TABLA DE CONTENIDO

1. INTRODUCCIÓN.

La Información es algo intangible que se produce, almacena, distribuye y se procesa, convirtiéndose en un activo vital para el buen funcionamiento y mejoramiento de la Gobernación de Nariño, de ahí que es necesario contar con procesos, políticas y lineamientos que permitan gestionar de manera adecuada y oportuna la seguridad de la información.

La política General de Seguridad y Privacidad de la Información expresa la voluntad por parte de la Dirección de la Gobernación de Nariño, de apoyar la implementación de un Sistema de Gestión de Seguridad y Privacidad de la información SGSI el cual debe ser de obligatorio cumplimiento para lograr los objetivos de protección de los activos de la información identificados y clasificados por parte de la entidad.

2. JUSTIFICACIÓN.

Día a día nos encontramos con amenazas que pueden explotar las vulnerabilidades que tenemos y poner en riesgo la estabilidad de la entidad, enfrentándola a consecuencias muy graves que pueden afectar la estabilidad financiera, legal y de imagen o reputación.

Es por esta razón que es necesario iniciar un proceso de implementación de controles de seguridad de la información a través de un modelo de Gestión de Seguridad y privacidad de la información que nos permita evitar la materialización de riesgos y en todo caso reducir el impacto de los mismos.

La política General de Seguridad de la Información es la base para dar inicio al proceso de implementación del Sistema de Gestión de Seguridad y Privacidad de la Información, según las necesidades de la entidad y cumpliendo con las normas relacionadas y lineamientos vigentes.

3. OBJETIVOS.

3.1. GENERAL

Implementar un Sistema de Gestión de Seguridad y Privacidad de la Información, que permita proteger los activos de la información y asegure el correcto tratamiento de riesgos de la información identificados en la Gobernación de Nariño.

3.2. ESPECIFICOS

- Generar políticas específicas, procedimientos y lineamientos que apoyen la implementación de herramientas tecnológicas de prevención.
- Propender por una cultura de concientización de seguridad de la información en todos los niveles de la entidad, a fin de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y disponibilidad de la información.

- Asegurar la continuidad del servicio y minimizar el impacto causado por los riesgos identificados, logrando así mantener la confianza y responder frente a las necesidades de sus diferentes grupos de interés.
- Cumplir con la normatividad vigente, el direccionamiento estratégico y la mejora continua, a través de la medición de la efectividad de los controles del Sistema de Gestión de Seguridad y Privacidad de la Información.
- Salvaguardar la tecnología utilizada para el procesamiento de información frente a amenazas internas o externas, deliberadas o accidentales.

4. ALCANCE.

La política de seguridad y privacidad de la información aplica a todos los procesos y servicios de la entidad, para todos los funcionarios, contratistas, proveedores, usuarios externos y demás partes interesadas, que en ejercicio de sus funciones o en uso de los servicios de la entidad creen, procesen, almacenen o compartan información.

5. DEFINICIÓNES.

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: Es el mecanismo mediante el cual regulamos los aspectos relativos a la seguridad de la información en una prestación de servicios, acorde a las funciones a desempeñar en la entidad.

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.

AUTENTICIDAD: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidad.

BACKUP DE INFORMACIÓN: Se refiere a la copia y archivo de datos de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos.

CONFIDENCIALIDAD: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.

DATACENTER: Se denomina también Centro de Procesamiento de Datos (CPD) a aquella ubicación o espacio donde se concentran los recursos necesarios (TI) para el procesamiento de la información de una organización.

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.

DECLARACIÓN DE APLICABILIDAD: Documento que describe los objetivos de control y los controles pertinentes y aplicables para el mismo.

DISPONIBILIDAD: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando esta así lo requiera.

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.

CUSTODIO: Es una parte designada de la entidad, un cargo o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación de privilegios de acceso, modificación y borrado.

IMPACTO: Resultado de un incidente de seguridad de la información.

INCIDENTE DE SEGURIDAD DE LA INFORMACION: Ocurrencia de uno o varios eventos que atentan contra la confidencialidad, la integridad y la disponibilidad de la información y que violan la Política de Seguridad de la Información de la organización.

INTEGRIDAD: Propiedad de salvaguardar la exactitud y estado completo de los activos.

