# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## I. INTRODUCCIÓN:

La información es considerada el activo más importante y valioso para todas las organizaciones, y un recurso indispensable para el desarrollo y cumplimiento sus objetivos misionales. La información puede llegar a ser vulnerable, sensible o crítica y por lo tanto requiere de una evaluación para determinar su nivel de protección necesario para mitigar o evitar posibles situaciones de riesgo e impacto asociado a la pérdida de su disponibilidad, integridad o confidencialidad.

A través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la Política de Gobierno Digital (antes estrategia Gobierno en Línea-GEL). Forma parte del componente de Seguridad y Privacidad de la Información, acorde con las mejores prácticas de seguridad y estándares internacionales como ISO 27001 e ISO 31000 y COSO (análisis y gestión de riesgos).

Para la Gobernación de Nariño es indispensable establecer un modelo de gestión de seguridad y privacidad de la información, para salvaguardar la información de la entidad en todos sus aspectos, garantizando la seguridad de los datos, el cumplimiento de las normas legales, teniendo en cuenta la norma NTC/IEC ISO 27001:2013, las políticas de seguridad digital y continuidad del servicio de MinTIC y el Modelo Integrado de Planeación y Gestión MIPG de la entidad.

El Plan de seguridad y privacidad de la información, pretende establecer un conjunto de actividades, estrategias y herramientas, basadas en el ciclo PHVA(Planear, Hacer, Verificar y Actuar), para crear condiciones de uso confiable en el entorno digital y físico de la información, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información en la Gobernación de Nariño y el establecimiento de controles para mitigar las posibles afectaciones a los activos que soportan los procesos y la gestión diaria de la entidad en el desempeño de sus funciones.

De igual manera se busca contribuir al incremento de la transparencia y acceso a la información Pública, cumplimiento de la Ley de protección de datos personales, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.

# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## II. OBJETIVO GENERAL:

Construir el plan de seguridad y privacidad de la información, con actividades y estrategias alineadas con la norma NTC/IEC ISO 27001:2013, las políticas de seguridad digital y continuidad del servicio de MinTIC y el Modelo Integrado de Planeación y Gestión MIPG, con el fin de proteger, preservar y administrar la confidencialidad, integridad, disponibilidad y autenticidad de la información de la Gobernación de Nariño, enmarcado en el ciclo de mejoramiento continuo PHVA.

## III. OBJETIVOS ESPECÍFICOS:

1. Apropiar y adoptar aspectos normativos, políticas y marco de referencia, que se tendrá en cuenta para la formulación del plan de seguridad y privacidad de la información.
2. Definir las etapas que se desarrollarán para definir las estrategias de seguridad informática y de la información en la entidad, equipo de trabajo y cronograma de ejecución.
3. Elaborar el plan de seguridad y privacidad de la información, asociado con las políticas y procesos que hacen parte integral del SGSI. Actualización de política de seguridad de la información.
4. Presentar el plan de seguridad y privacidad de la información, para su aprobación y publicación.
5. Implementar el plan de seguridad y privacidad de la información, y dar a conocer al personal de la entidad.
6. Gestionar los riesgos de seguridad y privacidad de la información, Seguridad Digital y continuidad de la operación de manera integral.
7. Aplicar mecanismos definidos para la seguridad física y digital de la información, que conlleven a mantener la confidencialidad, integridad, legalidad, confiabilidad y continuidad de la información en la entidad.
8. Establecer contingencias para mitigar incidentes de Seguridad y Privacidad de la Información, y Seguridad Digital de forma efectiva, eficaz y eficiente.
9. Hacer uso eficiente y seguro de los recursos TI (humanos, físicos, financieros, tecnológicos) para garantizar la continuidad de la prestación de los servicios.
10. Definir los lineamientos necesarios para el manejo de la información tanto física como digital en el marco de una gestión documental basada en Seguridad y Privacidad de la Información.
11. Adquirir e implementar hardware y software para fortalecer la infraestructura tecnológica en beneficio de la seguridad física y digital de la información.

**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

12. Promover la adopción de mejores prácticas y generar conciencia para el cambio organizacional, necesario para la apropiación de la Seguridad y Privacidad de la Información por parte de los usuarios internos y externos de la entidad...
13. Elaborar y reglamentar procedimientos para la implementación de buenas prácticas contenidas en el plan de seguridad y privacidad de la información física y digital.
14. Aplicar procedimientos y normatividad relacionada con la protección de datos personales, garantizando su cumplimiento y legalidad en los sistemas de información.
15. Seguimiento y control permanente en la aplicación del plan de seguridad y privacidad de la información, aplicando el ciclo de mejoramiento continuo PHVA (planear, hacer, verificar, actuar).

