Secretaría TIC, Innovación y Gobierno Abierto

Gobernación de Nariño

2025

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

TABLA DE CONTENIDO

3. Introducción.

La información es un elemento intangible que se produce, almacena, distribuye y procesa, constituye un activo fundamental para el buen funcionamiento y el progreso de la Gobernación de Nariño. En este sentido, la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) se convierte en una herramienta estratégica para proteger este activo invaluable.

El MSPI, a través de sus lineamientos de seguridad y privacidad, se debe integrar en todos los procesos, trámites, servicios, sistemas de información, infraestructura y activos de información de la Gobernación de Nariño. Su misión principal es asegurar la confidencialidad, integridad, disponibilidad y privacidad de la información, elementos clave para la toma de decisiones precisas, la transparencia y la eficiencia en la administración pública.

La Política de Seguridad y Privacidad de la Información refleja el compromiso institucional de la Gobernación de Nariño, respaldado por la Dirección, con la implementación de un Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI). Este sistema, de cumplimiento obligatorio para todos los empleados y contratistas, busca proteger integralmente los activos de información que han sido identificados y clasificados por la entidad

La Gobernación de Nariño, a través de la Política de seguridad y privacidad de la información reafirma su compromiso con la protección de los activos de información, reconociendo su importancia estratégica para el desarrollo y bienestar de la comunidad. La implementación exitosa de este modelo permitirá fortalecer una gestión pública moderna, eficiente, segura y transparente, al servicio de los ciudadanos.

4. Objetivo.

Establecer los lineamientos definidos por la Secretaría Tic, Innovación y Gobierno Abierto, teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información, las políticas de Seguridad Digital y Gobierno Digital y demás requisitos de ley y las necesidades de las partes interesadas, que permita proteger los activos de la información y asegure el correcto tratamiento de riesgos de la información identificados en la Gobernación de Nariño.

5. Alcance.

La política de seguridad y privacidad de la información es transversal y aplica a todos los procesos y servicios de la entidad, para todos los funcionarios, contratistas, proveedores, usuarios externos y demás partes interesadas, que en ejercicio de sus funciones o en uso de los servicios de la entidad creen, procesen, almacenen o compartan información.

6. 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.

- **Acuerdo de confidencialidad:** es el mecanismo mediante el cual regulamos los aspectos relativos a la seguridad de la información en una prestación de servicios, acorde a las funciones a desempeñar en la entidad.

- **Amenaza:** es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.

- **Autenticidad:** busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidad.

- **Backup de información:** se refiere a la copia y archivo de datos de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos.

- **Confidencialidad:** propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.

- **Datacenter:** se denomina también centro de procesamiento de datos (CPD) a aquella ubicación o espacio donde se concentran los recursos necesarios (TI) para el procesamiento de la información de una organización.

- **Dato personal:** cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

- **Dato personal privado:** es el dato que por su naturaleza íntima o reservada sólo es relevante para la persona titular del dato. Ejemplos: libros de los comerciantes, documentos privados, información extraída a partir de la inspección del domicilio.

- **Dato personal semiprivado:** es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato referente al cumplimiento e incumplimiento de las obligaciones financieras o los datos relativos a las relaciones con las entidades de la seguridad social, entre otros.

- **Dato público:** es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales, y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

- **Dato sensible:** se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

- **Declaración de aplicabilidad:** documento que describe los objetivos de control y los controles pertinentes y aplicables para el mismo.

- **Disponibilidad:** propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.

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

- **Custodio:** es una parte designada de la entidad, un cargo o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación de privilegios de acceso, modificación y borrado.

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

- **Incidente de seguridad de la información:** ocurrencia de uno o varios eventos que atentan contra la confidencialidad, la integridad y la disponibilidad de la información y que violan la Política de Seguridad de la Información de la organización.

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

- **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.

- **No repudio:** el emisor no puede negar que envió porque el destinatario tiene pruebas del envío. El receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor pueda negar tal envío.

- **Partes interesadas:** persona u organización que puede afectar o ser afectada o percibirse a sí misma como afectada por una decisión o actividad.