MEJOR PRÁCTICA: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

NO REPUDIO: El emisor no puede negar que envió porque el destinatario tiene pruebas del envío. El receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor pueda negar tal envío.

PARTES INTERESADAS: Persona u organización que puede afectar o ser afectada o percibirse a sí misma como afectada por una decisión o actividad.

PLAN DE SENSIBILIZACIÓN: Es un proceso que involucra actividades, divulgación de información, estrategias audiovisuales y prácticas, para impactar a las partes interesadas sobre su comportamiento y/o reforzar en aplicación de buenas prácticas sobre seguridad de la información.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN: Declaración de alto nivel que describe los objetivos y posición de la entidad frente a la Seguridad de la información.

PROPIETARIO / RESPONSABLE DE LA INFORMACIÓN: Individuo, entidad o dependencia que tienen bajo su responsabilidad la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información. Los propietarios de la información deben garantizar la seguridad, integridad, disponibilidad y confidencialidad de la información y deben coordinar la implementación de políticas con otros propietarios de información y con propietarios de infraestructura. Los propietarios deben especificar cómo se debe utilizar la información y como se debe proteger, además de definir cómo se administrarán los procedimientos de control y cómo se aplicarán los niveles apropiados de protección para la información acorde con su clasificación.

PROPIETARIOS DE INFRAESTRUCTURA: Administradores de recursos tecnológicos utilizados para el manejo y/o administración de la información. Son responsables por la funcionalidad, operación, continuidad, manejo y uso de todos los sistemas compartidos, las redes, el soporte y el mantenimiento, el software estándar, los sistemas telefónicos y de comunicaciones, y los servicios relacionados. Los propietarios de infraestructura son responsables de coordinar los servicios de recuperación de los elementos de tecnología informática y de implementar y manejar efectivamente las funciones y procedimientos de seguridad para cumplir con las necesidades de los propietarios de la información y de la Entidad.

RIESGO: Es la probabilidad que un incidente o evento adverso ocurra para causar una pérdida o daño en un activo de información.

SEGURIDAD DE LA INFORMACIÓN: Conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

TERCEROS: Toda persona, jurídica o natural, como proveedores, contratistas o consultores, que provean servicios o productos a la Entidad.

TRATAMIENTO DE RIESGOS: A partir del riesgo definido, se aplican los controles con los cuales se busca que el riesgo no se materialice.

USUARIOS: Personas que, directa o indirectamente, tengan algún tipo de relación con la Entidad y/o que tengan acceso a los recursos tecnológicos de la Entidad

VULNERABILIDAD: Es una debilidad del sistema informático que puede ser utilizada 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.

6. NIVEL DE CUMPLIMIENTO.

La entidad se compromete a cumplir con la normatividad legal vigente y las políticas establecidas en materia de seguridad y privacidad de la información.

Para ello, se establecerán mecanismos de seguimiento y evaluación periódica del cumplimiento de la política y se promoverá una cultura de seguridad y privacidad de la información en la entidad.

7. MARCO NORMATIVO.

- Ley No 599 de 2000 - Código penal: Título VII BIS, de los atentados contra la Confidencialidad, la Integridad y la Disponibilidad de los datos y los Sistemas Informáticos.
- Ley Estatutaria 1266 De 2008 – “Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”.
- La Ley 1273 de 2009 – “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

- Artículo 1 - Adicionase el Código Penal con un título VII bis denominado "de la Protección de la Información y de los Datos.

  Artículo 269ª - Acceso abusivo a un sistema informático.
  Artículo 269C - Interceptación de datos informáticos.
  Artículo 269D - Daño informático.
  Articulo 269F - Violación de Datos Personales.
  Articulo 269H - Circunstancias de Agravación Punitiva.

- Ley Estatutaria 1581 De 2012 – "Por la cual se dictan disposiciones generales para la protección de datos personales".
- Decreto 1377 De 2013 – "Tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales".
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1008 de 2018, "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones
- Documento CONPES 3854, Política Nacional de Seguridad Digital
- Documento CONPES 3975, Política Nacional para la Transformación Digital e Inteligencia Artificial, del 8 de noviembre de 2019. El Consejo Nacional de Política Económica y social (CONPES)
- Norma NTC-ISO-IEC 27001:2013

8. POLITICA SEGURIDAD DE LA INFORMACIÓN.

La Gobernación de Nariño, comprometida con sus usuarios, la comunidad, proveedores, clientes y de más partes interesadas, establece la necesidad de implementar un Sistema de Gestión de Seguridad y Privacidad de la Información encaminado a proteger los activos de la información a través de la generación de Políticas específicas, procedimientos, lineamientos, apoyo en la implementación de herramientas tecnológicas de prevención y forjar una cultura de concientización de seguridad de la información en todos los funcionarios y contratistas de la entidad, todo esto con el objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la información, garantizando la continuidad del servicio y minimizar el impacto causado por los riesgos identificados, logrando así mantener la confianza y responder frente a las necesidades de sus diferentes grupos de interés.

