 <p>GOBERNACIÓN DE NARIÑO</p>	<p>CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN Y HERRAMIENTAS DIGITALES</p>	<p>CÓDIGO: GTC-P-04</p>
		<p>VERSIÓN: 01</p>
		<p>FECHA VERSIÓN: 12/03/2026</p>
		<p>PÁGINA: 1 de 9</p>

### 1. Objetivo.

Establecer el procedimiento para los lineamientos, responsabilidades y actividades necesarias para realizar el control de acceso a los sistemas de información y herramientas digitales de la Gobernación de Nariño, garantizando el uso adecuado y seguro de los activos de información.


### 2. Alcance.

Este procedimiento aplica a todos los funcionarios, contratistas/proveedores y terceros autorizados, que requieran acceso a sistemas de información institucionales (locales o en la nube), aplicaciones, plataformas tecnológicas, páginas web y herramientas digitales autorizadas, inicia con la solicitud de activación o revocación de acceso y termina con la asignación de credenciales inactivación de acceso en sistemas de información y páginas web.

### 3. Definiciones.

- **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.
- **Autenticación:** proceso mediante el cual un sistema de información verifica la identidad de un usuario antes de permitirle el acceso, utilizando mecanismos como usuario y contraseña, certificados digitales, tokens o doble factor de autenticación.
- **Cambio:** Adición, modificación o eliminación planificada o no planificada que pueda afectar un servicio, infraestructura, proceso o activo de información.
- **Confidencialidad:** propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.
- **Control de acceso:** conjunto de políticas, procedimientos, controles técnicos y administrativos que regulan el acceso a los sistemas de información y a la página web de la Gobernación de Nariño, garantizando que solo los usuarios autorizados accedan a los recursos permitidos.
- **Credenciales de acceso:** información confidencial e intransferible utilizada para autenticar a un usuario, como nombre de usuario, contraseña, token o certificado digital. Su uso indebido constituye una falta a las políticas de seguridad de la información.
- **Disponibilidad de la información:** se refiere a la seguridad que la información puede ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.
- **Doble factor de autenticación (2FA):** mecanismo de seguridad que requiere al menos dos factores diferentes de autenticación, fortaleciendo la protección frente a accesos no

<p>PROCESO ASOCIADO: GESTIÓN DE TECNOLOGÍA</p>	<p>DEPENDENCIA ASOCIADA: SECRETARÍA TIC, INNOVACIÓN Y GOBIERNO ABIERTO</p>
--	--

 <p>GOBERNACIÓN DE NARIÑO</p>	<p>CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN Y HERRAMIENTAS DIGITALES</p>	<p>CÓDIGO: GTC-P-04</p>
		<p>VERSIÓN: 01</p>
		<p>FECHA VERSIÓN: 12/03/2026</p>
		<p>PÁGINA: 2 de 9</p>


autorizados.

- **Gestión de accesos:** proceso que incluye la solicitud, evaluación, aprobación, asignación, modificación, revisión periódica y revocación de accesos a los sistemas de información y a la página web institucional.
- **Integridad:** se refiere a la garantía de que una información no ha sido alterada, borrada, reordenada, copiada, etc., bien durante el proceso de transmisión o en su propio equipo de origen.
- **Página web institucional:** plataforma digital oficial de la Gobernación de Nariño, incluidos sus portales y subsitios, destinada a la publicación de información institucional y la prestación de servicios digitales.
- **Perfil de acceso:** conjunto predefinido de permisos asignados a un usuario según su rol, cargo y responsabilidades, aplicando el principio de mínimo privilegio.
- **Principio de mínimo privilegio:** principio de seguridad que establece que los usuarios deben contar únicamente con los permisos estrictamente necesarios para el desempeño de sus funciones
- **Proveedor:** persona natural o jurídica que presta un servicio a la Gobernación de Nariño bajo un contrato o acuerdo formal.
- **Registro de accesos:** bitácora o mecanismo de trazabilidad que almacena información sobre los accesos otorgados, modificados o revocados, con fines de control y auditoría.
- **Revocación de acceso:** proceso mediante el cual se deshabilitan los permisos de un usuario cuando cesa su relación con la entidad, cambia de funciones o incumple las políticas de seguridad.
- **Rol:** conjunto de responsabilidades y permisos definidos dentro de un sistema o plataforma web.
- **Sistema de información:** conjunto organizado de aplicaciones, datos, infraestructura, procedimientos y personas que permiten gestionar información para el cumplimiento de los objetivos institucionales.
- **Usuario:** persona autorizada para acceder a los sistemas de información o a la página web institucional bajo las condiciones definidas por la Gobernación de Nariño.