- **Plan de sensibilización:** es un proceso que involucra actividades, divulgación de información, estrategias audiovisuales y prácticas, para impactar a las partes interesadas sobre su comportamiento y/o reforzar en aplicación de buenas prácticas sobre seguridad de la información.

- **Política de seguridad de la información:** declaración de alto nivel que describe los objetivos y posición de la entidad frente a la Seguridad de la información.

- **Propietario / responsable de la información:** individual, entidad o dependencia que tienen bajo su responsabilidad la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.

- **Propietarios de infraestructura:** administradores de recursos tecnológicos utilizados para el manejo y/o administración de la información. Son responsables por la funcionalidad, operación, continuidad, manejo y uso de todos los sistemas compartidos, las redes, el soporte y el mantenimiento, el software estándar, los sistemas telefónicos y de comunicaciones, y los servicios relacionados.

- **Riesgo:** es la probabilidad que un incidente o evento adverso ocurra para causar una pérdida o daño en un activo de información.

- **Seguridad de la información:** conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información.

- **Sistema de gestión de seguridad de la información - SGSI:** conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

- **Terceros:** toda persona, jurídica o natural, como proveedores, contratistas o consultores, que provean servicios o productos a la Entidad.

- **Tratamiento de riesgos:** a partir del riesgo definido, se aplican los controles con los cuales se busca que el riesgo no se materialice.

- **Usuarios:** personas que, directa o indirectamente, tengan algún tipo de relación con la Entidad y/o que tengan acceso a los recursos tecnológicos de la Entidad.

- **Vulnerabilidad:** es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

Según la norma ISO 27001, la seguridad de la información consiste en la implementación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además abarcar otras propiedades, como la autenticidad, la responsabilidad y la fiabilidad.

La seguridad de la información es una pieza fundamental para que la empresa pueda llevar a cabo sus operaciones sin asumir demasiados riesgos, puesto que los datos que se manejan son esenciales para el devenir del negocio. Además, también hay que tener en cuenta que la seguridad de la información debe hacer frente a los riesgos**,** analizarlos, prevenirlos y encontrar soluciones rápidas para eliminarlos si se diera el caso.

Existen tres principios que debe respetar la gestión de la información en cualquier empresa para poder cumplir, de forma correcta, los criterios de eficiencia y eficacia. Como algo general, se entiende que mantener un sistema seguro y fiable, es garantizar tres aspectos: confidencialidad, integridad y disponibilidad.

CONFIDENCIALIDAD: se refiere a evitar que personas o programas no autorizados accedan a la información. Se debe restringir el acceso físico a los activos de información a través de mecanismos técnicos diseñados para tales fines.

INTEGRIDAD: hace referencia a la cualidad de la información para ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros. La integridad se pierde cuando la información se modifica o cuando parte de ella se elimina.

DISPONIBILIDAD: es la capacidad de acceder a la información cuando se necesita, a través de los canales adecuados siguiendo los procesos correctos.

La prevención de la pérdida de integridad de los datos proporciona disponibilidad, además de garantizar el funcionamiento adecuado de los activos tecnológicos que sirven para repositorios y procesamiento de datos.

MinTIC elaboró el Modelo de Seguridad y Privacidad de la Información – MSPI y define los lineamientos para la implementación de la estrategia de seguridad digital, con el objetivo de formalizar al interior de las entidades un sistema de gestión de seguridad de la información – SGSI y seguridad digital, el cual contempla su operación basado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento; el modelo consta de cinco (5) fases las cuales permiten que las entidades puedan gestionar y mantener adecuadamente la seguridad y privacidad de sus activos de información:

a. Diagnóstico: Se debe iniciar con un diagnóstico o un análisis GAP, cuyo objetivo es identificar el estado actual de la entidad respecto a la adopción del MSPI. Se recomienda usar este diagnóstico al iniciar el proceso de adopción, con el fin de que su resultado sea un insumo para la fase de planificación y luego al finalizar la Fase 4 de mejora continua.
b. Planificación: Determina las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta su mapa de procesos, el tamaño y en general su contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más importante del ciclo.
c. Operación: La entidad implementa los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.
d. Evaluación de desempeño: la entidad determina de qué manera va a ser evaluado la adopción del modelo.
e. Mejoramiento Continuo: se establecen procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición. Cada una de las fases se dará por completada, cuando se cumplan todos los requisitos definidos en cada una de ellas.

