# SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

**Versión 1.3-2014**

## Política de Seguridad y Privacidad de la Información de la Gobernación de Nariño.



*Elaborador por: New Technologie- San Juan de Pasto – Celular: 3014326374*

# INTRODUCCIÓN

La Entidad ha reconocido la información como uno de los activos más importantes de la organización, haciendo necesaria la protección de la misma frente a amenazas que puedan poner en peligro la continuidad de los niveles de competitividad, de gestión pública, y de conformidad legal necesarios para alcanzar las metas administrativas y del plan departamental de desarrollo Nariño Mejor 2012-2015.

Con la formulación de la presente Política de Seguridad de la Información, la Gobernación, materializa la gestión responsable de información que proyecta garantizar la integridad, confidencialidad y disponibilidad de este importante activo, teniendo como eje el cumplimiento de los objetivos y metas trazadas en la administración pública.

Esperamos que este contenido se convierta en un documento interno de trabajo que aporte al mejoramiento continuo, susceptible de complementos y nuevas versiones.

## Resolución No. 395 de Diciembre 11 de 2014.

Mediante la cual, La entidad aprobó la implementación del Sistema de Gestión de Seguridad de la Información en la Gobernación de Nariño, con base a la Norma ISO 27001-2013, decreto 2693 de 2012 y normatividad adicional vigente.

## Conceptos Básicos

La seguridad de la información se entiende como la preservación, aseguramiento y cumplimiento de las siguientes características de la información:

• Confidencialidad: Los activos de información solo pueden ser accedidos y custodiados por usuarios que cuente con permisos para ello.

• Integridad: El contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.

• Disponibilidad: Los activos de información sólo pueden ser obtenidos a corto plazo por los usuarios que cuenten con los permisos adecuados.

## Comité para la Seguridad de la Información.

La Gobernación de Nariño, proyecta la organización de la Seguridad de la información, por medio de la creación de una comisión técnica denominada Comité de Seguridad de la Información cuya composición y funciones serán reglamentadas por una mesa de trabajo compuesta por:

- Secretario de Gobierno o Líder GEL
- Secretaria General del Departamento.
- Subsecretaria Talento Humano
- Jefe Oficina de Control Interno de la Gestión
- Jefe Archivo General
- Oficina de Gestión Tecnológica.

Los integrantes del comité deberán revisar y actualizar anualmente la Política de Seguridad de la Información, presentando los proyectos o propuestas al Gobernador del Departamento para su aprobación mediante acto administrativo correspondiente.

L@s Secretari@s, Directores de departamento o Jefes de Dependencias u Oficinas, deben identificar y valorar los activos de información que pertencen a las respectivas áreas, y deben seguir los lineamientos de gestión enmarcados en esta política y en los estándares, normas, guías y procedimientos recomendados por el Comité de Seguridad de la Información y aprobados y adoptados por el Gobernador del Departamento.

## Política de Seguridad de la Información

La política de seguridad es un documento de alto nivel que denota el compromiso del Gobernador del Departamento con la seguridad de la información. Esta política contribuye a minimizar los riesgos asociados a daños, proyecta la eficiencia administrativa y asegura el cumplimiento de las funciones misionales de la entidad apoyadas en el uso adecuado de TICs.

## ALCANCE

Esta política es de aplicación en el conjunto de Secretarias, Departamentos, subsecretarias , oficias y dependencias que componen la Gobernación de Nariño, a sus recursos, a la totalidad de los procesos internos o externos vinculados a la Administración Pública a través de contratos o

convenios con terceros y a todo el personal de Gobernación, independiente de su tipo de vinculación, la dependencia a la cual se encuentre adscrito y el nivel de funciones o labores que ejecute.

## OBJETIVOS

a) Preservar, proteger y administrar de forma eficiente la información de la Gobernación de Nariño junto con las medios utilizados para la manipulación o procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de los características de confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

b) Mantener la Política de Seguridad de la Información actualizada, vigente, operativa y controlada, enmarcada en el tratamiento de los riesgos de la información de la Gobernación de Nariño, para asegurar la sostenibilidad de la misma y el nivel de eficacia.