#### 4. Condiciones y/o políticas específicas de operación

El procedimiento de Control de acceso a sistemas de información y herramientas digitales, hace parte del conjunto de procedimientos de seguridad y privacidad de la información que constituyen una base sólida para que en la Gobernación de Nariño se realice una implementación transversal de la Política de seguridad de la información y seguridad digital,


<p>PROCESO ASOCIADO: GESTIÓN DE TECNOLOGÍA</p>	<p>DEPENDENCIA ASOCIADA: SECRETARÍA TIC, INNOVACIÓN Y GOBIERNO ABIERTO</p>
--	--

 <p><b>GOBERNACIÓN DE NARIÑO</b></p>	<b>CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN Y HERRAMIENTAS DIGITALES</b>	<b>CÓDIGO: GTC-P-04</b>
		<b>VERSIÓN: 01</b>
		<b>FECHA VERSIÓN: 12/03/2026</b>
		<b>PÁGINA: 3 de 9</b>

para salvaguardar sus activos de información, sus procesos y los servicios que presta.


- Los accesos se otorgarán exclusivamente con base en las funciones del cargo o actividades contractuales.
- Está prohibido solicitar o mantener accesos que no sean estrictamente necesarios.
- Los perfiles de acceso deben revisarse periódicamente para evitar acumulación indebida de permisos.
- Las credenciales de acceso son personales, únicas e intransferibles
- Está prohibido compartir usuarios, contraseñas o mecanismos de autenticación con otros funcionarios, contratistas o terceros.
- El usuario será responsable de todas las actividades realizadas con sus credenciales.
- Las contraseñas deben cumplir criterios mínimos de complejidad definidos por la Secretaría TIC en la Guía de gestión de contraseñas
- Deben cambiarse periódicamente y de manera obligatoria en el primer ingreso.
- No se permite reutilizar contraseñas anteriores.
- Ante sospecha de compromiso, la contraseña debe cambiarse inmediatamente y reportarse a la Secretaría TIC.
- Para accesos administrativos, críticos o de alto privilegio, se deberá implementar doble factor de autenticación (2FA) cuando la tecnología lo permita.
- Los accesos remotos o desde redes externas estarán sujetos a controles adicionales de seguridad.
- Los accesos a la administración y edición de la página web se asignarán únicamente a personal autorizado.
- Los roles de editor, publicador y administrador estarán claramente definidos.
- Toda publicación o modificación de contenido debe cumplir los lineamientos institucionales y normativos vigentes.
- Se mantendrá trazabilidad de cambios y responsables.
- Está prohibido utilizar los sistemas de información y la página web para fines personales, políticos, comerciales o no autorizados.
- No se permite la instalación de software, extensiones o complementos sin autorización de la Secretaría TIC.
- El acceso desde dispositivos no autorizados estará restringido o sujeto a controles adicionales
- Todo cambio de rol, funciones o dependencia debe ser informado oportunamente para la actualización de accesos.
- La revocación de accesos debe realizarse de manera inmediata ante:
  - Terminación de vínculo laboral o contractual
  - Cambio de funciones
  - Incumplimiento de políticas de seguridad y privacidad de la información
  - Incidentes de seguridad de la información
- Todos los accesos, modificaciones y revocaciones deberán quedar registrados.
- La Secretaría TIC (o sus proveedores externos) podrá realizar monitoreo preventivo para detectar accesos inusuales o no autorizados.

<b>PROCESO ASOCIADO: GESTIÓN DE TECNOLOGÍA</b>	<b>DEPENDENCIA ASOCIADA: SECRETARÍA TIC, INNOVACIÓN Y GOBIERNO ABIERTO</b>
--	--

 <p><b>GOBERNACIÓN DE NARIÑO</b></p>	<b>CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN Y HERRAMIENTAS DIGITALES</b>	<b>CÓDIGO: GTC-P-04</b>
		<b>VERSIÓN: 01</b>
		<b>FECHA VERSIÓN: 12/03/2026</b>
		<b>PÁGINA: 4 de 9</b>

- La información de los registros será utilizada exclusivamente para fines de seguridad, control y auditoría.
- Los usuarios deben conocer y cumplir las políticas de seguridad y privacidad de la información de la Gobernación de Nariño.
- El desconocimiento de estas políticas no exime de responsabilidad, ya que se encuentran publicadas en la página web e intranet institucional.
- El incumplimiento podrá dar lugar a sanciones administrativas, contractuales o legales, según corresponda.

