Tabla de contenido

1. INTRODUCCIÓN

La Guía de Gestión de Contraseñas de la Gobernación de Nariño establece los lineamientos, criterios y controles necesarios para la adecuada administración de las credenciales de acceso utilizadas en los sistemas de información, aplicaciones, plataformas tecnológicas, servicios en la nube, redes y demás activos tecnológicos de la entidad.

Las contraseñas constituyen uno de los principales mecanismos de autenticación y control de acceso; sin embargo, su uso inadecuado representa uno de los riesgos más frecuentes en materia de seguridad digital. Prácticas como contraseñas débiles, reutilización de credenciales, almacenamiento inseguro o la falta de controles técnicos incrementan la probabilidad de accesos no autorizados, fuga de información, suplantación de identidad y afectación a la continuidad de los servicios institucionales.

En este contexto, la presente guía se enmarca en el Sistema de Seguridad Digital **y en el** Modelo de Seguridad y Privacidad de la Información (MSPI) definido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), y se articula con la normatividad vigente en Colombia, así como con buenas prácticas internacionales en gestión de accesos y control de identidades.

Su aplicación busca fortalecer la cultura de seguridad de la información en la Gobernación de Nariño, promover la responsabilidad individual de los usuarios frente al uso de sus credenciales, y establecer controles preventivos, detectivos y correctivos que contribuyan a garantizar la confidencialidad, integridad y disponibilidad de los activos de información.

2. OBJETIVO.

Establecer los lineamientos, controles y buenas prácticas para la gestión segura de contraseñas en la Gobernación de Nariño, con el fin de proteger los sistemas de información y los activos digitales frente a accesos no autorizados, uso indebido de credenciales y demás riesgos asociados a la autenticación.

3. ALCANCE.

La guía de gestión de contraseña aplica a Servidores públicos de la Gobernación de Nariño, Contratistas, proveedores y terceros con cuentas de acceso a sistemas de información a infraestructura tecnológica, aplicaciones, bases de datos, redes, correo electrónico institucional, servicios en la nube y demás activos de información de la entidad.

4. DEFINICIONES.

- **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.

- **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 del Estado 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.

- **Contraseña:** Conjunto confidencial de caracteres (letras, números y símbolos) que utiliza un usuario para autenticarse y demostrar su identidad al acceder a un sistema de información, aplicación, red o servicio digital.

- **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, procesos y mecanismos que permiten autorizar, restringir, registrar y supervisar el acceso a la información, sistemas 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.

- **Cuenta de usuario:** es el conjunto de credenciales, permisos y configuraciones

asignadas a una persona o sistema, que permite identificarla y autenticarla para acceder a los sistemas de información, aplicaciones, redes o servicios digitales de una entidad.

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

- **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.

- **Doble factor de autenticación:** es un mecanismo de seguridad que exige al usuario dos factores distintos de verificación para confirmar su identidad antes de acceder a un sistema, aplicación o servicio digital.

- **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.

- **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.

- **Prevención:** Se deben aplicar controles que minimicen el riesgo de compromiso de credenciales.

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

- **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.

- **Responsabilidad individual:** Es la capacidad de cada usuario para responder de manera personal por del uso y protección de su contraseña.

- **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.

- **Trazabilidad:** Es la capacidad de seguir el recorrido completo de un producto a través de todas las etapas de su cadena de suministro

- **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.

5. CONDICIONES Y/O POLÍTICAS ESPECÍFICAS DE OPERACIÓN.

La guía de gestión de contraseñas hace parte de la Política de Control de acceso que integra el sistema de seguridad y privacidad de la información de la Gobernación de Nariño.

Condiciones generales:

- La contraseña es un código único, personal e intransferible, que no debe ser divulgado o compartido con terceras personas, el no observar esta buena práctica constituye una violación a la Política de seguridad y privacidad de la información de la entidad.
- Un usuario registrado y autorizado en la Entidad, se debe autenticar siempre con su contraseña personal para acceder a los Sistemas de Información y a los servicios tecnológicos.
- Toda cuenta de usuario de la infraestructura tecnológica debe identificar una persona en la vida real, funcionario, contratista o tercero, no se deben permitir el uso de cuentas genéricas o anónimas.
- En caso de requerirse el acceso a las cuentas de un funcionario que se encuentre fuera de las instalaciones de la Entidad, únicamente el jefe inmediato o superior realizará la solicitud a la Secretaría TIC y ésta autorizará a la mesa de ayuda para asignar una contraseña temporal con una duración específica, y luego la cuenta será desactivada; el solicitante será responsable de lo que suceda con los activos de información y la seguridad por la duración del evento.

  Una vez el funcionario retorne a las oficinas deberá ser informado del cambio de contraseña y solicitará la activación de su cuenta actualizando su contraseña. Manteniendo la confidencialidad de la misma.