## Responsabilidades asignadas

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de la Gobernación de Nariño, independiente del tipo de vinculación, el área o dependencia a la cual se encuentre adscrito y el nivel del cargo o funciones que desempeñe.

El Gobernador del Departamento de Nariño aprueba esta Política y es responsable de la aprobación y adopción de las actualizaciones.

El Comité de Seguridad de la Información de la entidad es responsable de revisar, proyectar y proponer a la administración departamental en cabeza del Gobernador, para su aprobación, el documento de la Política de Seguridad de la Información, las funciones generales en materia de seguridad de la información y la estructuración, recomendación, seguimiento y mejora continua del Sistema de Gestión de Seguridad de Información de la Gobernación de Nariño. Es responsabilidad de dicho comité definir las estrategias de capacitación en materia de seguridad de la información al interior de la Administración Departamental.

El Coordinador del Comité de Seguridad de la Información será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la socialización, implementación, seguimiento y control de la política.

Los propietarios de activos de la información, son responsables de la clasificación, mantenimiento, actualización y valoración de la misma; así como de documentar y mantener actualizada la clasificación efectuada, definiendo el perfil de los usuarios, y el nivel de permisos de acceso a la información de acuerdo a sus cargos, funciones y competencias. Tienen la responsabilidad de mantener de forma íntegral, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.

Quien ejerza el cargo de Subsecretari@ de Talento Humano, deberá notificar a todo el personal que se vincule con la Gobernación de Nariño, el detalle de las obligaciones respecto al cumplimiento de la Política de Seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas , guías y lineamientos que surjan del Sistema de Gestión de la Seguridad de la Información. De igual forma, será responsable de la notificación y socialización de la presente Política y de los cambios o actualizaciones que en ella se produzcan a todo el

personal, a través de la suscripción de los acuerdos de Confidencialidad y de labores de capacitación continua en materia de seguridad según los lineamientos establecidos por el Comité de Seguridad de la Información de la Entidad.

Los profesionales universitarios y equipo de trabajo de la Oficina de Gestión Tecnológica en coordinación con la Secretaría General del Departamento deben seguir los lineamientos de la presente política y cumplir los requerimientos que en materia de seguridad informática se establezcan para la operación, administración, comunicación y mantenimiento de los sistemas de información e infraestructura tecnológica de la Entidad.

El Archivo General del Departamento en colaboración con la oficina de Gestión tecnológica determinaran el inventario de activos de información y recursos tecnológicos de los cuales son propietarios o custodios, el cual será revisado y avalado por el Almacén General del Departamento en responsabilidad de los respectivos líderes.

Quien ejerza el cargo de Director@ del Departamento Administrativo de Contratación verificará que los contratos, convenios u otra documentación de la entidad con servidores públicos y con terceros incluya los lineamientos de la Política de Seguridad de la Información de la Entidad.

Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer y cumplir la Política de Seguridad de la Información vigente.

La Oficina de Control Interno de la Gestión, es responsable de realizar seguimiento y control periódico sobre información contenida en documentos, sistemas de información y/o actividades vinculadas con la gestión de activos de información. Es responsabilidad de esta área informar sobre el cumplimiento de los lineamientos y medidas de seguridad de la información establecidas por esta Política, y normas adicionales vigentes.

## Identificación, clasificación y valoración de activos de información.

Cada área o dependencia de la Entidad, bajo supervisión del Comité de Seguridad de la Información, y con base en el inventario de activos de la información, entregado por la empresa NEW TECHNOLOGIE debe mantener un inventario de los activos de información con la que se cuenta, ya sea procesada y producida. La forma y medios en donde se incorpore la clasificación, valoración, ubicación y acceso de la información, las especifica el Comité de Seguridad de la Información, correspondiendo a la Oficina de gestión tecnológica brindar herramientas que permitan la administración eficiente del inventario por cada área o dependencia, garantizando la disponibilidad, integridad y confidencialidad de los datos.

## Seguridad de la información en el Talento Humano

Todas y todos los servidores públicos de la Gobernación de Nariño, independiente del tipo de vinculación laboral o contractual, la dependencia o área a la cual se encuentre adscrito y el nivel de funciones, tareas o actividades que desempeñe debe contar con un perfil de uso de los recursos de información, incluyendo el hardware y software asociado. La oficina de Gestión Tecnológica debe mantener un directorio completo y actualizado de los perfiles creados.

