Política de seguridad digital

Secretaría TIC, Innovación y Gobierno Abierto
Gobernación de Nariño

2026 | Versión 1

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

Tabla de contenido

Introducción

La Política de Seguridad Digital representa el compromiso de la Gobernación de Nariño con la protección de los activos de información que manejan funcionarios, contratistas y terceros, en un entorno digital, que soportan los procesos de la entidad en el ejercicio de sus funciones misionales, y que apoya la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación de políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información en la entidad.

En el plan de trabajo de la política de seguridad digital se establecen lineamientos, procedimientos, responsabilidades y controles, dirigidos a que la entidad haga uso masivo, responsable, seguro y confiable de los activos de información en entorno digital, en todos sus ámbitos de aplicación, a través de la implementación y fortalecimiento de estrategias para identificar, gestionar y mitigar los riesgos asociados al uso de la tecnología y servicios digitales .

1. Objetivo

Definir lineamientos y estrategias para la gestión sistemática y cíclica de riesgos de seguridad digital, que permitan blindar el funcionamiento adecuado de los activos de información en un entorno digital, garantizando su disponibilidad, integridad y confidencialidad.

2. Alcance

El alcance del Plan de acción es proteger los activos de información de la Gobernación de Nariño en un entorno digital, minimizar los riesgos y asegurar la continuidad del servicio.

3. Marcos

3.1. Marco conceptual

Aceptación del Riesgo: decisión de aceptar un riesgo.

Activo: información o sistema relacionado con el tratamiento de la misma que tenga valor para la entidad y es necesaria para realizar los procesos misionales, estratégicos, operativos o de apoyo.

Alcance: ámbito de la entidad que queda sometido a la Política de Seguridad y Privacidad de la Información.

Alerta: una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

Amenaza: es la causa potencial de un incidente, el cual puede dar como resultado un daño a la entidad.

Análisis de riesgos: es el uso sistemático de la información para identificar fuentes y estimar el riesgo.

Antivirus: software de seguridad diseñado para detectar, prevenir y eliminar código malicioso o malware (virus, troyanos, ransomware, spyware) de computadoras y dispositivos móviles.

Aplicaciones: todo el software que se utiliza para la gestión de la información.

Auditor: persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

Auditoría: proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad de la Política de Seguridad y Privacidad de la Información.

Autenticación: proceso que tiene por objetivo validar la identificación de una entidad o sistema.

Autenticidad: los activos de información sólo pueden estar disponibles verificando la identidad de un sujeto o recurso, propiedad que garantiza que la identidad de un sujeto o recurso es la que manifiesta.

Estándar: regla que especifica una acción o respuesta que se debe seguir a una situación dada.

Ciberseguridad: conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio.

COLCERT: Grupo de Respuesta a Emergencias Cibernéticas de Colombia) es la entidad nacional líder, adscrita al MinTIC, encargada de coordinar la prevención, mitigación y respuesta a incidentes de seguridad digital.

Compromiso de la alta dirección: alineamiento firme de la Dirección de la entidad con el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora de la Política de Seguridad y Privacidad de la Información.

Confiabilidad: es la capacidad de un producto de realizar su función de la manera esperada.

Confidencialidad: es el Acceso a la información por parte únicamente de quienes estén autorizados.

Control: las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Control correctivo: control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

Datos: son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la entidad.

Firewall: sistema de seguridad, ya sea hardware o software, que monitoriza, filtra y controla el tráfico de red entrante y saliente, actuando como una barrera entre una red de confianza (como una red doméstica) y una red no confiable (como Internet) para prevenir accesos no autorizados y ciberamenazas

Gestión del riesgo: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Impacto: resultado de un incidente de seguridad de la información.

Incidente: evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones de la entidad y amenazar la seguridad de la información.

Información: es un activo, esencial para las actividades de una entidad.

Información pública reservada: información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos.

Información pública clasificada: es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley; Ley 1712/2014.

Información pública: es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal. Ley 1712/2014 que ha sido declarada legalmente o por su propietario, de conocimiento público y accesible a cualquier persona. Ej. Rendición de cuentas presentada por la entidad, Plan de acción de la Entidad, datos abiertos, entre otros.