7. Marco normativo.

- Ley No 599 de 2000 - Código penal: Título VII BIS
- Ley Estatutaria 1266 De 2008
- La Ley 1273 de 2009
- Artículo 1 - Adicionase el Código Penal con un título VII bis
- Artículo 269a
  Artículo 269C
  Artículo 269D
  Articulo 269F
  Artículo 269H
- Ley Estatutaria 1581 De 2012
- Decreto 1377 de 2013
- 1581 de 2012
- Decreto 886 de 2014
- Decreto 1078 de 2015
- Decreto 1008 de 2018
- Decreto 1078 de 2015
- Documento CONPES 3854
- Documento CONPES 3975

La Gobernación de Nariño, consciente de la importancia de sus activos de información en el cumplimiento de su misión institucional, establece la presente política de Seguridad y Privacidad de la Información, orientada a garantizar la confidencialidad, integridad y disponibilidad de la información. Esta política se implementará mediante un Sistema de Gestión de Seguridad de la Información (SGSI) que proteja los activos informáticos, fortalezca la confianza en la relación con el Estado y los ciudadanos, y asegure el estricto cumplimiento de la normatividad vigente.

La Gobernación de Nariño en su propósito de dar cumplimiento con la política de seguridad y privacidad de la información, establece los siguientes objetivos:

a. Generar políticas específicas, procedimientos y lineamientos que apoyen la implementación de herramientas tecnológicas de prevención.
b. Propender por una cultura de concientización de seguridad de la información en todos los niveles de la entidad, a fin de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y disponibilidad de la información.
c. Asegurar la continuidad del servicio y minimizar el impacto causado por los riesgos identificados, logrando así mantener la confianza y responder frente a las necesidades de sus diferentes grupos de interés.
d. Cumplir con la normatividad vigente, el direccionamiento estratégico y la mejora continua, a través de la medición de la efectividad de los controles del Sistema de Gestión de Seguridad y Privacidad de la Información.
e. Salvaguardar la tecnología utilizada para el procesamiento de información frente a amenazas internas o externas, deliberadas o accidentales.

8.1. COMPROMISO DE LA ALTA DIRECCIÓN.

La Gobernación de Nariño se compromete a apoyar y liderar activamente la creación, ejecución, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI). Además, se compromete a realizar revisiones periódicas para evaluar el progreso de la implementación del SGSI. La Gobernación garantizará los recursos necesarios, tanto tecnológicos como humanos capacitados, para llevar a cabo la implementación y sostenimiento del sistema. Asimismo, integrará la seguridad de la información en la toma de decisiones estratégicas.

8.2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN - ROLES Y RESPONSABILIDADES.

La Gobernación de Nariño, define los roles y responsabilidades para la implementación del MSPI y el cumplimiento de los lineamientos de seguridad descritos en esta política y los demás documentos derivados.

ROL	RESPONSABILIDADES
Comité institucional de Gestión y Desempeño	● Aprobación y seguimiento de políticas, planes, programas, proyectos, estrategias y herramientas necesarias para la implementación y mejora continua del SGSI en la Gobernación de Nariño. ● Promover activamente una cultura de seguridad y privacidad de la información basada en riesgos, para la entidad. ● Aprobar los roles y responsabilidades relacionados con la seguridad de la información en todos los niveles de la entidad. ● Aprobar y adoptar decisiones que permitan la gestión y minimización de riesgos críticos de seguridad de la información. ● Las demás que tengan competencia en relación con el estudio, análisis y recomendaciones en materia de seguridad y privacidad de la información.
Responsable de Seguridad de la Información	● Liderar la planificación, implementación, despliegue y sostenibilidad del SGSI en la entidad. ● Proyectar y actualizar, promover y mantener la Política de Seguridad y Privacidad de la Información. ● Proyectar y actualizar periódicamente, la Política de Seguridad y Privacidad de la Información y Tratamiento de datos personales, y presentar para aprobación del comité de gestión y desempeño institucional. ● Socializar y promover el cumplimiento de las Políticas de Seguridad y Privacidad de la Información y Tratamiento de datos personales. ● Definir, elaborar e implementar las políticas específicas, planes, procedimientos, estándares y demás documentos relacionados con el SGSI. ● Realizar seguimiento a la implementación del SGSI y cronograma de ejecución, para gestionar la mejora continua del mismo.