El Comité de Seguridad de la Información determina cuales son los atributos que deben definirse para los diferentes perfiles.

El Comité de Seguridad de la Información debe elaborar, mantener, actualizar, mejorar y difundir el manual de "Responsabilidades Personales para la Seguridad de la Información en la Gobernación de Nariño".

La responsabilidad de custodia de cualquier documento o archivo mantenido, usado o producido por el personal que se retira, o cambia de cargo, recae en el jefe de departamento, secretaría o dependencia o supervisor del contrato; en todo caso el proceso de cambio en la cadena de custodia de la información debe hacer parte integral del procedimiento de terminación de la relación contractual o de cambio de cargo.

## Asuntos Operacionales y de Manejo

Para que las Políticas y estándares de seguridad sean efectivos, la Gobernación de Nariño debe utilizar métodos de trabajo, prácticas de negocios y procedimientos en el contexto de cumplir con las estrategias de la organización. Por lo tanto hay algunos asuntos como el control de cambios y la documentación de sistemas, procedimientos y estructura organizacional, que aunque no están relacionados directamente con la seguridad de la información, deben ser establecidos e implementados para proveer una protección adecuada de los activos de la información de la Entidad.

## Responsabilidades del personal de la Gobernación

Todas y todos los servidores públicos de la Gobernación de Nariño, independiente del tipo de vinculación laboral o contractual, departamento, secretaría o dependencia, a la cual se encuentre adscrito y las tareas o labores que desempeñe debe suscribir un acuerdo que contenga los términos y condiciones que regulan el uso de recursos de TI y las reglas y perfiles que autorizan el uso de la información institucional.

Los procedimientos para obtener los respectivos perfiles y las características de cada uno de ellos deben ser mantenidos y actualizados por cada departamento, secretaría o dependencia, de acuerdo a los lineamientos establecidos por la oficina de Gestión Tecnológica de la Entidad, en cuanto a los dispositivos de hardware y los elementos de software.

La Subsecretaria de Talento humano, en coordinación con la Oficina de gestión tecnológica se encargarán de crear, actualizar, mantener y ejecutar un plan de capacitación en seguridad de la información que proyecte la socialización y concientización individual y colectiva en temas de seguridad de la información en todo el personal.

La Oficina de gestión tecnológica deberá publicar en medios impresos y virtuales como intranet, correo electrónico, entre otros, información relacionada con temas de seguridad de la información tales como responsabilidad en la administración de documentos, archivos, buenas prácticas, amenazas de seguridad, entre otros.

## Responsabilidades de Usuarios Externos

Los usuarios externos y personal de organizaciones o empresas externas, deben estar autorizados por una persona designada en la Gobernación de Nariño quien será responsable del control y vigilancia en el uso adecuado de los accesos a la información y propender por la buena utilización de recursos tecnológicos si le son facilitados . Los procedimientos para el registro y control de dichos usuarios debe ser diseñado, implementado y mantenido por la Oficina de gestión en Tics, en coordinación con la sección de atención a la ciudadanía.

Los dueños de los activos de la información se encargaran en orientar a los usuarios externos autorizados para que hagan adecuado uso de la información y componentes tecnológicos facilitados.

Todos los usuarios externos sin excepción deben aceptar por escrito los términos y condiciones de uso de la información y recursos TICs institucionales. Las cuentas de usuarios externos deben ser de perfiles específicos y tener caducidad no superior a dos (2) meses, renovables de acuerdo a la naturaleza del usuario.

## Usuarios invitados y servicios de acceso público.

El acceso de usuarios no registrados solo debe ser permitido al sitio web, a modo de información institucional o interacción y transacción como ciudadanos, igualmente el servicio de internet al que puedan acceder debe estar protegido con contraseña pública, pero se debe contar con restricción de sitios web no autorizados y limites en la capacidad de ancho de banda. Si los usuarios invitados no surtieron el proceso de registro, no se permite el acceso a cualquier otro tipo de recursos de información, aplicación y/o herramientas TICs.

## Seguridad Física y del entorno

Se debe tener acceso controlado y restringido al datacenter y cuartos de comunicaciones principales. La Oficina de gestión en TICs elaborarán y mantendrán las normas, controles y registros de acceso a dichas áreas.

