SECRETARÍA TIC, INNOVACIÓN Y GOBIERNO ABIERTO

2025

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

Tabla de contenido

3. INTRODUCCIÓN.

La seguridad de la información es fundamental para la protección de los activos de la entidad y para asegurar la confianza de los usuarios internos y externos. Las relaciones con los proveedores juegan un papel trascendental en el ecosistema de seguridad, ciberseguridad y protección de la privacidad, ya que estos pueden tener acceso a activos de información, datos sensibles y sistemas críticos.

La Política de seguridad de la información en la relación con proveedores establece las directrices y controles para gestionar de forma segura, eficaz y conforme al marco normativo, las relaciones conformadas entre la Gobernación de Nariño y sus terceros o proveedores interno y externos, en cuanto al acceso a los activos de información (software, servicios tecnológicos, telecomunicaciones, archivos digitales, bases de datos, equipos informáticos, correo electrónico institucional, etc.) para el ejercicio de sus funciones, obligaciones, actividades contractuales, y cualquier tipo de interacción con entidad relacionada con los objetivos y misión institucional.

4. OBJETIVO.

Determinar los lineamientos necesarios para garantizar la protección de los activos de información que se encuentran al acceso de los proveedores de la Gobernación de Nariño, contra amenazas y vulnerabilidades que puedan afectar los principios de integridad, disponibilidad y confidencialidad de la información.

5. ALCANCE.

La Política de Seguridad en la relación con los Proveedores aplica a todas las dependencias de la Gobernación de Nariño, y a todos sus terceros y/o proveedores (funcionarios y contratistas) que, para la ejecución de sus funciones o ejecución de sus obligaciones contractuales, tengan acceso a los activos de información de la entidad, en su operación, procesamiento, almacenamiento, eliminación, recepción, transmisión y publicación.

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:** documento contractual mediante el cual una o ambas partes se comprometen a proteger y no divulgar información sensible o confidencial a la que tengan acceso durante la relación contractual, asegurando su uso exclusivo para los fines establecidos y previniendo accesos no autorizados, conforme a los requisitos legales, normativos y de seguridad de la organización.

- **Acuerdo de nivel de servicio (SLA)(ANS):** es un contrato formal entre un proveedor de servicios y una entidad, que define claramente qué servicios se prestarán, cómo se medirán (tiempo de actividad, respuesta, resolución), los horarios, responsabilidades y las

consecuencias (sanciones/compensaciones) si no se cumplen los objetivos de rendimiento acordados, asegurando expectativas claras y calidad del servicio.

- **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.

- **Ciberseguridad:** se entiende como la capacidad de una entidad para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética, buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio de las interacciones digitales.

- **Confidencialidad:** propiedad de la información que pretende garantizar que esta sólo es accedida por personas o sistemas autorizados.

- **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.

- **Correo electrónico institucional:** es el servicio de correo que le asigna la entidad a cada colaborador para que lo utilice en el desarrollo de sus funciones.

- **Dato:** es una representación simbólica (numérica, alfabética, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.

- **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.

- **Datos sensibles:** información que requiere protección adicional debido a su naturaleza confidencial, como datos personales, financieros o estratégicos.

- **Disponibilidad:** propiedad de la información que pretende garantizar el acceso y uso de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

- **Información:** conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

- **Integridad:** propiedad de la información que pretende mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

- **Protección de datos personales:** conjunto de técnicas jurídicas e informáticas encaminadas a garantizar los derechos de las personas sobre el control de su información personal y sobre la confidencialidad, integridad y disponibilidad de esta.

- **Proveedor:** terceros que suministran bienes o servicios a una organización, incluyendo los que ofrecen servicios especializados de ciberseguridad para proteger los activos de información frente a amenazas y riesgos.

- **Riesgo:** posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

- **Seguridad digital:** es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante, incluye la seguridad de la información (Políticas, Procedimientos y demás controles) y la seguridad informática (Herramientas de seguridad).

- **Transferencia de información:** proceso mediante el cual la información es enviada, recibida o compartida entre personas, áreas, sistemas o terceros, utilizando medios electrónicos o físicos. Debe realizarse cumpliendo controles que aseguren la confidencialidad, integridad y disponibilidad de la información transferida, conforme a su

clasificación y a las políticas organizacionales.

