# 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 Gobernación de Nariño, en el marco de su compromiso con la seguridad de la información, la protección de los datos personales y la gestión responsable de sus recursos tecnológicos, establece la presente Política de Control de Acceso, como parte integral de la Política de Seguridad y Privacidad de la Información y del Modelo de Seguridad y Privacidad del Gobierno Digital.

Esta política define los principios, lineamientos y responsabilidades que regulan el acceso a los activos de información entre los cuales se encuentran: áreas de procesamiento, redes y comunicaciones, recursos de plataforma tecnológica y recursos institucionales, sistemas de información, plataformas, bases de datos, servicios en la nube, etc., con el fin de preservar su confidencialidad, integridad y disponibilidad, según la normatividad, controles y lineamientos vigentes.

## 4. Objetivo.

Establecer los lineamientos institucionales para el control de acceso a los activos de información de la Gobernación de Nariño, garantizando que el acceso sea autorizado, limitado, controlado y acorde con los perfiles y responsabilidades de cada usuario.

## 5. Alcance.

Esta Política aplica a Todos los funcionarios, contratistas/proveedores y terceros que accedan a recursos tecnológicos de la Gobernación de Nariño, todos los activos de información, y todas las dependencias, sus procesos misionales, estratégicos, apoyo y evaluación.

## 6. Marco Conceptual

- **Acceso remoto:** uso de mecanismos tecnológicos para conectarse a sistemas internos desde ubicaciones externas.

- **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.

- **Autenticación:** proceso para validad la identidad de un usuario antes de permitir el acceso a un sistema.

- **Autorización:** proceso mediante el cual se definen y asignan permisos a un usuario o rol para realizar acciones específicas.

- **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.

- **Control de acceso:** conjunto de medidas, **p**rocesos y mecanismos que **p**ermiten autorizar, restringir, registrar y supervisar el acceso a la información, sist**emas** o recursos tecnológicos**.**

- **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.

- **Creación de usuario:** procedimiento por el cual se asigna un usuario y contraseña a funcionarios, contratistas y terceras partes para el ingreso a la red institucional, correo electrónico, sistemas de información e infraestructura tecnológica.

- **Credenciales:** medios utilizados para autenticar la identidad de un usuario: nombre de usuario, contraseña, tokens, certificados digitales, mfa, entre otros.

- **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.

- **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.

- **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.

- **Inactivación de usuario:** proceso mediante el cual se suspende de manera temporal o definitiva el acceso del usuario a la red, correo electrónico, infraestructura tecnológica y sistemas de información dependiendo de la solicitud.

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

- **Información clasificada:** información cuyo acceso se limita por razones legales, de seguridad, interés público o protección de datos personales.

- **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.

- **Privilegios:** capacidades o permisos concedidos a un usuario para ejecutar funciones dentro de un sistema.

- **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.

- **Roles y perfiles:** estructura que agrupa permisos y responsabilidades asignadas a usuarios según su función dentro de la organización.

- **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).

- **Sistemas de información:** es un conjunto de componentes interrelacionados que trabajan juntos para recopilar, procesar, almacenar y difundir información con el fin de apoyar la toma de decisiones y la obtención de objetivos organizacionales.

- **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.

- **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 603 de 2000
- Ley 1266 de 2008
- La Ley 1273 de 2009
- Ley 1581 de 2012
- Decreto 1377 de 2013
- Ley 1581 de 2012
- Decreto 1078 de 2015
- Decreto 1081 de 2015
- CONPES 3701 de 2011
- CONPES 3854 de 2016
- CONPES 3995 de 2020
- Decreto 620 de 2020
- Modelo de Seguridad y Privacidad de la Información (MSPI) – MinTIC.
- Norma ISO/IEC 27001:2022
- Norma ISO/IEC 27002:2022
- Manual de seguridad y privacidad de la información – MinTIC - Estrategia de Gobierno Digital

## 8. Descripción del Desarrollo de la Política

### 8.1. PRINCIPIOS RECTORES

- Autenticación: Toda persona debe identificarse de forma única para acceder a los activos de información.
- Autorización: Los permisos se asignan según rol, función y necesidad.
- Responsabilidad: Cada usuario es responsable de las actividades realizadas con sus credenciales.
- Privacidad: Se garantiza la protección de la información tratada por la entidad.
- Auditoría: Todo acceso será susceptible de verificación y seguimiento.