Seguridad en los equipos:

Los servidores que contengan información y servicios institucionales deben ser mantenidos en un ambiente seguro y protegido por lo menos con:

• Controles de acceso y seguridad física.

• Detección de incendio y sistemas de extinción de conflagraciones.

• Controles de humedad y temperatura.

• Bajo riesgo de inundación.

• Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

Toda información institucional en formato digital debe ser mantenida en servidores aprobados por la Oficina de Gestión en TICs. No se permite el alojamiento de información institucional en

servidores externos sin respectiva aprobación escrita del comité de seguridad de la información de la Entidad.

Los equipos importantes de comunicaciones deben ser alimentados por sistemas de potencia eléctrica regulados y estar protegidos por UPS.

La oficina de Gestión de TICs, debe asegurar que la infraestructura a red de datos de área local este cubierta por mantenimiento y soporte adecuados tanto para hardware como para software.

Las estaciones de trabajo deben estar correctamente aseguradas y operadas por personal de la institución el cual debe estar capacitado acerca del contenido de esta política y de las responsabilidades personales en el uso y administración de la información institucional.

Los medios que alojan copias de seguridad deben ser conservados de forma correcta de acuerdo a las políticas y estándares que para tal efecto elabore y mantenga el Comité de Seguridad en la Información.

Las dependencias tienen la responsabilidad de adoptar y cumplir las normas definidas para la creación y el manejo de copias de seguridad.

# Administración de las comunicaciones y operaciones

## Reporte y revisión de incidentes de seguridad

El personal vinculado a la Gobernación de Nariño, debe reportar con diligencia, eficiencia y responsabilidad presuntas violaciones de seguridad a través de su jefe de dependencia a la Oficina de Gestión en TICs. Cuando la ocasión lo amerite y existan casos especiales dichos reportes podrán realizarse directamente por la persona que encuentre el incidente o novedad. La oficina de gestión en TICs , debe garantizar las herramientas informáticas para que se realicen tales reportes.

El Comité de Seguridad de la Información debe diseñar, mantener y difundir las normas, procesos y guías para el reporte y revisión de incidentes de seguridad.

En conformidad con la ley, la Gobernación de Nariño podrá interceptar o realizar seguimiento a las comunicaciones por diferentes mecanismos previa autorización del Comité de seguridad de la información, y en todo caso notificando previamente a los afectados por esta decisión.

La Oficina de Gestión de TICs mantendrá procedimientos escritos para la operación de sistemas de información cuya no disponibilidad suponga un impacto alto en el desarrollo normal de actividades o afecte la continuidad del negocio. Se debe realizar seguimiento a los procedimientos establecidos para asegurar la confiabilidad del servicio que prestan.

# Protección contra software malicioso y hacking.

Se debe proteger todos los sistemas de información teniendo en cuenta un enfoque multi-nivel que involucre controles humanos, físicos técnicos y administrativos. El Comité de Seguridad de la Información elaborará y mantendrá un conjunto de políticas, normas, estándares, procedimientos y guías que garanticen la mitigación de riesgos asociados a amenazas de software malicioso y técnicas de hacking.

Como control básico, todas las estaciones de trabajo de la Gobernación de Nariño, edificio central y sedes externas deben estar protegidas por software antivirus con arquitectura cliente-servidor, con capacidad de actualización automática en cuanto a firmas de virus. Los usuarios de la estaciones no están autorizados a deshabilitar este control.

Es deber de la Oficina de Gestión en TICs, hacer seguimiento al tráfico de la red de área local, cuando se tenga evidencias de actividad inusual o detrimentos en el desempeño.

El área encargada deben mantener actualizada una base de datos con alertas de seguridad reportadas por organismos competentes y actuar en conformidad cuando una alerta pueda tener un impacto considerable en el desempeño de los sistemas de información, aplicaciones y software en general.

## Copias de Seguridad

Toda información que se encuentre contenida en el inventario de activos de información institucional o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada con copias de seguridad tomadas de acuerdo a los procedimientos documentados por el Comité de Seguridad de la Información. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en lugares seguros.