- **Usuario:** cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información, para propósitos propios de su labor.

- **Vulnerabilidad:** es una debilidad de un activo informático, o sistema de información que puede ser explotada por una o más amenazas 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.

7. MARCO NORMATIVO

- Ley 1266 de 2008
- La Ley 1273 de 2009
- Ley 1581 de 2012
- Decreto 1078 de 2015
- Decreto 1377 de 2013
- CONPES 3995 de 2020
- Decreto 620 de 2020
- Modelo de Seguridad y Privacidad de la Información (MSPI) – MinTIC.
- Norma ISO/IEC 27001:2013.
  Dominio A.15 Relaciones con los proveedores
- Manual de seguridad y privacidad de la información – MinTIC - Estrategia de Gobierno Digital.

8. DESCRIPCIÓN DEL DESARROLLO DE LA POLÍTICA

8.1. ROLES Y RESPONSABILIDADES

ROL	RESPONSABILIDADES
Responsable de Seguridad de la Información Secretaría TIC, Innovación y Gobierno Abierto	Liderar la planificación, implementación, despliegue y sostenibilidad del Sistema se seguridad de información en la entidad. Proyectar y actualizar, promover y mantener la Política de Seguridad y Privacidad de la Información. Socializar y promover el cumplimiento de la Política específica de seguridad en la relación con proveedores y Tratamiento de datos personales. Definir, elaborar e implementar las políticas específicas, planes, procedimientos, estándares y demás documentos relacionados con el Sistema se seguridad de información en la entidad. 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 Sistema de seguridad de la información en la entidad. Definir, socializar e implementar los procedimientos de Gestión de Incidentes de seguridad de la información en la entidad. 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 Operativo de seguridad	Apoyar al responsable del Sistema de seguridad de la información, 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. Tramitar continuamente las consultas, solicitudes o reclamos, alineados a los datos personales. Apoyar la implementación del plan de tratamiento de datos personales.
Subsecretaría de Talento Humano	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. Adoptar la suscripción del Formato de Acuerdo de confidencialidad y Protección de datos personales, como requisito para la vinculación de personal en cualquier tipo de vinculación. El mismo será ingresado a la hoja de vida del personal con los documentos de posesión.
Unidades de Contratación (Dirección Administrativa de Contratación DAC, Secretaría de Educación SED, Unidad especial Junín Barbacoas)	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. Adoptar la suscripción del Formato de Acuerdo de confidencialidad y Protección de datos personales, como requisito para la presentación de ofertas en procesos de contratación y para la suscripción de contratos. El mismo será cargado en SECOP II con los documentos de legalización del contrato. Implementar cláusula de Seguridad y Privacidad de la Información en el Anexo contractual, que sea firmado por el proveedor y la entidad. Implementar en los formatos de estudios previos, la sección de

	seguridad y privacidad de la información, con las directrices y controles necesarios para cumplimiento de todos los proveedores de la entidad. Los lineamientos serán impartidos entre la Secretaría TIC, Innovación y Gobierno Abierto y el Departamento de Contratación de la entidad.
Jefes de Dependencias y responsables de contrataciones	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. Adicionar requisitos de seguridad y privacidad de la información en las obligaciones contractuales generales definidas por la Secretaría TIC y el DAC, y obligaciones específicas cuando se trate de proveedores de bienes y servicios tecnológicos**.**
Terceros o Proveedores	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. Cumplir con los requerimientos de seguridad de la información exigidos por la Gobernación de Nariño. Suscribir acuerdos de confidencialidad, tratamiento de datos personales y transferencia de información, con la Gobernación de Nariño en todas sus dependencias. Notificar de manera inmediata cualquier incidente de seguridad que pueda comprometer la confidencialidad, integridad y disponibilidad de los activos de información bajo su responsabilidad. Aceptar la realización de auditorías, revisiones o evaluaciones de cumplimiento, conforme a los establecido contractualmente o según lo determina la Gobernación de Nariño para verificar el cumplimiento de los controles de seguridad.

8.2. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LA RELACIÓN CON PROVEEDORES

Se deben acordar y documentar adecuadamente los requisitos de seguridad de la información necesarios para proteger los activos de la Gobernación de Nariño, con el objetivo de mitigar los riesgos asociados al acceso por parte de proveedores y terceros. Estos requisitos deben ser incorporados en todos los acuerdos y contratos con proveedores.