### 8.2. LINEAMIENTOS GENERALES DE CONTROL DE ACCESO

#### 8.2.1. GESTIÓN DE IDENTIDADES Y CREDENCIALES

El acceso a los activos de información de la Gobernación de Nariño, será realizado según el procedimiento y controles implementados por la Secretaría TIC, teniendo en cuenta la vinculación de personal en la entidad, funciones, obligaciones contractuales y autorización expresa por parte de los jefes de las dependencias y/o líderes de los procesos responsables de los activos de información.

- Cada usuario deberá contar con un identificador único para las credenciales de acceso.
- Se prohíbe el uso compartido de cuentas o contraseñas.
- Las contraseñas deben cumplir con políticas de complejidad y expiración definidas por la Secretaría TIC.
- Las credenciales deben ser revocadas inmediatamente al finalizar la relación laboral o contractual del usuario.

### 8.2.2. ACCESO A LA INFORMACIÓN

El personal vinculado a la entidad firmará un acuerdo de confidencialidad, seguridad de la información y tratamiento de datos personales, al iniciar su relación laboral o contractual con la Gobernación, por lo tanto, tiene pleno conocimiento de la importancia del bueno uso, protección de la información de la entidad y las políticas de seguridad relacionadas.

El acceso a la información será realizado según las funciones y obligaciones contractuales con el seguimiento por parte de los jefes inmediatos y supervisores de contratos.

De igual manera se dará acceso a la información a través de asignación de usuarios con credenciales seguras, roles y permisos autorizados por los jefes de las dependencias y/o líderes de los procesos responsables de la información.

- El acceso a datos personales o sensibles requiere autorización expresa del responsable de la información, según lo definido por la entidad en la Política de tratamiento de datos personales y plan de implementación.
- Se aplicará el principio de necesidad y proporcionalidad: solo se accederá a los datos requeridos para cumplir funciones y obligaciones contractuales.
- Se implementarán controles de trazabilidad para registrar cada acceso.

### 8.2.3. CONTROL DE ACCESO FÍSICO

El ingreso a los sitios donde se encuentra instalada la infraestructura tecnológica en el edificio principal de la Gobernación de Nariño y las sedes externas, será realizado según los procedimientos y controles definidos por la Secretaría TIC, exclusivamente para el personal autorizado.

- El ingreso a los Datacenter, centros de datos o áreas restringidas estará controlado por mecanismos de identificación y seguridad física.
- Se mantendrán registros de ingreso y salida.
- Solo el personal autorizado podrá manipular equipos o medios de respaldo.

### 8.2.4. CONTROL DE ACCESO LÓGICO

- Todos los sistemas institucionales deben contar con mecanismos de autenticación (usuario/contraseña, doble factor, etc.).
- Se aplicarán perfiles y roles diferenciados según el tipo de usuario, y los permisos que se encuentren definidos según las funciones, obligaciones contractuales y autorización por parte de los jefes y/o líderes de procesos.
- Los accesos administrativos o privilegiados deberán registrarse y auditarse, según los procedimientos definidos por la Secretaría TIC.

### 8.2.5. ACCESO REMOTO

El acceso remoto a los sistemas institucionales deberá realizarse mediante canales seguros (VPN o similares), autorizados y controlados por la Secretaría TIC.

### 8.2.6. MONITOREO Y AUDITORÍA

- La Secretaría TIC implementará herramientas de monitoreo de accesos, alertas y reportes de incidentes.
- Toda anomalía será reportada a la Secretaría TIC y equipo de seguridad digital de la entidad, para identificación y gestión de incidentes según el procedimiento establecido.

## 8.3. CONTROL DE CUMPLIMIENTO

El incumplimiento de esta política constituye falta disciplinaria o contractual y podrá dar lugar a sanciones según el régimen interno, el Código Disciplinario Único y las normas aplicables sobre seguridad de la información y protección de datos.

## 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 |