Todo esto en concordancia con la misión y visión de la entidad, la normatividad vigente, los principios de la función administrativa y comprometidos con la Mejora continua a través de la

medición de la efectividad de los controles del Sistema de Gestión de Seguridad y Privacidad de la Información.

La Gobernación de Nariño, aprueba la política general y políticas específicas de seguridad de la información que se generen y ofrece respaldo tanto económico y administrativo para llevar a cabo todo el proceso de implementación y continuidad de un Sistema de Gestión de Seguridad y Privacidad de la Información completamente alineado a la misión, visión y planes estratégicos de la entidad.

La política se debe aplicar por parte de todos los funcionarios, contratistas, usuarios, clientes, proveedores y demás partes interesadas, los cuales deben comprometerse con el cumplimiento total de esta política y las específicas que se generen en torno a la seguridad de la información.

La Secretaría TIC, Innovación y Gobierno Abierto, es responsable de velar por la implementación, el cumplimiento y seguimiento de la política de seguridad de la información.

La política general y sus objetivos serán revisados y actualizados una vez al año, en los casos en que se vea necesario se ajustarán antes de su revisión y posteriormente se presentará para aprobación.

Se socializará la política por los medios de comunicación con los que cuenta actualmente la Gobernación de Nariño.

El incumplimiento de toda política que se genere entorno a la Seguridad de la información y Ciberseguridad será sancionado de acuerdo con el nivel de incumplimiento, impacto generado y proceso disciplinario que la Gobernación de Nariño tenga definido.

Los recursos deben ser utilizados bajo principios legales y éticos, ya que están dispuestos para labores orientadas a la visión y misión de la entidad.

Para dar uso aceptable de los recursos tecnológicos los empleados, clientes y proveedores deben acogerse a los siguientes deberes:

- La información relacionada con la entidad es propiedad exclusiva de ella, debe solicitarse permiso formal cuando se requiera realizar manipulación de la misma
- La información creada en relación con las operaciones propias de la entidad debe ser almacenada y clasificada en los dispositivos y sistemas de información que pertenecen a la misma, según directrices de la secretaría TIC y directivos de la entidad.

El uso inaceptable de los recursos tecnológicos:

- Transmisión de contenido que atente contra los valores y la ética de la entidad o de cualquier información difamatoria que afecte el contexto interno y externo de la misma.

- Uso y transmisión de material electrónico, violando derechos de propiedad intelectual.
- El Inicio de sesión en activos con credenciales de autenticación ajenas.
- Uso excesivo de los recursos para fines no relacionados con las labores asignadas causando lentitud en los objetivos misionales.
- Alteración de información con datos incorrectos y difusión de los mismos al interior de la entidad y de manera externa.
- Eliminación de información desde los dispositivos informáticos y sistema de información que se encuentren a su cargo, para restringir su acceso y procesos de empalme.
- El uso de software malicioso para generar degradación de los activos de información de la entidad o de terceros.

9. LINEAMIENTOS PARA OPERATIVIZAR LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

Definir y asignar los recursos para la Implementación de la política:	La Dirección de la Gobernación de Nariño, ofrece respaldo tanto económico y administrativo para llevar a cabo todo el proceso de implementación y continuidad de un Sistema de Gestión de Seguridad y Privacidad de la Información.
Crear la Oficina de Seguridad de la información	Infraestructura adaptada y modificada en la Secretaría TIC, Innovación y Gobierno Abierto.
Contratar un Oficial de Seguridad de la Información	Profesional en seguridad de la información, quien se encarga de planificar, administrar y alinear las iniciativas de seguridad con los objetivos misionales y supervisar el cumplimiento del Sistema de Gestión de Seguridad y Privacidad de la Información.
Conformar el Comité de Seguridad de la Información	La Dirección de la Gobernación de Nariño asigna un grupo de líderes de área quienes se encargan de tomar las decisiones sobre la estrategia general de seguridad y controlar que se implemente adecuadamente.