Las Unidades de Contratación y la Secretaría TIC, Innovación y Gobierno Abierto deberán:

- Identificar y exigir los controles de seguridad de la información a tener en cuenta en el acceso de los proveedores a los activos de información de la Gobernación de Nariño.

- Tener en cuenta los procesos y procedimientos que va a implementar la Gobernación de Nariño, al igual que los procesos y procedimientos que debe exigir a sus proveedores, incluidos:

    - La identificación y documentación de los tipos de proveedores, como: servicios TI, servicios profesionales, componentes de infraestructura de TI, etc., a quienes la Gobernación de Nariño dará acceso a sus activos de información.
    - La definición de los tipos de acceso a la información que se permitirá a los proveedores, el seguimiento y el control de acceso.
    - Los requisitos mínimos de seguridad de la información para cada tipo de información y tipo de acceso, que sirva como base para los acuerdos (Acuerdos de confidencialidad, Acuerdos de Niveles de Servicios), los cuales deberán cumplir los proveedores.

- Identificar los tipos de obligaciones aplicables a los proveedores para proteger los activos de información de la Gobernación de Nariño.

La Secretaria TIC, Innovación y Gobierno Abierto y la Subsecretaria de Talento Humano deberán:

- Identificar y exigir los controles de seguridad de la información a tener en cuenta en el acceso de los funcionarios a los activos de información de la Gobernación de Nariño.

- Gestionar el manejo de incidentes y contingencias asociadas con el acceso de proveedores, incluidas las responsabilidades tanto de la Gobernación de Nariño como de los proveedores.

- Brindar formación sobre toma de conciencia para el personal de la Gobernación de Nariño, que interactúa con el personal de los proveedores, con respecto a las reglas apropiadas de interacción y comportamiento, de acuerdo con el tipo y el nivel de acceso del proveedor a los activos de información de la Gobernación de Nariño.

8.3. TRATAMIENTO DE LA SEGURIDAD DENTRO DE LOS ACUERDOS CON PROVEEDORES

Los riesgos de seguridad de la información asociados con el acceso de proveedores a los activos de la Gobernación de Nariño deben ser identificados, evaluados y tratados adecuadamente. Esto incluye la implementación de controles específicos para mitigar los riesgos identificados y asegurar que los proveedores cumplan con los requisitos de seguridad establecidos.

La Secretaria TIC, Innovación y Gobierno Abierto deberá establecer y acordar los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la Gobernación de Nariño.

Las Unidades de Contratación deberán exigir que, en todos los contratos o convenios con terceras partes, se realice el Acuerdo de confidencialidad, seguridad de la información y tratamiento de datos personales.

Las Unidades de Contratación y la Secretaría TIC, Innovación y Gobierno Abierto, incluirán en el Acuerdo de confidencialidad con los proveedores:

- Objetivo y definiciones relacionadas con el Acuerdo
- Descripción de las obligaciones respecto a la Confidencialidad y Seguridad de la Información sobre los activos de información a los que van a tener acceso los proveedores.
- Autorización de tratamiento de datos personales.
- Descripción de la Propiedad de la Información
- Normatividad aplicada
- Vigencia del Acuerdo

8.4. CADENA DE SUMINISTRO EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES.

Adicionalmente al Acuerdo de Confidencialidad con los proveedores, para los contratos correspondientes a tecnología, la Secretaria TIC puede incluir un anexo con requisitos específicos para gestionar y mitigar los riesgos de seguridad de la información asociados con la cadena de suministro de servicios y productos de tecnologías de la información y comunicaciones (TIC). Estos requisitos deben asegurar que los proveedores implementen controles adecuados para proteger la confidencialidad, integridad y disponibilidad de la información en todas las etapas de la cadena de suministro.