<b>PROCESO ASOCIADO: GESTIÓN DE TECNOLOGÍA</b>	<b>DEPENDENCIA ASOCIADA: SECRETARÍA TIC, INNOVACIÓN Y GOBIERNO ABIERTO</b>
--	--

	<b>CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN Y HERRAMIENTAS DIGITALES</b>	<b>CÓDIGO:</b> GTC-P-04
		<b>VERSIÓN:</b> 01
		<b>FECHA VERSIÓN:</b> 12/03/2026
		<b>PÁGINA:</b> 1 de 9

#### 4.1 Descripción de actividades.

##### 1. Solicitud de activación o revocación de acceso

Fuente de entrada	Entrada	Descripción de la actividad	Punto de Control	Responsable	Salida	Receptor de salida
Dependencias entidad Secretaría TIC	Formulario GTC-F-19 de solicitud de acceso	La dependencia solicitante debe diligenciar el Formulario GTC-F-19 de solicitud de acceso indicando los datos del solicitante (jefe de dependencia o líder de proceso), datos del usuario de acceso, tipo de vinculación, cargo y dependencia, número de contrato, sistema o página web, rol y permisos requeridos, y justificación. El formulario se diligenciará a través del intranet en el menú SOS TIC, dispuesto por la Secretaría TIC y se envía notificación al correo electrónico institucional tic@narino.gov.co.		Jefes de Dependencias  Secretaría TIC	Formulario GTC-F-19 de solicitud de acceso diligenciado	Secretaría TIC


Si la solicitud corresponde a creación de Usuario se procede con el ítem 2.

Si la solicitud corresponde a revocación de acceso se procede con el ítem 5.

##### 2. Revisión y Aprobación.

Fuente de entrada	Entrada	Descripción de la actividad	Punto de Control	Responsable	Salida	Receptor de salida
Dependencias entidad Secretaría TIC	Formulario GTC-F-19 diligenciado	Los profesionales de la Secretaría TIC encargados de administración de sistemas de información y páginas web verifican la solicitud de acceso y define el rol adecuado.		Profesionales Secretaría TIC	Análisis técnico	Profesionales Secretaría TIC

<b>PROCESO ASOCIADO:</b> GESTIÓN DE TECNOLOGÍA	<b>DEPENDENCIA ASOCIADA:</b> SECRETARÍA TIC, INNOVACIÓN Y GOBIERNO ABIERTO
---	---


	<b>CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN Y HERRAMIENTAS DIGITALES</b>	<b>CÓDIGO: GTC-P-04</b>
		<b>VERSIÓN: 01</b>
		<b>FECHA VERSIÓN: 12/03/2026</b>
		<b>PÁGINA: 2 de 9</b>

		<p>Según el análisis realizado aprueba o rechaza la solicitud, de ser necesario solicitan mayor aclaración o soportes de vinculación del personal a la dependencia.</p> <p>Si la solicitud es rechazada, se envía respuesta al correo electrónico del solicitante, con la justificación correspondiente.</p> <p>Si la solicitud de aprobada se continúa con el paso 3.</p>				
--	--	--	--	--	--	--

### 3. Asignación de credenciales de acceso.

Fuente de entrada	Entrada	Descripción de la actividad	Punto de Control	Responsable	Salida	Receptor de salida
Profesionales Secretaría TIC	Formulario GTC-F-19 diligenciado  Análisis técnico	<p>El profesional de la Secretaría TIC responsable de(los) sistema(s) de información o página web objeto de la solicitud, proceso de realizar lo siguiente:</p> <ul style="list-style-type: none"> <li>- Creación de usuario y credenciales únicas de acceso.</li> <li>- Notificación al usuario mediante correo electrónico.</li> <li>- Envío de instrucciones y material de capacitación sobre el manejo del sistema o página web (cuando se cuente con el mismo), al correo electrónico del usuario.</li> </ul>		Profesionales Secretaría TIC	Credenciales de acceso creadas	Dependencias entidad Secretaría TIC

<b>PROCESO ASOCIADO: GESTIÓN DE TECNOLOGÍA</b>	<b>DEPENDENCIA ASOCIADA: SECRETARÍA TIC, INNOVACIÓN Y GOBIERNO ABIERTO</b>
--	--

	<b>CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN Y HERRAMIENTAS DIGITALES</b>	<b>CÓDIGO:</b> GTC-P-04
		<b>VERSIÓN:</b> 01
		<b>FECHA VERSIÓN:</b> 12/03/2026
		<b>PÁGINA:</b> 3 de 9

		<p>El sistema deberá obligar el cambio de contraseña en el primer ingreso del usuario.</p> <p>Se registra el acceso otorgado en el formato de solicitud de acceso.</p>				
--	--	--	--	--	--	--