Los registros de copias de seguridad deberán almacenarse en una base de datos creada para tal fin. El comité debe definir el procedimiento de copia de seguridad, administración y custodia de los backups. La Oficina de Gestión en TICs debe proveer las herramientas para que las dependencias puedan consultar la bitácora de la información y registros de copias de seguridad. La Oficina de Control Interno debe efectuar auditorías aleatorias que permitan determinar el correcto funcionamiento de los procesos de copia de seguridad.

Las actividades de copias de seguridad de información crítica debe ser ejecutada y mantenida de acuerdo a cronogramas definidos y publicados por el área encargada.

La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios, es decir La responsabilidad de realizar las copias y mantener actualizadas las mismas, recae directamente sobre cada dueño del activo de la información en la Entidad. Los usuarios deben entregar al respectivo jefe de dependencia las copias de seguridad para su registro y custodia. Se debe facilitar los medios para realizar dichas actividades, sin que esto genere responsabilidad a la oficina de Gestión de Tics.

## Administración de redes de área local.

La configuración de terminales de red, enrutadores, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red; debe ser documentada, respaldada por copia de seguridad y mantenida por la oficina de Gestión de Tics en la Entidad.

Todo equipo tecnológico debe ser revisado, registrado y aprobado por la oficina de Gestión en Tics, antes de conectarse a cualquier nodo de la Red de comunicaciones y datos institucional. Dicha dependencia debe desconectar aquellos dispositivos que no estén aprobados y reportar tal conexión como un incidente de seguridad para ser analizado e investigado.

## Intercambio de Información con Entidades Externas.

Las peticiones de información por parte de entes externos deben ser aprobadas por la oficina de Control Interno de la Gestión, y redireccionados a los responsables del manejo y custodia .

Las peticiones de información por parte de entes externos debe ser realizada por un medio valido que permita el registro de la solicitud, donde debe identificarse, el remitente, el asunto y la fecha. T

oda la información institucional debe ser manejada de acuerdo a la legislación colombiana, normatividad vigente.

## Internet y Correo Electrónico Y Sistemas de información automatizados

Las normas de uso de Intranet, Internet, antivirus, sistemas operativos, sistemas de información automatizados, paquetes ofimáticos y de los servicios de correo electrónico serán elaboradas, mantenidas y actualizadas por el Comité de Seguridad de la Información y en todo caso este comité debe velar por el cumplimiento del código de ética institucional y el manejo responsable de los recursos de tecnologías de la información y las comunicaciones.

## Instalación de Software

Todas las instalaciones de software que se realicen sobre sistemas operativos previamente instalados en la Gobernación de Nariño, deben ser aprobadas por la Oficina de Gestión en TICs de acuerdo a los procedimientos elaborados para tal fin .

No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor en especial la ley 23 de 1982 y relacionadas. La Oficina de Gestión en TICs debe desinstalar cualquier software ilegal y registrar este hecho como un incidente de seguridad que debe ser investigado.

Corresponde a la Oficina de Gestión en TICs, mantener una base de datos actualizada que contenga un inventario del software autorizado para su uso e instalación en los sistemas informáticos institucionales.

## Control de Acceso

### Categorías de Acceso

El acceso a los recursos de tecnologías de información institucionales deben estar restringidos según los perfiles de usuario definidos por el Comité de Seguridad de la Información.

### Control de Claves y Nombres de Usuario

El acceso a información restringida debe estar controlado. Se recomienda el uso de sistemas automatizados de autenticación que manejen credenciales o firmas electrónicas.

Corresponde a la Oficina de Gestión en TICs elaborar, mantener y publicar los documentos de servicios de red que ofrece la institución a sus funcionarios, ciudadanía y terceros. Adicionalmente debe elaborar, mantener y publicar procedimientos de administración de cuentas de usuario para el uso de servicios de red.

El acceso a sistemas de cómputo y los datos que contienen es responsabilidad exclusiva del personal encargado de tales aplicativos o sistemas de información.

La Gobernación de Nariño debe propender por mantener al mínimo la cantidad de cuentas de usuario que los funcionarios y terceros deben poseer para acceder a los servicios de red.

El control de acceso a los dispositivos intermedios de red es responsabilidad de la Oficina de Gestión en TICs. Dichas contraseñas deben ser codificadas o encriptadas y almacenadas de forma segura.

