Seguridad de la Información.

Contexto estratégico	
Factores externos	**Factores externos**
Económicos: disponibilidad de capital, emisión de deuda o no pago de la misma, liquidez, mercados financieros, desempeño, competencia.	**Económicos:** disponibilidad de capital, emisión de deuda o no pago de la misma, liquidez, mercados financieros, desempeño, competencia.
Medioambientales: emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.	**Medioambientales:** emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
Políticos: demografía, responsabilidad social, terrorismo.	**Políticos:** demografía, responsabilidad social, terrorismo.
Tecnológicos: interrupciones, comercio desarrollo, producción, mantenimiento electrónico, datos externos, tecnología emergente.	**Tecnológicos:** interrupciones, comercio desarrollo, producción, mantenimiento electrónico, datos externos, tecnología emergente.

4.2. Identificación de riesgos

Para la identificación de riesgos se realizó sesiones de trabajo con el personal de la Secretaría TIC, Innovación y Gobierno Abierto a cargo de los activos de la información y se establecieron los riesgos con base a los diferentes escenarios donde estos se podrían materializar.

4.3. Valoración de riesgos

Una vez identificados los riesgos se realizó la respectiva evaluación de cada uno, valorando la probabilidad y el impacto, obteniendo así su nivel de criticidad.

4.4. Definición del Plan de tratamiento.

Con los riesgos identificados y valorados en la Matriz de riesgos, se detallan controles existentes y se establecen controles de seguridad según los estándares establecidos en la Norma ISO 27001 y los recursos con los cuales cuenta la entidad.

Una vez definido el Plan de tratamiento con las acciones propuestas para minimizar y mitigar los riesgos, se socializa al personal de la Secretaría TIC, Innovación y Gobierno Abierto para definir procedimientos, responsables y tiempos de aplicación.

La identificación, valoración y controles de seguridad (plan de tratamiento de riesgos) se definen desarrollando la Matriz de Identificación y Valoración de Riesgos actualizada de MinTIC.

4.5. Materialización

Si se llegase a materializar un riesgo, este debe ser reportado a la Secretaría TIC, Innovación y Gobierno Abierto para su tratamiento según el Procedimiento de Gestión de incidentes de seguridad digital y el Plan de tratamiento de riesgos.

Cuando se materialice un riesgo que no esté identificado, de igual manera se le debe dar el tratamiento y posteriormente registrarlo en la matriz de riesgos para su valoración.

De igual manera debe ser reportado a COLCERT de MinTIC según el formulario establecido en la plataforma para tales fines.

4.6. Oportunidad de mejora

Cuando se hace la identificación de riesgos existe la probabilidad de encontrar oportunidades de mejora, estas se deben registrar de igual manera en la matriz. Por lo anterior la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

4.7. Medición

El monitoreo y seguimiento de los riesgos y controles de seguridad de la Información, se realizará por parte del profesional responsable en la Secretaria TIC, quien deberá asegurar la ejecución y documentar las evidencias de implementación, funcionamiento y efectividad de los controles.

El reporte de seguimiento a la ejecución de controles se debe medir con indicadores orientados a determinar el porcentaje de ejecución de los controles definidos para mitigar los riesgos identificados.

5. Matriz operativa del plan institucional.

La matriz operativa del presente plan institucional contiene varias actividades de gestión que permitirán cumplir con el objetivo general planteado anteriormente.

Actividad de gestión	Producto	Meta	Fecha límite mm/año	Soporte o evidencia	Responsable
Actualización de la Matriz de análisis, evaluación y valoración de riesgos sobre inventario de activos de información del proceso de Gestión de Tecnología (según ultima matriz de MinTIC).	Un proceso de Gestión de tecnología y sus activos de información actualizados en la matriz de análisis y evaluación de riesgos.	1	03/2026	Matriz de análisis y evaluación de riesgos actualizada.	Secretaría TIC, Innovación y Gobierno Abierto
Actualización y definición de controles sobre los riesgos identificados y valorados (norma ISO 27001:2022) en el proceso de Gestión de Tecnología.	Un plan de tratamiento de riesgos con la definición de controles específicos sobre los riesgos identificados y valorados.	1	05/2026	Matriz de plan de tratamiento de riesgos actualizada.	Secretaría TIC, Innovación y Gobierno Abierto
Socialización y aplicación de controles de seguridad establecidos en el Plan de tratamiento de Riesgos de Gestión de Tecnología.	Cinco o más controles de seguridad aplicados sobre los riesgos valorados.	5	12/2026	Soportes de aplicación de controles.	Secretaría TIC, Innovación y Gobierno Abierto
Monitorear los controles definidos y aplicados sobre el plan de tratamiento de riesgos de Gestión de Tecnología.	Un informe de seguimiento y monitoreo sobre el plan de tratamiento de riesgos de gestión de tecnología.	1	12/2026	Informe de seguimiento y monitoreo.	Secretaría TIC, Innovación y Gobierno Abierto

Actividad de gestión	Producto	Meta	Fecha límite mm/año	Soporte o evidencia	Responsable
Identificación de oportunidades de mejora acorde al seguimiento de la ejecución de los controles aplicados en el plan de tratamiento de riesgos.	Un plan de tratamiento de riesgos modificado según las oportunidades de mejora identificadas.	1	12/2026	Matriz de plan de tratamiento de riesgos actualizada Evidencias de aplicación de controles	Secretaría TIC, Innovación y Gobierno Abierto

6. Monitoreo y seguimiento.

El responsable de este plan es el secretario TIC, Innovación y Gobierno Abierto y su equipo de trabajo, quien deberá liderar la ejecución del mismo y articular esfuerzos con las demás dependencias para lograr el cumplimiento de las actividades aquí planteadas. Así mismo, de manera periódica realizará ejercicios de autocontrol con su equipo de trabajo para verificar el avance de las mismas, identificar alertas tempranas y garantizar la ejecución de las actividades de gestión.

Por su parte, la Secretaría de Planeación realizará monitoreo permanente al cumplimiento del presente plan para determinar el avance del mismo y socializar los resultados en el Comité Institucional de Gestión y Desempeño (CIGD). Cuando se requiera, brindará acompañamiento a la dependencia responsable del presente plan para que realice los ajustes que sean necesarios y se sometan a consideración del CIGD para su respectiva aprobación.

El seguimiento lo realizarán conjuntamente la Secretaría de Planeación y la Oficina de Control Interno de Gestión de manera semestral o en el momento en que se requiera.

7. Revisión, aprobación y verificación.

Revisión:	Aprobación:	Verificación:
Jonnathan Huertas	**Jonnathan Huertas**	**Armando Rosero García**
Secretario TIC, Innovación y Gobierno Abierto	Secretario TIC, Innovación y Gobierno Abierto	Secretario de Planeación