Información semi – privada: es aquella que por versar sobre información personal o impersonal y no estar comprendida por la regla general anterior, presenta para su acceso y conocimiento un grado mínimo de limitación, de tal forma que la misma sólo puede ser obtenida y ofrecida por orden de autoridad administrativa en el cumplimiento de sus funciones o en el marco de los principios de la administración de datos personales.

Información privada: es aquella que por versar sobre información personal o no, y que, por encontrarse en un ámbito privado, sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones. Es el caso de los libros de los comerciantes, de los documentos privados, de las historias clínicas o de la información extraída a partir de la inspección del domicilio.

Instalaciones: son todos los lugares en los que se almacenan o utilizan los sistemas de información.

Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Inventario de activos: lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance de la Política de Seguridad y Privacidad de la Información, que tengan valor para la entidad y necesiten por tanto ser protegidos de potenciales riesgos.

IPS: sistema de prevención de intrusos.

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

ISO 19011: guía de utilidad para el desarrollo de las funciones de auditor interno para una Política de Seguridad y Privacidad de la Información.

ISO 27001: estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005.

ISO 27002: código de buenas prácticas en gestión de la seguridad de la información.

ISO IECTR 18044: guía de utilidad para la gestión de incidentes de seguridad de la información.

ITIL IT Infrastructure Library: un marco de gestión de los servicios de tecnologías de la información.

Legalidad: el principio de legalidad o Primacía de la ley, es un principio fundamental del Derecho público conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la ley de su jurisdicción y no a la voluntad de las personas.

Lista de chequeo: apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo.

Medida correctiva: medida de tipo reactivo orientada a eliminar la causa de una no conformidad asociada a la implementación y operación de la Política de Seguridad y Privacidad de la Información con el fin de prevenir su repetición.

Medida preventiva: medida de tipo proactivo orientada a prevenir potenciales no conformidades asociadas a la implementación y operación de la Política de Seguridad y Privacidad de la Información.

Mejor práctica: una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta.

MSPI: Modelo de seguridad y privacidad de la información.

No conformidad: situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

No repudio: los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.

Phishing: tipo de delito encuadrado dentro del ámbito de las estafas, que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

Plan de continuidad del negocio: plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos: documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política: declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

Política de escritorio limpio: política que indica a los funcionarios, contratista y demás colaboradores de la entidad, que deben dejar su escritorio libre de cualquier tipo de información que pueda ser usada para perjudicar a la entidad.

Política de seguridad: documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Procedimiento: definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos.

Responsabilidad: las múltiples partes interesadas deben asumir la responsabilidad de la gestión del riesgo de seguridad digital.

Riesgo: combinación de la probabilidad de un evento y sus consecuencias.

Riesgo inherente: es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

Riesgo residual: el riesgo que permanece tras el tratamiento del riesgo.

Segregación de tareas: separar tareas sensibles entre distintos funcionarios o contratistas para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

Selección de controles: proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

Seguridad digital: es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado.

Terceros: toda persona natural o jurídica que tenga una relación directa o indirecta con la entidad.

Tratamiento del riesgo: proceso para modificar el riesgo.

Usuario: directivos, funcionarios, contratistas, terceros y otros colaboradores de la entidad, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red y a quienes se les otorga un nombre de usuario y una clave de acceso.

Valoración de riesgos: proceso completo de análisis y evaluación de riesgos.

Virus: tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o conocimiento del usuario.

Vulnerabilidad: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

3.2. Marco normativo

Ley 1273 de 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 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.
Ley 1928 de 2018	Por medio de la cual se aprueba el «convenio sobre la ciberdelincuencia», adoptado el 23 de noviembre de 2001.
Ley 1978 de 2019	Por la cual se moderniza el Sector de las Tecnologías de la Información y las Comunicaciones -TIC, se distribuyen competencias, se crea un Regulador Único y se dictan otras disposiciones
Ley 2080 de 2021	Establece los lineamientos de uso de medios electrónicos en los procedimientos administrativos de las entidades públicas.
Decreto 1263 de 2012	Por el cual se adiciona el Título 22 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de definir lineamientos y estándares aplicables a la Transformación Digital Pública
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones. Derogado Parcialmente por el Decreto 1081 de 2015
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.
CONPES 3854 de 2016	Política Nacional de Seguridad Digital.
Norma Técnica Colombiana NTC ISO 27000:2013	Requisitos para la Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la información.