	● Liderar la gestión de Riesgos de seguridad de la información, implementación de controles, y seguimiento al plan de tratamiento de riesgos. ● Liderar la formulación del plan de comunicaciones y sensibilización de seguridad y privacidad de la información, y su implementación en todas las dependencias de la entidad, usuarios externos y demás partes interesadas. ● Gestionar los recursos físicos, humanos y financieros, necesarios para la implementación y mejora continua del SGSI en la entidad. ● Definir, socializar e implementar los procedimientos de Gestión de Incidentes de seguridad de la información en la entidad. ● Seguimiento permanente a los incidentes de seguridad, y poner en conocimiento de las dependencias con competencia funcional cuando se detecten irregularidades o prácticas que atenten contra la seguridad y privacidad de la información de acuerdo con la normatividad vigente. ● Liderar el comité de seguridad de la información, para asegurar el liderazgo y cumplimiento de los roles y responsabilidades definidos en el SGSI. ● Atender las auditorías internas y externas en materia de seguridad de la información, y gestionar los planes de mejora producto de las mismas. ● Definir Indicadores de la Seguridad y Privacidad de la Información, y medición de cumplimiento periódico.
Equipo Estratégico de Seguridad y Privacidad de la Información	● Apoyar la implementación del SGSI en la Gobernación de Nariño, según el Modelo de Seguridad y privacidad de la Información de MinTIC y las normas vigentes relacionadas. ● Revisar los diagnósticos del estado de la seguridad de la información en la entidad. ● Acompañar e impulsar el desarrollo de proyectos de seguridad. ● Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la entidad. ● Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información. ● Aprobar el uso de metodologías y procesos específicos para la seguridad de la información. ● Participar en la formulación y evaluación de planes de

	acción para mitigar y/o eliminar riesgos. ● Realizar seguimiento periódico del SGSI (por lo menos una vez al año), y aplicar acciones pertinentes según los resultados obtenidos y la medición de indicadores de eficiencia y eficacia. ● Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad. ● Poner en conocimiento de la entidad, los documentos generados al interior del equipo de seguridad de la información que impacten de manera transversal a la misma. ● Las demás funciones inherentes a la naturaleza del equipo.
Equipo Operativo del Proyecto	● Apoyar al responsable del SGSI, en la proyección e implementación de las políticas, planes, proyectos y procedimientos de seguridad de la información y tratamiento de datos personales, según las actividades y responsabilidades asignadas. ● Apoyar en la adquisición de infraestructura (bienes y servicios) tecnológica para fortalecer la seguridad informática en la entidad. ● Implementar controles de seguridad de acuerdo al plan de tratamiento de riesgos y declaración de aplicabilidad. ● Operar la infraestructura de red, dispositivos de seguridad informática y sistemas de información, con las reglas y mecanismos necesarios para garantizar la confidencialidad, integridad y disponibilidad de los activos de información de la entidad. ● Gestionar los incidentes de seguridad y documentarlos para la construcción de la base de conocimientos, control y trazabilidad permanente. ● Participar en las reuniones y auditorías a las que sea designado por el responsable del SGSI, y gestionar la información y/o actividades que le sean asignadas. ● Oficiar como consultores de primer nivel en cuanto a las dudas técnicas y de procedimiento que se puedan suscitar en el desarrollo del proyecto. ● Garantizar y poder informar oportunamente el ejercicio de los derechos de los dueños de los datos personales identificados. ● Debe tramitar continuamente las consultas, solicitudes o reclamos, esto se define actualmente como atención de los PQR alineados a los datos personales.

