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

Secretaría TIC, Innovación y Gobierno Abierto
Gobernación de Nariño

2025 | Versión 1

Tabla de contenido

Introducción

El Plan de Tratamiento de Riesgos de Seguridad de la Información constituye un componente esencial en la salvaguarda de la integridad, confidencialidad y disponibilidad de los activos de información de la Entidad. Este plan se idea con el propósito de planificar acciones específicas que mitiguen 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 de la información con una mayor objetividad.

Este plan se rige en cumplimiento con las directrices establecidas por el Estado colombiano, como se refleja en normativas clave como CONPES 3995 de 2020, el Modelo de Seguridad y Privacidad de la información MSPI de MINTIC y regulaciones como el Decreto 1008 de 14 de junio de 2018, así como la Resolución 500 de 2021. Además, se alinea con estándares internacionales de seguridad, incluyendo ISO 27001 e ISO 31000:2018, adoptando buenas prácticas para la administración del riesgo y el diseño de controles en entidades públicas.

1. Objetivo

- Establecer los controles destinados a mitigar la materialización de los riesgos de seguridad de la información identificados sobre los activos de la infraestructura tecnológica de la entidad.
- Implementar estrategias para el tratamiento de riesgos y la implementación continua de mejoras en la seguridad y privacidad de la información.
- Lograr que las partes interesadas confíen de manera incrementada en el manejo de la información almacenada y gestionada por la Entidad

2. Alcance

Aplica para los riesgos de seguridad de la información identificados sobre la infraestructura tecnológica de la Entidad, valorados en los niveles de severidad Alto y Medio.

3. Marcos

3.1. Marco conceptual

En esta sección se presentan los principales conceptos relacionados con la temática que se abordan en el plan institucional.

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

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.

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

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 (Accountability), no repudio y fiabilidad.

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

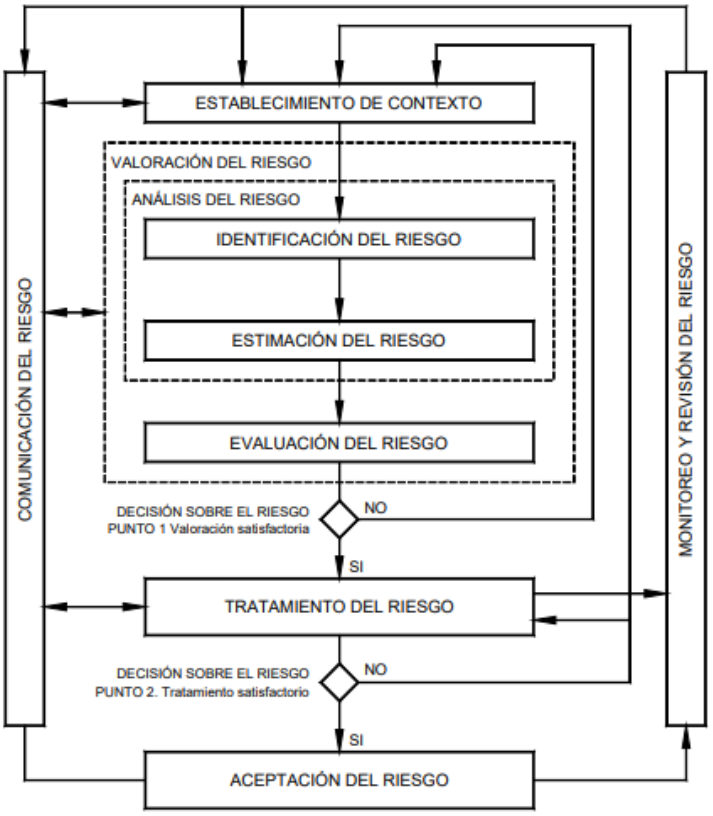
3.2. Marco normativo

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 1499 de 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 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.
ISO/IEC 27005:2009	Gestión de riesgos de seguridad de información.
Política de Administración de Riesgos de la Gobernación de Nariño.	
Metodología de Gestión de Riesgos de Seguridad de la Información	
Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6 DAFP.	

3.3. Marco referencial/antecedentes

Para elaborar el plan de tratamiento de riesgos de seguridad y privacidad de la información, se utilizó como referencia la “Metodología de Gestión del Riesgo de Seguridad de la Información Gobernación de Nariño”, el cual se basa en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6 y el Modelo nacional gestión riesgo seguridad información en entidades públicas.



4. 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, que se encuentra como Anexo.

CONTEXTO ESTRATÉGICO	
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.

5. Identificación de riesgos

Para la identificación de riesgos se realizó sesiones de trabajo con los profesionales de la Secretaría TIC a cargo de los activos de la información clasificados en los niveles críticos en el inventario y se establecieron los riesgos con base a los diferentes escenarios donde estos se podrían materializar.

6. 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.

7. Definición y aprobación de mapas de riesgos y planes 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 27001:2013 y definido el Plan de tratamiento con las acciones propuestas para la reducción de los riesgos se presenta para aprobación por el Secretario de la dependencia.

El plan de tratamiento de riesgos se encuentra definido de manera específica en el archivo en Excel Matriz de Identificación y Valoración de Riesgos - Plan tratamiento de riesgos - SGSI Gobernación de Nariño 2024.

8. Materialización

Si se llegase a materializar un riesgo, este debe ser reportado a la secretaría Tic para darle tratamiento y posterior a este se debe valorar nuevamente en la matriz 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.

9. 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.