4. Descripción del desarrollo de la política

En materia de Seguridad Digital, el Documento CONPES 3854 de 2016 incorpora la Política Nacional de Seguridad Digital coordinada por la Presidencia de la República, para orientar y dar los lineamientos respectivos a las entidades.

Con la política se fortalecen las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, así como en la creación e implementación de instrumentos de resiliencia, recuperación y respuesta nacional en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país.

Ámbito de Aplicación: entidades que conforman la Administración Pública en los términos del Artículo 39 de la Ley 489 de 1998 y los particulares que cumplen funciones administrativas. La implementación de la Política de Gobierno Digital en las Ramas Legislativa y Judicial, en los órganos de control, en los autónomos e independientes y demás organismos del Estado, se realizará bajo un esquema de coordinación y colaboración armónica en aplicación de los principios señalados en los artículos 113 y 209 de la Constitución Política (Art. 2.2.9.1.1.2. - Decreto 1078 de 2015)

Lineamientos generales para la implementación: en el orden nacional, en los Comités Sectoriales de Gestión y Desempeño se darán las directrices para su implementación. Además, la articulación en materia de Seguridad Digital estará a cargo del enlace sectorial de seguridad digital quién será el encargado de rendir cuentas al Coordinador Nacional de Seguridad Digital acerca de la implementación de la Política Nacional de Seguridad Digital en el respectivo sector.

De otro lado, en el Comité Institucional de Gestión y Desempeño se deben articular los esfuerzos, recursos, metodologías y estrategias para asegurar la implementación de la política. Para ello, se debe designar un responsable de Seguridad Digital que también es el responsable de la Seguridad de la Información en la entidad, el cual debe pertenecer a un área transversal que haga parte de la Alta Dirección. Para las entidades cabeza de sector, el responsable de Seguridad Digital será el designado como enlace sectorial de seguridad digital.

En el orden territorial, MinTIC definirá los lineamientos para que las entidades territoriales definan la figura del enlace de Seguridad Digital territorial para la implementación de la política de Seguridad Digital, así como las instancias respectivas para la articulación con el Coordinador Nacional de Seguridad Digital.

Criterios diferenciales para la Política de Seguridad Digital: la implementación de la política, se hará a través de la adopción e implementación del Modelo de Gestión de Riesgos de Seguridad Digital, que será desarrollado y socializado por MinTIC, por parte de las entidades y departamentos administrativos de la rama ejecutiva inicialmente, para los entes territoriales y demás partes interesadas, se adelantarán jornadas de sensibilización en temas de Seguridad Digital. Adicionalmente, las entidades designadas, deberán dar cumplimiento a todas las actividades relacionadas en el plan de acción de seguimiento PAS del CONPES 3854 de 2016.

Análisis de resultados FURAG: los resultados del Formulario Único de Reporte de Avance en la Gestión – FURAG, de la política de seguridad digital para la Gobernación de Nariño, se evidencia una evolución significativa en el fortalecimiento de las capacidades institucionales para proteger los activos de información y garantizar entornos digitales seguros.

Histórico FURAG	2018	2019	2020	2021	2022	2023	2024
Seguridad digital	64,1	59,6	80,1	75,0	33,0	44,8	57,7

En 2018, la Gobernación de Nariño registró un puntaje de 64,1, lo que evidenciaba un nivel aceptable de implementación de prácticas relacionadas con la seguridad digital. Para 2019, el resultado disminuyó ligeramente a 59,6, lo cual puede interpretarse como un momento de ajuste en la adopción de los lineamientos del MIPG y en la consolidación de los procesos asociados a la gestión de la información.