#### 4. Control de acceso.

Fuente de entrada	Entrada	Descripción de la actividad	Punto de Control	Responsable	Salida	Receptor de salida
Profesionales Secretaría TIC	Formulario GTC-F-19 diligenciado  Correo electrónico	<p>El profesional de la Secretaría TIC responsable, verifica que el usuario ingrese al sistema o página web objeto de la solicitud, con el fin de confirmar si el acceso es correcto y los permisos se encuentran acorde a lo requerido.</p> <p>Lo anterior mediante comunicación a través de correo electrónico y llamadas telefónicas.</p> <p>Si se verifica algún inconveniente, se procede a realizar los ajustes necesarios y/o aclaraciones al usuario y dependencia.</p>		Profesionales Secretaría TIC	Credenciales de acceso creadas  Correo electrónico	Secretaría TIC

#### 5. Revocación de acceso.

Fuente de entrada	Entrada	Descripción de la actividad	Punto de Control	Responsable	Salida	Receptor de salida
Dependencias entidad Secretaría TIC	Formulario GTC-F-19 diligenciado	El responsable de la Secretaría TIC revisa la solicitud de revocación de acceso, si es necesario se solicitará aclaraciones a la		Profesionales Secretaría TIC	Revocación de acceso aplicada	Jefe dependencia

<b>PROCESO ASOCIADO:</b> GESTIÓN DE TECNOLOGÍA	<b>DEPENDENCIA ASOCIADA:</b> SECRETARÍA TIC, INNOVACIÓN Y GOBIERNO ABIERTO
---	---

	<b>CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN Y HERRAMIENTAS DIGITALES</b>	<b>CÓDIGO:</b> GTC-P-04
		<b>VERSIÓN:</b> 01
		<b>FECHA VERSIÓN:</b> 12/03/2026
		<b>PÁGINA:</b> 4 de 9


		<p>dependencia solicitante.</p> <p>Se procede con la revocación de acceso o inactivación de usuario en el sistema o página web correspondiente.</p> <p>Notificación al usuario de la dependencia solicitante mediante correo electrónico, sobre la revocación realizada.</p> <p>Se registra el acceso revocado en el formulario de solicitud de acceso.</p>				
--	--	---	--	--	--	--

#### 6. Seguimiento y auditoría.

Fuente de entrada	Entrada	Descripción de la actividad	Punto de Control	Responsable	Salida	Receptor de salida
Secretaría TIC	Credenciales de acceso a los sistemas de información y páginas web	Los profesionales de la Secretaría TIC realizarán seguimiento permanente al acceso de los usuarios a los sistemas de información y páginas web, acompañamiento a los usuarios y atención sobre los ajustes que deban ser realizados sobre los roles y permisos otorgados.		Profesionales Secretaría TIC	Seguimiento a los perfiles de usuario	Secretaría TIC

#### 7. Fin

<b>PROCESO ASOCIADO:</b> GESTIÓN DE TECNOLOGÍA	<b>DEPENDENCIA ASOCIADA:</b> SECRETARÍA TIC, INNOVACIÓN Y GOBIERNO ABIERTO
---	---

 <p><b>GOBERNACIÓN DE NARIÑO</b></p>	<b>CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN Y HERRAMIENTAS DIGITALES</b>	<b>CÓDIGO:</b> GTC-P-04
		<b>VERSIÓN:</b> 01
		<b>FECHA VERSIÓN:</b> 12/03/2026
		<b>PÁGINA:</b> 1 de 9

## 5. Diagrama de flujo.

N/A

## 6. Documentos relacionados.

- Política general de seguridad y privacidad de la Información Gobernación de Nariño
- Política nacional de Gobierno Digital y Seguridad Digital
- Modelo de seguridad y privacidad de la información MSPI de MinTIC
- Norma NTC/IEC ISO 27001:2013
- Plan Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
- Norma ISO/IEC 27001
- Ley 1581 de 2012
- Decreto 1078 de 2015
- Política de Control de Acceso Gobernación de Nariño
- Manual de Usabilidad y Estructura de Sitios Web de la Gobernación de Nariño.
- Términos y condiciones de uso del sitio web. Gobernación de Nariño
- Política de tratamiento de datos personales
- Formato GTC-F-19 Solicitud de acceso

## 8. Anexos.

N/A

## 8. Control de cambios.

Versión	Fecha de versión	Descripción del cambio	Responsable
01	12/03/2026	Creación del documento	

## 9. Responsable.

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

## 10. 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

<b>PROCESO ASOCIADO:</b> GESTIÓN DE TECNOLOGÍA	<b>DEPENDENCIA ASOCIADA:</b> SECRETARÍA TIC, INNOVACIÓN Y GOBIERNO ABIERTO
---	---