- El usuario es el responsable de garantizar la seguridad de la información a su cargo, la cual está disponible en medios electrónicos y a través de documentos físicos, utilizando para ello en todo momento las mejores prácticas de manejo documental, contraseñas seguras y dándole a esta el uso adecuado.

- Las contraseñas tendrán un periodo de vigencia de Veintiocho (28) días, fecha en la cual se obligará a cambiarse de acuerdo con las mejores prácticas y políticas de seguridad, de lo contrario se desactiva la cuenta.

- Es importante precisar que el usuario y la contraseña, es el mecanismo de identificación de un usuario ante la Entidad para el uso de los recursos tecnológicos y de información, esta identificación, permite manejar los perfiles y permisos de los usuarios, hacer el seguimiento y trazabilidad en caso de problemas de acceso y seguridad.

Marco normativo y de referencia:

- Constitución Política de Colombia.
- Ley 1581 de 2012 – Protección de Datos Personales.
- Decreto 1074 de 2015.
- Ley 1712 de 2014 – Ley de Transparencia.
- Decreto 612 de 2018 – Seguridad Digital.

- CONPES 3854 de 2016 – Política Nacional de Seguridad Digital.
- Modelo de Seguridad y Privacidad de la Información (MSPI) – MINTIC.
- Norma ISO/IEC 27001 – Controles de acceso.
- Norma ISO/IEC 27002 – Gestión de contraseñas.

6. DESCRIPCIÓN DEL DESARROLLO DE ACTIVIDADES

6.1. PRINCIPIOS DE LA GESTIÓN DE CONTRASEÑAS

La gestión de contraseñas en la Gobernación de Nariño se rige por los siguientes principios:

- **Confidencialidad:** Las contraseñas son información sensible y personal.
- **Responsabilidad individual:** Cada usuario es responsable del uso y protección de su contraseña.
- **No compartición:** Las contraseñas no deben ser compartidas bajo ninguna circunstancia.
- **Trazabilidad:** Todo acceso debe poder ser auditado.
- **Prevención:** Se deben aplicar controles que minimicen el riesgo de compromiso de credenciales.

6.2. LINEAMIENTOS PARA LA CREACIÓN DE CONTRASEÑAS

6.2.1. REQUISITOS MÍNIMOS

Las contraseñas deberán cumplir como mínimo con los siguientes criterios:

- Longitud mínima de **12 caracteres**.
- Incluir al menos:
  - Una letra mayúscula.
  - Una letra minúscula.
  - Un número.
  - Un carácter especial.
- No contener información personal del usuario (nombre, cédula, fecha de nacimiento, cargo, etc.).
- No reutilizar contraseñas anteriores.

6.2.2. FRASES DE CONTRASEÑA

Se recomienda el uso de frases de contraseña (passphrases), fáciles de recordar, pero difíciles de adivinar, por ejemplo, combinaciones de palabras, números y símbolos.

6.3. USO Y MANEJO SEGURO DE CONTRASEÑAS

- No escribir contraseñas en papel ni almacenarlas en lugares visibles.
- No guardar contraseñas en navegadores sin mecanismos de cifrado aprobados.
- No enviar contraseñas por correo electrónico, mensajería instantánea o llamadas telefónicas.
- Utilizar gestores de contraseñas autorizados por la entidad, cuando aplique.
- Cerrar sesión al finalizar el uso de sistemas o equipos compartidos.

6.4. CAMBIO Y VIGENCIA DE CONTRASEÑAS

- Las contraseñas deberán cambiarse como mínimo cada **90 días**.
- El cambio inmediato de contraseña será obligatorio cuando:

  - Exista sospecha de compromiso.
  - Se presente un incidente de seguridad.
  - El usuario haya compartido accidentalmente su contraseña.
- No se permite reutilizar las últimas 5 contraseñas.

6.5. GESTIÓN DE CONTRASEÑAS PRIVILEGIADAS

Las cuentas con privilegios elevados (administradores, bases de datos, servidores, redes) deberán cumplir controles adicionales:

- Uso exclusivo para actividades administrativas.
- Contraseñas con mayor complejidad y longitud mínima de **15 caracteres**.
- Almacenamiento cifrado y controlado.
- Registro y monitoreo de accesos.
- Revisión periódica de la necesidad del privilegio.

6.6. AUTENTICACIÓN MULTIFACTOR (MFA)

Cuando sea técnicamente viable, la Gobernación de Nariño implementará autenticación multifactor (MFA) como complemento a las contraseñas, especialmente en:

- Accesos remotos.
- Servicios en la nube.
- Cuentas privilegiadas.
- Sistemas críticos.