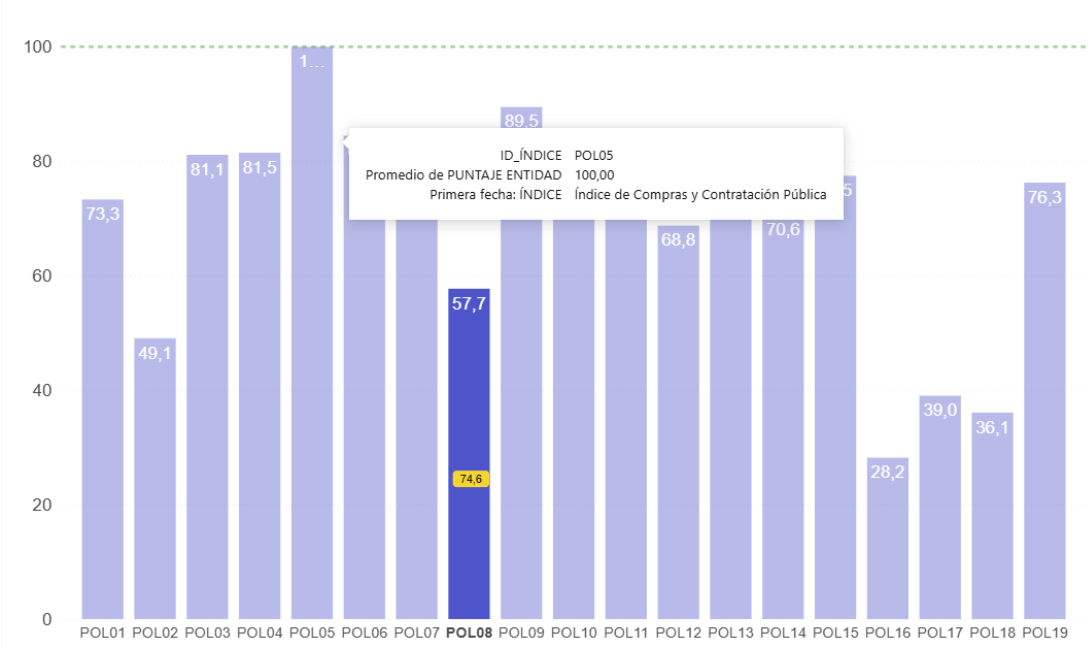
Posteriormente, en 2020, se observa un avance significativo al alcanzar un puntaje de 80,1, siendo este el resultado más alto del periodo analizado. Este incremento sugiere que durante ese año se fortalecieron las acciones institucionales orientadas a mejorar la gestión de la seguridad digital, en 2021, aunque el resultado disminuyó ligeramente a 75,0, la entidad mantuvo un desempeño favorable, lo que indica que los esfuerzos institucionales continuaban generando resultados positivos.

Sin embargo, en 2022 se presenta una disminución significativa en el puntaje, alcanzando 33,0, lo que refleja un escenario de mayor exigencia en la evaluación o la existencia de brechas en la implementación de algunos componentes de la política de seguridad digital. Este descenso puede estar relacionado con cambios en los criterios de medición del FURAG, el fortalecimiento de los estándares nacionales en materia de seguridad de la información.

A partir de 2023 se evidencia un proceso gradual de recuperación. Ese año la Gobernación de Nariño obtuvo un puntaje de 44,8, lo que indica que se empezaron a adelantar acciones orientadas a mejorar la implementación de la política. Para 2024, el resultado aumentó a 57,7, reflejando avances en el fortalecimiento de la gestión institucional en materia de seguridad digital, aunque aún existe margen para continuar mejorando y alcanzar nuevamente los niveles de desempeño registrados en años anteriores.

En este sentido, es importante fortalecer aspectos como la gestión integral de los riesgos de seguridad de la información, la actualización de políticas y procedimientos institucionales, la formación y sensibilización de los servidores públicos en buenas prácticas de seguridad digital y la implementación de mecanismos de monitoreo y respuesta ante posibles incidentes informáticos. Estas acciones contribuirán a consolidar una cultura institucional orientada a la protección de la información y al uso seguro de las tecnologías, elementos fundamentales para garantizar la confianza de la ciudadanía y la continuidad de los servicios digitales que presta la Gobernación de Nariño.

Análisis comparativo resultados de FURAG 2024 de la Gobernación de Nariño y el grupo par: teniendo en cuenta las siguientes graficas se generar un análisis de los resultados para la política de seguridad digital para la vigencia 2024.



