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 protección de la información es un pilar fundamental dentro de la Gobernación de Nariño, dado que la entidad administra datos sensibles, estratégicos y personales de ciudadanos, funcionarios y actores institucionales. En el marco de la seguridad digital y del Modelo de Seguridad y Privacidad de la Información (MSPI), se hace necesario adoptar prácticas que reduzcan riesgos asociados a la exposición, pérdida o divulgación indebida de información.

La implementación de las prácticas de Pantalla Limpia y Escritorio Limpio busca fortalecer la cultura de seguridad de la información, promoviendo comportamientos responsables que garanticen la confidencialidad, integridad y disponibilidad de los activos de información tanto en medios físicos como digitales. Este documento establece los lineamientos obligatorios que deben cumplir todos los usuarios que acceden a la infraestructura tecnológica y documental de la Gobernación de Nariño.

4. Objetivo.

Establecer los lineamientos para la implementación y cumplimiento de prácticas de Pantalla y Escritorio Limpio en la Gobernación de Nariño, con el fin de minimizar riesgos de acceso no autorizado, fuga de información, manipulación indebida y exposición de activos de información.

5. Alcance.

Esta política aplica a todos los funcionarios públicos, contratistas, pasantes, proveedores y terceros que tengan acceso a información, sistemas, dispositivos o instalaciones de la Gobernación de Nariño.

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. 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.

- **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.

- **Escritorio limpio:** medidas para mantener el espacio físico libre de documentos, dispositivos o elementos con información sensible cuando no están en uso.

- 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.

- **Pantalla limpia:** práctica de bloquear, cerrar o proteger el acceso visual y operativo a la información en pantalla cuando el usuario se ausente.

- **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. 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 603 de 2000
- Ley 1266 de 2008
- La Ley 1273 de 2009
- Ley 1581 de 2012
- Decreto 1377 de 2013
- 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. LINEAMIENTOS GENERALES

8.1.1. Pantalla Limpia

- Bloquear el computador al retirarse del puesto de trabajo, incluso por lapsos breves.
- Mantener contraseñas confidenciales y no compartirlas.
- Evitar dejar sistemas o documentos digitales abiertos cuando no estén en uso.
- Usar salvapantallas con bloqueo automático.
- No utilizar notas adhesivas con contraseñas visibles.
- Aplicar filtros de privacidad cuando sea necesario.

8.1.2. Escritorio Limpio

- Guardar documentos físicos con información institucional en archivadores o cajones con llave.
- No dejar carpetas, expedientes o medios de almacenamiento a la vista.
- Mantener el área organizada y libre de elementos innecesarios.
- Resguardar dispositivos móviles y medios extraíbles (lugares seguros bajo llave).
- Utilizar métodos seguros de destrucción de documentos.
- Configurar la impresión segura cuando aplique.

8.2. REQUISITIOS MÍNIMOS

8.2.1. Requisitos mínimos de escritorio limpio (físico)

a) Documentos en papel

- No dejar documentos con información sensible en el escritorio cuando el puesto esté desatendido.
- Archivar documentos en muebles con cierre o en áreas designadas al terminar su uso.
- Utilizar carpetas cerradas o cajas bajo llave para expedientes en uso por tiempo limitado.
- No dejar impresiones con información personal o sensible en impresoras compartidas; recogerlas inmediatamente.
- Realizar la transferencia de documentos a archivo departamental de manera oportuna según los lineamientos establecidos por dicha dependencia.
- Evitar colocar recipientes con comida o líquido cerca a los documentos, que pueda derramarse y ocasionar la pérdida o distorsión de la información.

b) Equipos Informáticos.

- Evitar colocar recipientes con comida o liquido cerca a los equipos informáticos (computadores, teclado, mouse, impresoras, escáner, etc.) que pueda derramarse y ocasionar la pérdida o daño de los equipos.
- Ubicar los equipos informáticos en un lugar adecuado y con el espacio suficiente para su conservación sin riesgos de caídas que puedan traer pérdida total o parcial de los mismos.

c) Medios extraíbles

- Evitar el uso de USB y medios extraíbles no autorizados.
- Cuando se usen, registrarlos y cifrarlos. Al terminar, guardarlos en lugar seguro o eliminarlos según procedimiento establecido por la Secretaría TIC.

d) Dispositivos personales y equipos no gestionados

- Está prohibido conectar equipos personales no autorizados a la red o activos de la entidad sin autorización formal (jefe inmediato y Secretaría TIC)
- Los teléfonos y dispositivos personales deben guardarse adecuadamente y no contener copias no autorizadas de información institucional.

e) Elementos visibles en el escritorio

- No exhibir listas de contraseñas, notas con datos confidenciales y/o sensibles o pantallas impresas a la vista de visitantes.
- Mantener solo los elementos necesarios para la tarea del día.