6.7. REGLAS.

Reglas obligatorias para el uso, administración y control de contraseñas en la operación diaria de los sistemas de información de la Gobernación de Nariño.

6.7.1. ASIGNACIÓN Y ACTIVACIÓN DE CUENTAS

- Toda cuenta de usuario deberá estar asociada a una persona identificable o a un servicio autorizado.
- La creación de cuentas requerirá solicitud formal y autorización del jefe inmediato o supervisor del contrato.
- Las contraseñas iniciales deberán ser temporales y forzar el cambio en el primer inicio de sesión.
- Está prohibido el uso de cuentas genéricas o compartidas, salvo aquellas técnicamente justificadas y debidamente autorizadas.

6.7.2. USO ACEPTABLE DE CONTRASEÑAS

- Las contraseñas son de uso personal e intransferible.
- No está permitido compartir contraseñas con otros usuarios, superiores jerárquicos, personal de TI o terceros.
- Ningún funcionario o contratista está autorizado a solicitar la contraseña de otro usuario.
- Las actividades realizadas con una cuenta de usuario serán responsabilidad del titular de la cuenta.

6.7.3. ALMACENAMIENTO Y PROTECCIÓN DE CONTRASEÑAS

- Está prohibido almacenar contraseñas en texto plano, archivos sin cifrar o medios inseguros.
- No se permite el uso de notas adhesivas, libretas o documentos visibles para almacenar contraseñas.
- El uso de gestores de contraseñas solo será permitido cuando estos cuenten con cifrado fuerte y sean autorizados por el área de TI.

6.7.4. CAMBIO, SUSPENSIÓN Y REVOCACIÓN

- Las contraseñas deberán cambiarse conforme a la vigencia definida en esta guía.
- Las cuentas deberán ser suspendidas inmediatamente cuando:
  - El usuario finalice su vínculo laboral o contractual.
  - Exista sospecha de compromiso de credenciales.
  - Se detecten accesos no autorizados o comportamientos anómalos.
- La revocación de accesos deberá realizarse como máximo dentro de las **24 horas** siguientes al retiro del usuario.

6.7.5. ACCESOS REMOTOS Y FUERA DE LAS INSTALACIONES

- Todo acceso remoto deberá realizarse mediante mecanismos seguros autorizados (VPN, MFA).
- Está prohibido el acceso a sistemas institucionales desde equipos públicos o no confiables.
- Los dispositivos utilizados para acceso remoto deberán cumplir con los controles mínimos de seguridad definidos por la entidad.

6.7.6. INCIDENTES Y EXCEPCIONES OPERATIVAS

- Todo incidente relacionado con contraseñas deberá ser reportado de forma inmediata.
- Las excepciones a estas políticas deberán estar debidamente justificadas, documentadas y aprobadas por el responsable de Seguridad de la Información.
- Las excepciones tendrán carácter temporal y estarán sujetas a revisión periódica.

6.7.7. CONTROLES TÉCNICOS ESPECÍFICOS.

Indicadores de cumplimiento MSPI

Con el fin de medir la efectividad de la gestión de contraseñas, se establecen los siguientes indicadores de desempeño en el marco del MSPI:

a. Indicadores de implementación

- Porcentaje de sistemas con política de contraseñas configurada
  Fórmula: (Sistemas con política / Total de sistemas) x 100
- Porcentaje de usuarios con MFA habilitado
  Fórmula: (Usuarios con MFA / Total de usuarios) x 100
- Porcentaje de cuentas privilegiadas gestionadas conforme a la guía
  Fórmula: (Cuentas privilegiadas controladas / Total cuentas privilegiadas) x 100

b. Indicadores de cumplimiento

- Porcentaje de usuarios que cambian su contraseña dentro del periodo establecido
- Número de incidentes relacionados con contraseñas comprometidas
- Porcentaje de bloqueos de cuenta gestionados oportunamente

c. Indicadores de mejora continua

- Reducción anual de incidentes por uso indebido de credenciales
- Porcentaje de usuarios capacitados en gestión segura de contraseñas

6.8. SEGUIMIENTO Y CONTROL

Los resultados de la aplicación de la guía de gestión de contraseñas serán revisados por el equipo operativo de seguridad digital de la Secretaría TIC y socializados al equipo de seguridad y gobierno digital liderado por la Secretaría TIC de la entidad, con el fin de:

- Analizar avances y dificultades
- Definir acciones correctivas.

7. DOCUMENTOS Y REGISTROS RELACIONADOS.

Guía de implementación MSPI MinTIC.

8. REFERENCIAS BIBLIOGRÁFICAS.

Guía de implementación MSPI MinTIC.
https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

9. ANEXOS.

NA

10. CONTROL DE CAMBIOS.

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

11. RESPONSABLE.

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

12. 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