La Gobernación de Nariño obtiene un puntaje global de 57,7, mientras que el grupo par alcanza un promedio de 74,6. Esta diferencia evidencia una brecha aproximada de 16,9 puntos, lo que indica que, aunque la entidad ha avanzado en la implementación de la política, aún existen aspectos estructurales y de gestión que deben fortalecerse para alcanzar niveles de desempeño similares a los de entidades con características comparables. Al analizar los componentes específicos de la política, se tiene la siguiente información:

1. **Despliegue de controles:** en este componente, la Gobernación de Nariño obtiene 89,3 puntos, mientras que el grupo par registra 86,6. Este resultado muestra que la entidad se encuentra ligeramente por encima del promedio de su grupo de referencia, lo que sugiere que existe una adecuada implementación de controles relacionados con la seguridad de la información, tales como mecanismos de protección de los sistemas, control de accesos, medidas de prevención frente a incidentes y acciones orientadas a salvaguardar los activos de información institucional. Este aspecto se configura como una fortaleza institucional, ya que demuestra avances en la adopción de prácticas operativas de seguridad digital.

2. **Implementación de lineamientos de política:** para este ítem la Gobernación obtiene 57,1 puntos, mientras que el grupo par alcanza 74,8, lo que representa una brecha significativa cercana a los 17,7 puntos. Esto evidencia que, si bien existen avances en la adopción de la política de seguridad digital, aún se requiere fortalecer la formalización, actualización y apropiación institucional de los lineamientos, así como su integración dentro de los procesos de planeación, gestión institucional y gobierno de tecnologías de la información.

3. **Asignación de recursos:** en este aspecto se observa la mayor brecha comparativa, ya que la Gobernación de Nariño presenta un resultado de 41,7 puntos, mientras que el grupo par alcanza 68,1, con una diferencia aproximada de 26,4 puntos. Este resultado sugiere que uno de los principales desafíos institucionales se relaciona con la disponibilidad y gestión de recursos humanos, técnicos y financieros destinados al fortalecimiento de la seguridad digital. La limitada asignación de recursos puede impactar la capacidad institucional para implementar plenamente los lineamientos de la política, desarrollar herramientas tecnológicas de protección, fortalecer la infraestructura digital y consolidar equipos especializados en seguridad de la información.

El análisis comparativo evidencia que la Gobernación de Nariño cuenta con avances importantes en la implementación de controles de seguridad digital, lo cual refleja esfuerzos operativos por proteger los activos de información institucional. Sin embargo, persisten brechas relevantes en aspectos estratégicos y de gestión, especialmente en la implementación integral de los lineamientos de la política y en la asignación de recursos, factores que resultan determinantes para consolidar un sistema robusto de seguridad digital.

A su vez, es necesario fortalecer la gobernanza de la seguridad digital, promoviendo una mayor articulación entre la planeación institucional, la gestión de tecnologías de la información y la asignación de recursos. Asimismo, se recomienda avanzar en la institucionalización de los lineamientos de seguridad de la información, fortalecer los procesos de gestión de riesgos digitales y promover la capacitación de los servidores públicos en buenas prácticas de seguridad digital. Estas acciones permitirán cerrar las brechas identificadas frente al grupo par y consolidar un entorno tecnológico más seguro y confiable para la administración departamental.

4.1. Plan de trabajo

El plan de trabajo de la presente política contiene varias actividades de gestión que permitirán cumplir con el objetivo general planteado anteriormente. Con el propósito de medir estas actividades se incluyen los respectivos productos y las metas que se programaron para la presente vigencia. Cada actividad tiene definida la fecha límite para su ejecución y la evidencia que soporta el cumplimiento de cada una. Así mismo, se relaciona el responsable quien liderará la articulación institucional que sea necesaria para lograr la ejecución satisfactoria de este plan de trabajo que se encuentra anexo a este documento.

5. Control de cambios.

Versión	Fecha de versión	Descripción del cambio	Responsable
01	23 de febrero de 2026	Creación del documento	

6. Responsable.

El responsable de este documento es el secretario TIC, Innovación y Gobierno Abierto, quien debe revisarlo, y si es necesario actualizarlo.

7. Revisión, aprobación y verificación.

(La revisión debe ser realizada por el jefe inmediato, la aprobación debe ser realizada por el líder del proceso).

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