8.2.2. Requisitos mínimos de pantalla limpia (digital)

a) Bloqueo de sesión

- Configurar el bloqueo automático de pantalla con un tiempo máximo de inactividad de 2 minutos (tiempo establecido por Secretaría TIC).
- Bloquear manualmente la pantalla siempre que el usuario se ausente del puesto de trabajo.

b) Gestión de sesiones y acceso remoto

- Cerrar las sesiones en sistemas de información, plataformas, aplicaciones o bases de datos cuando no estén en uso.
- No compartir sesiones ni credenciales.

c) Visualización de información

- Evitar abrir o mostrar información privada y/o sensible en monitores ubicados en áreas de tránsito o con visibilidad externa.

- Utilizar filtros de privacidad en pantallas donde haya riesgo de observación por terceros.

d) Uso de aplicaciones y ventanas

- Minimizar o cerrar ventanas con información privada y/o sensible si hay visitantes o reuniones informales.

e) Reuniones y pantallas compartidas

- Antes de compartir pantalla en videoconferencias, cerrar aplicaciones o pestañas que no sean estrictamente necesarias y ocultar notificaciones.
- Utilizar salas virtuales seguras y herramientas aprobadas por Secretaría TIC.

8.3. CONTROLES TÉCNICOS ASOCIADOS

8.3.1. Políticas y configuración en activos de Información de TI

a) Implementar bloqueo automático de estaciones de trabajo y dispositivos móviles.

b) Políticas de cifrado en dispositivos portátiles y medios extraíbles.

c) Gestión de parches y actualizaciones para prevenir vulnerabilidades que permitan el acceso no autorizado.

d) Implementación de equipos, software y reglas de seguridad para prevenir acceso no autorizado y detectar intentos de intrusión.

8.3.2. Monitoreo y registro

a) Habilitar registros de acceso y alertas frente a inicios de sesión inusuales o violaciones de políticas (a través de los equipos, software y reglas implementadas).

8.3.3. Control de acceso físico

a) Áreas con información clasificada, privada y sensible deben contar con control de acceso físico (tarjetas, cerraduras, registro de visitantes).

8.3.4. Gestión de impresión y destrucción segura

a) Políticas para recolección y destrucción de impresiones con información clasificada, privada y sensible (triturado o gestión documental segura). Procedimientos establecidos por Archivo.

8.3.5. Herramientas de administración de dispositivos

a) Uso de soluciones MDM/EMM para dispositivos móviles; control de inventario de activos.

8.4. FORMACIÓN, CONCIENTIZACIÓN Y COMUNICACIÓN

a) Capacitación inicial y periódica para todo el personal sobre principios y prácticas de Escritorio/Pantalla Limpia.
b) Campañas de sensibilización (publicaciones, pendones, correos, recordatorios) con ejemplos prácticos.
c) Inclusión de la política en inducción para nuevos empleados y cláusulas contractuales para contratistas.

8.5. PROCEDIMIENTOS OPERATIVOS (RESUMEN)

8.5.1. Procedimiento para ausentarse del puesto de trabajo

a) Guardar documentos sensibles.
b) Bloquear pantalla o cerrar sesión.
c) Guardar o asegurar dispositivos portátiles.

8.5.2. Procedimiento para reuniones con terceros/visitantes

a) Retirar o asegurar documentos; usar salas designadas.
b) No compartir contraseñas ni credenciales.

8.5.3. Procedimiento de impresión y recolección

a) Verificar cola de impresión y recoger inmediatamente.
b) Marcar documentos clasificados, privados y sensibles para gestión segura.

8.5.4. Procedimiento para uso de medios extraíbles

a) Solicitud previa cuando su uso es imprescindible; registro; cifrado; eliminación segura.

8.5.5. Procedimiento de reporte de incumplimiento o incidente

a) Informar de manera inmediata a la Secretaría TIC y Talento Humano según corresponda.
b) Documentar el incidente: fecha, hora, activos afectados, acciones realizadas, según procedimiento de gestión de incidentes de seguridad establecido por la Secretaría TIC.

8.6. 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.

Es necesario realizar auditorías internas periódicas para verificar cumplimiento en sedes y estaciones de trabajo, inspecciones aleatorias y chequeos programados por los jefes de área.

La Secretaría TIC debe aplicar indicadores de cumplimiento de implementación de MSPI.

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