10. Recursos

Los recursos disponibles en la entidad para la Gestión del riesgo es el siguiente:

Recursos	Descripción
Humanos	• Directivos: Comité Institucional de Gestión y Desempeño • Secretaria TIC, Innovación y Gobierno Abierto • Profesionales Universitarios • Técnicos Contratistas de apoyo
Técnicos	• Matriz de Riesgos del Sistema de Gestión de Seguridad y Privacidad de la información SGSI • Dispositivos de seguridad interna y perimetral firewall • Software Antivirus
Logísticos	• Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos. • Videos y piezas publicitarias para Plan de capacitación y sensibilización a personal de la entidad.
Financieros	• Presupuesto de recursos propios asignado para cada vigencia.

11. Presupuesto para la implementación de controles

La gestión y asignación de los recursos para la ejecución del plan de tratamiento de riesgos está a cargo del Secretario de la dependencia, quién deberá responsabilizarse del seguimiento a la implementación de las actividades de control definidas en el Plan.

12. Medición

El monitoreo y seguimiento de los riesgos de Seguridad de la Información, se realiza por parte del profesional Universitario delegado por el Secretario de la dependencia, 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. Estos se deben registrar en la matriz de riesgos en la sección de Plan de tratamiento de riesgos-seguimiento.

Matriz Plan de Tratamiento de Riesgos

PLAN DE TRATAMIENTO DE RIESGOS		RESPONSABLE	SEGUIMIENTO			
CONTROLES NORMA ISO 27001	ACCIONES O TAREAS		PERIODO	FECHA DE SEGUIMIENTO	INDICADORES	
A.11.2.2 SERVICIOS DE SUMINISTRO Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Adquirir gradualmente equipos, dispositivos, elementos de red y eléctricos redundantes.	Secretario TIC y Profesionales Universitarios de la secretaría TIC	Tirmestral		Eficacia	Número de equipos adquiridos
A.15.1.3 CADENA DE SUMINISTO DE TECNOLOGIA DE INFORMACION Y COMUNICACION: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	Gestionar oportunamente la contratación del servicio, teniendo en cuenta los procedimientos del Departamento de Contratación.	Secretario TIC y Profesionales Universitarios de la secretaría TIC	Tirmestral		Eficacia	Disminución del número de reportes de indisponibilidad de servicio por la no contratación oportuna
A.7.1.1 SELECCION: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.	Gestionar las necesidades de personal con el perfil y la experiencia necesaria para suplir las necesidades de soporte a nivel interno en la entidad.	Secretario TIC y Profesionales Universitarios de la secretaría TIC	Tirmestral		Efectividad	Disminución en el tiempo de respuesta para la recuperación del servicio
A.15.2.2 GESTION DE CAMBIOS EN LOS SERVICIOS DE LOS PROVEEDORES: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la revaluación de los riesgos.	Planificar de manera adecuada, oportuna y articulada con las áreas involucradas los cambios con los proveedores e infraestructura del proveedor	Secretario TIC y Profesionales Universitarios de la secretaría TIC	Tirmestral		Efectividad	Disminución del número de veces de indisponibilidad del servicio por fallo en las comunicaciones
A.12.3.1 RESPALDO DE LA INFORMACION: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	Realizar copias de seguridad a los correos corporativos de manera periódica y programada	Secretario TIC y Profesionales Universitarios de la secretaría TIC	Tirmestral		Eficacia	Número de copias de seguridad realizadas
A.9.2.6 RETIRO O AJUSTE DE LOS DERECHOS DE ACCESO : Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	Verificar de manera mensual los correos en desuso o asignados a personal retirado para su inactivación previa copia de seguridad.	Secretario TIC y Profesionales Universitarios de la secretaría TIC	Tirmestral		Eficacia	Número de correos depurados
A. 13.2.3 MENSAJERIA ELECTRONICA: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	Capacitar y sensibilizar a los usuarios sobre el uso correcto del correo electrónico.	Secretario TIC y Profesionales Universitarios de la secretaría TIC	Tirmestral		Efectividad	Cantidad de personal capacitado
A.15.1.3 CADENA DE SUMINISTO DE TECNOLOGIA DE INFORMACION Y COMUNICACION: Los acuerdos con	Gestionar oportunamente la contratación del servicio, teniendo en cuenta los procedimientos del Departamento de	Secretario TIC y Profesionales Universitarios de la secretaría				

VULNERABILIDADES | CONTEXTO | CLASIFICACIÓN DEL RIESGO | PROBABILIDAD | IMPACTO | VALORACIÓN DEL RIESGO | PLAN DE TRATAMIENTO

Anexo Matriz de Identificación y Plan de tratamiento de Riesgos

13. Documentos y registros relacionados

Matriz de Identificación y Valoración de Riesgos - Plan tratamiento de riesgos - Gobernación de Nariño 2024.

14. Anexos

Anexo 1. SG-SI-GTC-G-01 **G**uía Metodología de Gestión del riesgo de seguridad de la información gobernación de Nariño.

Anexo 2. Matriz de Identificación y Valoración de Riesgos - Plan tratamiento de riesgos.

15. 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.

La matriz se encuentra como anexo al presente documento, ya que contiene el formato establecido técnicamente que inicia desde el registro de los activos de información, identificación, análisis, valoración de riesgos y finalmente el plan de tratamiento que se constituye en los controles establecidos para minimizar y mitigar cada riesgo.

16. 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.

17. Revisión, aprobación y verificación.

Revisión:	Aprobación:	Verificación:
Jonnathan Huertas	Jonnathan Huertas	Lized López Erazo
Secretario TIC, Innovación y Gobierno Abierto	Secretario TIC, Innovación y Gobierno Abierto	Secretaria de Planeación