- Establecer y definir los requisitos de seguridad de la información aplicables a la adquisición de productos o servicios de tecnología de la información y comunicaciones. Incluir también los requisitos generales de seguridad de la información para las relaciones con los proveedores.
- Solicitar a los proveedores de servicios de tecnología de la información y comunicaciones que divulguen los requisitos de seguridad de la organización a lo largo de toda la cadena de suministro, especialmente si subcontratan partes del servicio a terceros.
- Requerir que los proveedores compartan y apliquen prácticas de seguridad adecuadas a lo largo de la cadena de suministro para los productos de tecnología de la información y comunicaciones, especialmente si estos productos incluyen componentes adquiridos de otros proveedores.
- Implementar un proceso de seguimiento y métodos aceptables para validar que los productos y servicios de tecnología de la información y comunicaciones cumplan con los requisitos de seguridad establecidos.
- Implementar un proceso para identificar los componentes de productos o servicios que son críticos para mantener la funcionalidad. Estos componentes requieren una mayor atención y escrutinio, especialmente si son desarrollados fuera de la Gobernación de Nariño y subcontratados a otros proveedores.

- Definir reglas claras para compartir información relacionada con la cadena de suministro y cualquier problema o compromiso entre la Gobernación de Nariño y los proveedores.
- Implementar procesos específicos para gestionar el ciclo de vida y la disponibilidad de los componentes de tecnología de la información y comunicaciones. Esto incluye la gestión de riesgos asociados a componentes que ya no están disponibles porque los proveedores han salido del negocio o han dejado de suministrarlos debido a avances tecnológicos.

8.5. SEGUIMIENTO Y REVISIÓN DE LOS SERVICIOS DE LOS PROVEEDORES.

La Gobernación de Nariño debe monitorear, revisar y auditar regularmente los servicios prestados por terceros para asegurarse de que cumplan con los requisitos de seguridad de la información y los términos acordados en los contratos. Esto incluye la evaluación continua del desempeño del proveedor, la verificación del cumplimiento de los controles de seguridad y la identificación de posibles riesgos o incumplimientos.

De esta manera, la Secretaría TIC, Innovación y Gobierno abierto deberá hacer seguimiento, revisar y auditar con regularidad la presentación de servicios de los proveedores, que incluya:

- Asegurar que los términos y condiciones de seguridad de la información de los acuerdos se cumplan, y que los incidentes y problemas de seguridad de la información se gestionan apropiadamente.

- Definir un proceso de relacionamiento para la gestión del servicio entre la Gobernación de Nariño y el proveedor de servicios, a través de informes de supervisión y teniendo en cuenta el Procedimientos de gestión de incidentes de seguridad digital, para:

    - Hacer seguimiento de los niveles de desempeño de servicio para verificar el cumplimiento de los acuerdos.
    - Revisar los reportes de servicio elaborados por el proveedor y concertar reuniones de avance regulares, según se exija en los acuerdos.
    - Llevar a cabo auditorías de los proveedores, junto con la revisión de reportes de auditores independientes, si están disponibles, y acciones sobre las cuestiones identificadas.
    - Suministrar información acerca de incidentes de seguridad de la información y revisar esta información según exija en los acuerdos y en cualquier procedimiento de soporte.
    - Solicitar que el proveedor mantenga una capacidad de servicio suficiente, junto con planes de contingencia destinados a asegurar que se mantienen los niveles de continuidad del servicio acordados, después de fallas considerables en el servicio, o después de un desastre.

- En situaciones en que los proveedores requieran hacer instalaciones de activos de información de carácter tecnológico, tales como servidores, equipos de red, equipos de soporte, entre otros, será requisito base implementar configuraciones que cumplan con las políticas de seguridad de la información de la entidad, para lo cual, en caso necesario, deberán considerar ajustes en el acceso a los equipos, el monitoreo de

capacidad, la sincronización de hora, el registros de auditoría y los servicios de nombre de dominio. El proceso Gestión de Servicios e Infraestructura Tecnológica, tendrá la responsabilidad de verificar y validar la configuración de los equipos instalados, así como también de reportar las debilidades y oportunidades de mejora al proveedor del servicio previa solicitud del proceso dueño del producto y/o servicio del proveedor.

- Los proveedores podrán acceder en forma remota a los activos tecnológicos de la entidad únicamente a través de herramientas definidas por la Secretaría TIC.

- Se debe exigir a los proveedores la presentación de los planes de contingencia que aseguren la disponibilidad de la información, suministrada y procesada entre las partes.

- Todo el personal o sistema con acceso a la red corporativa de la entidad, tendrá la obligación de utilizar programas de antivirus licenciados con su base de firmas actualizadas.