	• Tener el compromiso de utilizar únicamente los datos personales que hayan sido obtenidos con autorización. • Siempre respetar y controlar las condiciones de privacidad y seguridad de la información del titular que interactúa con la Gobernación de Nariño. • Responder por el cumplimiento de las instrucciones y requerimientos impartidos por la autoridad legal o administrativa correspondiente.
Usuarios	• Conocer, aplicar y respetar las normas, procedimientos, manuales y buenas prácticas, definidos en las políticas de seguridad de la información y tratamiento de datos personales de la entidad del SGSI. • Mantener la confidencialidad, integridad y disponibilidad de la información, según las directrices impartidas por la Secretaría TIC y las restricciones de seguridad informática aplicadas en los activos de información. • Hacer buen uso de los activos de información de la entidad, para fines institucionales y según los permisos de acceso autorizados. • Participar activamente en la ejecución del plan de capacitación y sensibilización en seguridad de la información, adquirir los conocimientos y competencias necesarias para la protección, buen uso de los activos de información y minimizar la materialización de los riesgos. • Cumplir la legislación y regulación vigente en materia de Seguridad y Privacidad de la Información. • Notificar al responsable de seguridad y Soporte Técnico (Secretaría TIC) las anomalías o incidentes de seguridad, así como las situaciones sospechosas.

8.3. SANCIONES.

a. Cualquier violación a las políticas de seguridad de la información de la Gobernación de Nariño debe ser sancionada de acuerdo con los procedimientos disciplinarios establecidos en la entidad, a las normas, leyes y estatutos de la ley colombiana, así como la normativa atinente y supletoria, y apoyados en las leyes regulatorias de delitos informáticos de Colombia.

b. Las sanciones podrán variar dependiendo de la gravedad y consecuencias generadas de la falta cometida o de la intencionalidad de la misma.

8.4. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL SGSI.

La Gobernación de Nariño llevará a cabo revisiones periódicas del Sistema de Gestión de Seguridad de la Información (SGSI) para asegurar su eficacia y alineación con las directrices establecidas. Estas revisiones se enfocarán en evaluar indicadores clave del sistema, incluyendo el Índice Global de Incidentes, el porcentaje de gestión y vigilancia de incidentes, y otros indicadores que midan el cumplimiento de las mejores prácticas en seguridad de la información.

Además, se realizará un seguimiento continuo del avance en la implementación del Modelo de Seguridad y Privacidad de la Información del Ministerio TIC y la Política de Seguridad Digital, conforme a lo requerido por FURAG o cualquier herramienta designada para tal fin. El monitoreo de estos aspectos se apoyará en planes de seguridad y sensibilización, así como en la evaluación del desempeño y en el seguimiento de los planes de mejoramiento implementados.

8.5. DIRECTRICES ADQUISICION DE HERRAMIENTAS TIPO SOFTWARE.

La Gobernación de Nariño, como entidad pública comprometida con la protección de la información y la prestación de servicios digitales de calidad a la ciudadanía, establece en este documento las directrices que deben cumplir los proveedores de software de la entidad.

El cumplimiento de estos requisitos técnicos y de seguridad garantizará la continuidad operativa, la protección de los datos personales y el fortalecimiento de la infraestructura tecnológica de la Gobernación, estas directrices se encuentran alineadas con estándares internacionales como *ISO 27001, NIST 800-53, OWASP, y con las disposiciones del Ministerio de Tecnologías de la Información y las comunicaciones.

Los lineamientos propuestos se encuentran alineados con el Manual Operativo de Implementación de MIPG, específicamente con su política de Compras y Contratación Pública, además con la Guía de Buenas Practicas en la Adquisición de Software de la Agencia Nacional de Contratación Colombia Compra Eficiente.

8.5.1. Requisitos generales Adquisición de software

8.5.1.1. Requisitos de Calidad

Los proveedores deben garantizar la calidad de sus soluciones implementando procesos estructurados y metodologías reconocidas.

8.5.1.2. Metodologías de Desarrollo

- Uso de metodologías ágiles (Scrum, Kanban) o tradicionales (PMI, RUP).
- Cumplimiento de la *ISO 9001: Gestión de la Calidad*.
- Implementación de *controles de calidad automáticos* y *revisión manual del código fuente*.
- Documentación exhaustiva del ciclo de vida del software.

8.5.1.3. Gestión de Configuración y Cambios

Implementación de herramientas de gestión de versiones (Git, SVN).

- Documentación detallada de cada cambio para garantizar la trazabilidad.