Crear e Implementar un programa de capacitación y sensibilización en seguridad de la información.	El objetivo de este programa es lograr infundir una cultura en pro del uso de las buenas prácticas en seguridad y cumplimiento con las políticas y controles implementados con el Sistema de Gestión de Seguridad y Privacidad de la Información. El programa va dirigido a todos los funcionarios y contratistas de la entidad.
Implementar el proceso de Gestión de Incidentes de Seguridad de la Información.	La Gestión de incidentes de Seguridad de la Información debe contener: Formato de reporte de incidentes o eventos de seguridad de la información, Clasificación de incidentes, Tratamiento, Lecciones aprendidas.
Gestión del Riesgo	Gestionar los riesgos identificados de manera oportuna a través de controles de seguridad.
Medir la efectividad del funcionamiento del SGSI	Realizar seguimiento a través de indicadores relacionados con la efectividad de los controles implementados, el cumplimiento de políticas, las buenas prácticas en seguridad de la información y el reporte de incidentes, analizar resultados y definir acciones de mejora.

10. SOCIALIZACIÓN DE LA POLITICA DE SEGURIDAD.

La política de seguridad de la información se divulgará de manera sistemática hacia el personal de la entidad, mediante los medios de comunicación disponibles como son: intranet, correo electrónico institucional, y a través de las sesiones de capacitación en seguridad que se realicen de acuerdo al plan de sensibilización. Los líderes y gestores de la institución desplegarán la política al interior de cada uno de sus procesos, según directrices de la Secretaría TIC, con el propósito de que cada uno de sus funcionarios y contratistas la interiorice y comprenda cómo desde el rol que desempeña puede aportar al cumplimiento del compromiso con la seguridad.

De la misma forma para reforzar el conocimiento de la política se implementará las siguientes estrategias:

- Pendón de la política de seguridad,
- Volante que contiene la política para entregarse de manera personalizada a funcionarios, contratistas y demás partes interesadas,
- Video institucional de La Política General de Seguridad de Seguridad de la Información.
- Presentación de política a través de la intranet y pagina web institucional.
- Socialización por comunicación interna
- Presentación de la política de seguridad en la inducción y reinducción Interna
- Presentación de política General de Seguridad de la Información y programa a través de comunicaciones desde la Secretaría TIC o Directivos de la Gobernación de Nariño.

NOTA:
Lo anterior se ejecuta con autorización de la Gobernación de Nariño y alineados al tema contractual y de comunicaciones que la Entidad tenga establecida.

11. MONITOREO Y EVALUACIÓN DE LA POLÍTICA.

El cumplimiento del compromiso con la seguridad que hace la Gobernación de Nariño se realizará a través del monitoreo de aspectos claves de la seguridad con el apoyo de los Planes de seguridad y sensibilización, evaluación de desempeño entre otros.

- Indicadores para el monitoreo: Índice Global de Incidentes, porcentaje de gestión de Incidentes, Porcentaje de Vigilancia de Incidentes entre otros.
- Implementación de procedimientos de buenas prácticas en seguridad de la información.
- Indicadores propios para medir adherencia a las buenas prácticas implementadas.
- Seguimiento a planes de mejoramiento implementados.

12. DOCUMENTOS Y REGISTROS RELACIONADOS.

N/A.

13. ANEXOS.

N/A.

14. CONTROL DE CAMBIOS.

Versión	Fecha de versión	Descripción del cambio	Responsable
01	23/08/2023	Creación del Documento	Secretario TIC, Innovación y Gobierno Abierto

15. RESPONSABLE.

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

16. REVISIÓN, VALIDACIÓN Y APROBACIÓN.

Revisión:	Aprobación:	Verificación:
Nombre: Raúl Alejandro Ortiz Navarro	Nombre: Comité Institucional de Gestión y Desempeño	Nombre: Nixon Ortega Bravo
Cargo: Secretario TIC, Innovación y Gobierno Abierto	Cargo: Comité Institucional de Gestión y Desempeño	Cargo: Profesional Universitario 219 grado 04