- Utilizar software legalmente adquirido, en cumplimiento de la Ley 603 de 2000 o las normas que la reemplacen, modifiquen o adicionen. Para el efecto mantendrá indemne a la Gobernación de Nariño, de cualquier tipo de reclamación en tal sentido, y en caso de que la entidad se vea obligada a pagar algún tipo de sanción por el incumplimiento de la citada disposición, el proveedor se compromete a reembolsar a la entidad la totalidad de los gastos en que haya incurrido.

- Todo Proveedor y/o tercero que preste el servicio de desarrollo de Software a la entidad, debe implementar normas o las mejores prácticas de la industria en el desarrollo de las aplicaciones para garantizar la seguridad de los sistemas.

- Todo Proveedor y/o tercero que preste el servicio de desarrollo de Software, antes de enviar una aplicación a producción o ponerla a disposición de la entidad, debe realizar la revisión de los códigos fuente a través de un procedimiento manual o automático que permita identificar posibles vulnerabilidades en la codificación y su correspondiente solución. La no verificación de este procedimiento no exime al proveedor de su responsabilidad.

- Establecer con la Gobernación de Nariño, el procedimiento adecuado para el borrado seguro de la información propiedad de la entidad. Este procedimiento deberá ser desarrollado antes o durante el transcurso de la relación contractual.

Se prohíbe expresamente cualquier tipo de actividad que vaya en contravía de las políticas de seguridad de la información definidas al interior de la entidad, como lo son entre otras las siguientes:

- El uso de los recursos proporcionados por la Gobernación de Nariño, para la realización de actividades no relacionadas con el servicio contratado.

- La conexión a la red de equipos, dispositivos (portátiles personales, memorias USB, discos duros externos entre otros) y/o aplicaciones que no estén autorizados por la Secretaría TIC.

- Introducir en los sistemas de información o la red corporativa de la entidad, contenidos maliciosos, inadecuados, obscenos, amenazadores, inmorales u ofensivos entre otros.

- Introducir voluntariamente en la red corporativa de la entidad, cualquier tipo de malware sin importar el medio, (programas, macros etc.), dispositivo lógico, dispositivo físico o cualquier otro tipo de secuencias de órdenes que causen y/o que sean susceptibles de causar daño y/o alteración en los recursos informáticos.

Intentar obtener sin autorización explícita otros derechos de acceso distintos a los otorgados por la Gobernación de Nariño.

Intentar distorsionar y/o eliminar registros (log) de los sistemas de información de la entidad.

8.6. GESTIÓN DE CAMBIOS EN LOS SERVICIOS DE LOS PROVEEDORES.

Los cambios en la provisión de servicios por parte de los proveedores deben ser gestionados de manera que se mantengan y mejoren las políticas de seguridad de la información, los procedimientos y los controles específicos. Esto implica evaluar la criticidad de la información comercial, los sistemas y procesos involucrados, y realizar una reevaluación de riesgos antes de implementar cualquier cambio significativo.

Para gestionar los cambios en el suministro de servicios por parte de los proveedores, y garantizar el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información, la Secretaría TIC, Innovación y Gobierno Abierto debe, a través del Procedimiento de Gestión de Cambios, administrar estos cambios considerando la criticidad de la información, los sistemas y procesos involucrados de la Gobernación, así como la reevaluación de los riesgos de seguridad de la información.

Dentro de este procedimiento, deberá tener en cuenta los siguientes aspectos:

- Los cambios en los acuerdos con los proveedores.
- Los cambios hechos por la Gobernación de Nariño para implementar las mejoras a los servicios ofrecidos en la actualidad, el desarrollo de nuevas aplicaciones y sistemas, las modificaciones o actualizaciones a las políticas y procedimientos de la entidad, los controles nuevos o modificados para resolver incidentes de seguridad de la información y mejora de la seguridad.
- Los cambios en los servicios de los proveedores como cambios y mejoras en las redes, el uso de nuevas tecnologías.
- La adopción de nuevos productos o versiones más recientes en herramientas y ambientes de desarrollo.
- Cambios en las ubicaciones físicas de las instalaciones de servicio.
- Cambio en los proveedores de servicios.

9. Control de cambios.

Versión	Fecha de versión	Descripción del cambio	Responsable
01	15/12/2025	Creación del documento	

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