## IV. ALCANCE:

El plan de seguridad y privacidad de la información, está enmarcado en los controles de la norma NTC/IEC ISO 27001:2013, las políticas de seguridad digital y continuidad del servicio de MinTIC y el Modelo Integrado de Planeación y Gestión MIPG, y considera el análisis de riesgos a todos los procesos de la Gobernación de Nariño, que manejen, procesen o interactúen con información física y digital institucional.

Aplica a toda la entidad, funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que interactúen con la entidad en cumplimiento de sus funciones o recepción de servicios, y que compartan, utilicen, recolecten, suministren, procesen, intercambien o consulten información, así como también los entes de control o entidades que accedan de manera interna o externa a cualquier archivo de información física o digital independientemente de su ubicación.

Aplica a todo tipo de información histórica o activa, creada, recepcionada o procesada en la entidad, sin importar el medio de almacenamiento, presentación o ubicación.

## V. TÉRMINOS ASOCIADOS:

- Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

- Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e

información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

- Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

- Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

- Confidencialidad: propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
- Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

- Datos biométricos: parámetros físicos únicos de cada persona que comprueben su identidad y se evidencian cuando la persona o una parte de ella interacciona con el sistema (huella digital o voz).

- Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- Datos Personales Públicos: 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. (Decreto 1377 de 2013, art 3)

**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

- Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

- Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

- Disponibilidad: propiedad de ser accesible y utilizable por los usuarios autorizados de la entidad autorizados.

- Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas.

- Gestión del riesgo: proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

- Impacto: el coste para la empresa de un incidente “de la escala que sea”, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

- Incidente de seguridad de la información: Resultado de intentos intencionales o accidentales de romper las medidas de seguridad de la información impactando en la confidencialidad, integridad o disponibilidad de la información.

- Información Pública: Es aquella información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.

- Información: Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y transmitirla.

- Integridad: propiedad de exactitud y completitud de la información.

- Inventario de activos: lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan

valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. (ISO 27000.es,2012).

- Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.

- Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación.

- Riesgo: Es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o de los procesos. Se expresa en términos de probabilidad y consecuencias.

- Riesgo de seguridad y privacidad: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización. Se mide en términos de probabilidad y consecuencias.

- Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de 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).

- Sistema de Información: se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales

- Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

- Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

## PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

### VI. FASES DE CONSTRUCCIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN:

| Fases | Sesiones | Objetivo | Responsable | Tiempo estimado |
|---|---|---|---|---|
| **Fase 1: Planear** | Involucrar a los participantes e interesados | Consolidar el grupo encargado de construir el Plan de Seguridad y privacidad de la Información | Equipo de Trabajo de la Secretaría TIC, con la participación de las Dependencias involucradas con los objetivos de cada fase | Seis (6) meses |
| | Analizar el entorno y la normatividad vigente | Realizar un análisis de los factores externos políticos, económicos, sociales, tecnológicos y normatividad vigente que afecta la entidad pública. | | |
| | Definición del alcance del Plan de Seguridad y Privacidad de la Información | Definición del alcance del Plan de Seguridad y Privacidad la Información y su Alineación con PETIC | | |
| **Fase 2: Hacer** | Definición de políticas de seguridad de la Información | Actualizar la Política de Seguridad de la información. Aprobación, publicación y apropiación de la política. | | |
| | Construcción del Plan de Seguridad y Privacidad de la Información | Formular el Plan de Seguridad y Privacidad de la Información, aprobación por parte de la alta dirección. | | |
| | Presentar el Plan de Seguridad y Privacidad de la Información | Presentar el Plan de Seguridad y Privacidad de la Información en la entidad | | |
| | Asignación de recursos | Establecer personal, tiempo, dinero, etc. para la implementación del plan de seguridad y privacidad de la Información | | |
| | Implementación de la Política y Plan de Seguridad y Privacidad de la Información | Implementación de políticas, controles y procedimientos establecidos en el Plan de Seguridad y Privacidad de la Información | | |
| | Tratamiento de riesgo. | Realizar el tratamiento de Riesgos, asociados al plan de Seguridad y Privacidad de la Información | | |
| **Fase 3: Verificar** | Realización de auditorías internas. | Hacer auditorías internas de políticas, controles y procedimientos establecidos en el Plan de Seguridad y Privacidad de la Información | | |

## PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

| | | | | |
|---|---|---|---|---|
| | Medición de resultados. | Definir el tablero de indicadores para medir el avance en la estrategia de la implementación del Plan de Seguridad y Privacidad de la Información | | |
| **Fase 4: Actuar** | Aplicación de acciones correctivas y de mejora. | Aplicar acciones correctivas y de mejora de la implementación del Plan de Seguridad y Privacidad de la Información | | |