8.5.1.4. Seguridad y Gestión de Vulnerabilidades

La seguridad es una prioridad para la Gobernación. Los proveedores deben garantizar la confidencialidad, integridad y disponibilidad de las soluciones suministradas.

Las pruebas de penetración son obligatorias y deben realizarse antes de la puesta en producción y periódicamente.
Las pruebas de seguridad deben:

- Cubrir las áreas de aplicación web, redes, infraestructura y servicios API.
- Los resultados deben ser documentados en informes detallados, incluyendo vulnerabilidades detectadas, nivel de criticidad y medidas de mitigación.
- Las vulnerabilidades de nivel crítico y alto riesgo deben corregirse antes del despliegue.
- Monitorización continua para identificar vulnerabilidades en bibliotecas y componentes de terceros.
- Aplicación inmediata de parches de seguridad para vulnerabilidades críticas.

8.5.1.5. Virtualización de Máquinas y Separación de Entornos

La virtualización es esencial para la Gobernación de Nariño por sus beneficios en términos de escalabilidad, seguridad y separación de entornos críticos.

Los requisitos de virtualización son:

- Uso de tecnologías de virtualización como *VMware ESXi, Microsoft Hyper-V, KVM* o soluciones de contenedores como *Docker y Kubernetes*.
- Implementación de políticas de alta disponibilidad (HA) y recuperación ante desastres (DR).
- Protección de entornos virtualizados mediante *firewalls internos, segmentación de red y herramientas de detección de intrusiones (IDS/IPS) *.
- Estricta separación de entornos de desarrollo, pruebas y producción para evitar la exposición de datos sensibles.
- Los entornos deben ser independientes y administrados bajo políticas de seguridad diferenciadas.
- Implementación de sistemas de monitoreo centralizados para detectar anomalías en el uso de recursos.
- Optimización constante del rendimiento de las máquinas virtuales para garantizar su estabilidad.

8.5.1.6. Auditorías y Evaluaciones Periódicas

La Gobernación de Nariño se reserva el derecho de realizar auditorías periódicas para verificar el cumplimiento de estos requisitos.

Los aspectos que se evaluaran son:

- Correcta ejecución de las pruebas de seguridad.
- Implementación de medidas de protección de datos.
- Gestión de vulnerabilidades y actualizaciones.

El incumplimiento puede dar lugar a la terminación del contrato, sanciones legales y la inclusión del proveedor en listas de riesgo del sector público.

8.6. ADMINISTRACIÓN DE CENTROS DE DATOS.

Los servicios externos que adquiera la Gobernación de Nariño, para alojamiento de sistemas de información, sedes electrónicas y demás aplicaciones que requieran de un centro de datos, estos deberán ser de categoría TIER 4, puesto que es la categoría más alta de clasificación de centros de datos según el Uptime Institute. Este tipo de centro de datos garantiza el mayor nivel de seguridad, redundancia y disponibilidad, cumpliendo las siguientes condiciones técnicas:

- ✓ Disponibilidad del 99.995%: Solo permite un tiempo de inactividad máximo de 26 minutos por año.
- ✓ Redundancia total (2N+1): Todos los componentes (energía, refrigeración, red, etc.) están duplicados, lo que asegura funcionamiento continuo incluso durante fallos o mantenimientos.
- ✓ Sistema de distribución dual: Los equipos están conectados a dos fuentes de energía completamente independientes y simultáneamente activas.
- ✓ Tolerancia a fallos: El diseño permite continuar operando sin interrupciones, incluso en caso de fallo catastrófico.
- ✓ Seguridad física: Nivel alto de seguridad para evitar accesos no autorizados.

Estas directrices están alineadas con las políticas del MIPG (Modelo Integrado de Planeación y Gestión) de Gobierno Digital y Seguridad Digital.

9. Control de cambios.

Versión	Fecha versión	Descripción del Cambio	Responsable
01	23/08/2023	Creación del documento	
02	30/08/2024	Actualización	Secretaría TIC, Innovación y Gobierno Abierto
03	15/12/2025	Se adiciona los ítems 8.5.Directrices adquisición de herramientas tipo software, 8.6.Administración de centros de datos.	Jonnathan Huertas Salas

10. Responsable.

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

11. Revisión, Aprobación y Verificación.

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