Las claves de administrador de los diferentes sistemas deben ser conservadas por la coordinación de la Oficina de Gestión de TICs y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie.

Adicionalmente la oficina de gestión en Tics debe elaborar, mantener y actualizar el procedimiento y las guías para la correcta definición, uso y complejidad de claves de usuario.

Una vez se termine la relación contractual o laboral del personal con la Gobernación de Nariño, la oficina de gestión en TICs, debe expedir un certificado de suspensión y/o cancelación de las cuentas creadas al respectivo usuario, en todos y cada uno de los sistemas de información en los cuales estuviera activo (intranet, correo electrónico, sistemas de información automatizados, entre otros) durante un tiempo prudencial por la posible renovación de la relación contractual o laboral, una vez transcurrido el tiempo se dará de baja las cuentas si no hay renovación.

## Computación Móvil

La Gobernación de Nariño, en cabeza de la Oficina de gestión en TICs debe reconocer el alto grado de exposición que presenta la información y los datos almacenados en dispositivos portátiles (computadores portátiles, notebooks, PDA, celulares, etc). Con base a lo anterior, corresponde a la Subsecretaria de Talento Humano en conjunto con la Oficina de gestión en TICs elaborar, mantener e implementar planes de capacitación que propendan por la formación y mantenimiento de la conciencia en cuestión de seguridad de la información.

Las redes inalámbricas potencialmente introducen nuevos riesgos de seguridad que deben ser identificados, valorados y tratados de acuerdo a los lineamientos de la Política de Seguridad en redes inalámbricas que debe elaborar el Comité de Seguridad de la Información..

## Auditoria y Seguimiento

Todo uso que se haga de los recursos de tecnologías de la información en la Gobernación de Nariño deben ser seguidos y auditados de acuerdo con los lineamientos establecidos por la Oficina de Gestión en TICs

## Acceso Remoto

El acceso remoto a servicios de red ofrecidos por la Gobernación de Nariño debe estar sujeto a medidas de control definidas por el comité de seguridad de la información las cuales deben incluir acuerdos escritos de seguridad de la información.

## Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.

### Software

Para apoyar los procesos misionales y estratégicos la Gobernación de Nariño debe hacer uso intensivo de las Tecnologías de la Información y las Comunicaciones. Los sistemas de software utilizados pueden ser adquiridos a través de terceras partes o desarrollados por personal vinculado a la Gobernación de Nariño.

La Oficina de gestión en TICs debe, elaborar, mantener y difundir el " La Metodología de Desarrollo de Sistemas Software en la Gobernación de Nariño" que incluya lineamientos, procesos, buenas prácticas, plantillas y demás artefactos que sirvan para regular los desarrollos de software internos en un ambiente de mitigación del riesgo y aseguramiento de la calidad.

Todo proyecto de desarrollo de software interno debe contar con un documento de Identificación y Valoración de Riesgos del proyecto. La Gobernación de Nariño no debe emprender procesos de desarrollo – o mantenimiento – de sistemas software que tengan asociados riesgos altos no mitigados.

Los sistemas software adquiridos a través de terceras partes deben certificar el cumplimiento de estándares de calidad en el proceso de desarrollo y la integración con la platafomrma tecnológica existente en la entidad.

## Administración de Continuidad del Negocio

La Administración de Continuidad del Negocio debe ser parte integral del Plan de Administración de Riesgos de la Gobernación de Nariño

## Cumplimiento

Todo uso y seguimiento adecuado en el uso de los recursos de Tecnologías de la Información y las comunicaciones en la Entidad, debe estar de acuerdo a las normas y estatutos internos así como a la legislación nacional y normatividad vigente, incluyendo la resolución 266 de 30 de Septiembre de 2013 , por medio de la cual se regula el soporte tecnológico, compra de hardware y adquisición y/o desarrollo de software en la Gobernación de Nariño.

# REFERENCIAS


- Ley 527-1999 Ley de comercio electrónico.
- NTC- ISO-IEC -27001:2013. Sistema de Gestión de la Seguridad de la Información.
- Política para la Seguridad de la Información de la Universidad Distrital Francisco José de Caldas
- Manual de Procesos y Procedimientos de la Entidad -2008.