PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VIGENCIA 2023

GOBERNACIÓN DE NARIÑO

Secretaría TIC, Innovación y Gobierno Abierto

TABLA DE CONTENIDO

INTRODUCCIÓN

El avance de la tecnología y los requerimientos que el manejo de la información imponen en el mundo moderno, han hecho que la problemática de la gestión de la seguridad de la información sea cada vez un asunto más complejo y que requiere ser asumido por las organizaciones de una manera estructurada, con procesos permanentemente desarrollados en torno al tema, debido a que la gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Un Sistema de Gestión de Seguridad de la Información (SGSI) es un conjunto de políticas, procesos y procedimientos para gestionar de manera sistemática y segura la información de una Entidad. Los SGSI son el medio más eficaz para minimizar los riesgos, al asegurar que se identifican y valoran los activos y sus riesgos, considerando el impacto para la organización, y se adoptan los controles, procedimientos más eficaces y coherentes con la estrategia de la entidad. De esta manera, el objetivo de un SGSI es minimizar el riesgo y buscar la seguridad integral de la información.

El SGSI es el concepto central sobre el que se construyen las normas y sirve de base para el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de las Tecnologías de Información y Comunicaciones (MINTIC).

De igual manera, los SGSI constituyen el concepto central sobre el que se construye la norma NTC ISO/IEC 27001, la cual especifica los requerimientos para identificar, implementar, operar, monitorear, revisar, mantener y mejorar los mismos. Esta norma es la principal de la serie ISO 27000.

El 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, es claro en determinar la seguridad de la información como un principio rector de dicha política:

> *"… Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano…"*

Por otra parte, también señala la política de Gobierno Digital que la seguridad de la información es un habilitador transversal:

> *"… Habilitadores Transversales de la Política de Gobierno Digital: Son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital…"*

Este habilitador transversal, busca que las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad, disponibilidad, y privacidad de la información, así como la protección de los datos personales que tratan las entidades públicas en cumplimiento de la normatividad de protección de datos personales, el cual tiene soporte en el MSPI.

Por otra parte, la resolución número 00500 de marzo 10 de 2021, "por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital", establece en su artículo 2 – Ámbito de aplicación, lo siguiente:

> *"…Serán sujetos obligados de la presente resolución los señalados en el artículo 2.2.9.1.1.2. del Decreto 1078 de 2015 (DUR-TIC), "Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones…"*

En donde claramente, el Departamento de Nariño se considera como sujeto obligado.

Adicional a lo anterior, la misma resolución (00500 de marzo 10 de 2021), establece en su artículo 3 – Lineamientos generales, lo siguiente:

> *"… Los sujetos obligados deben adoptar medidas técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al plan de seguridad y privacidad de la información y así mitigar riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital. Las entidades deben contar con políticas, procesos, procedimientos, guías, manuales y formatos para garantizar el cumplimiento al ciclo PHVA del MSPI. En ese sentido, deben adoptar los lineamientos del MSPI, guía de riesgos y gestión de incidentes de seguridad digital que se relacionan en el Anexo 1 de la presente resolución.*
>
> *Para todos los procesos, trámites, sistemas de información, infraestructura tecnológica e infraestructura crítica de los sujetos obligados, se deben adoptar medidas de seguridad eficientes alienadas al MSPI, para prestar servicios de confianza, generando protección de la información de los ciudadanos, gestionando los riesgos y los incidentes de seguridad digital…"*

Por otra parte, la ley 1581 de 2012 ordena que *"la información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento"*, y establece el deber de los Responsables de Tratamiento de *"conservar la información bajo las condiciones de seguridad necesaria para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento"*.

Adicional a lo anterior, dicha ley (1581 de 2012) es aplicable al tratamiento de datos personales realizado por entidades de naturaleza pública o privada y que el artículo 25 creó el Registro

Nacional de Bases de Datos (RNBD), administrado por la Superintendencia de Industria y Comercio.

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.

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.

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Establecer un plan de seguridad de la información para el año 2023 que apoye el establecimiento, operación, mejora continua y sostenibilidad del Sistema de Administración de Riesgos de Seguridad de la Información de la Gobernación de Nariño, acorde con los requerimientos de la entidad, con el Plan de Desarrollo Mi Nariño en defensa de lo nuestro 2020 – 2023 y en cumplimiento a las disposiciones legales vigentes emitidas por el Gobierno Nacional.

2.2. OBJETIVOS ESPECIFICOS

1. Construcción del Sistema de Gestión de Seguridad de la Información SGSI de la Gobernación de Nariño, según los lineamientos de MINTIC, decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, normas ISO 27001 e ISO 31000 y COSO (análisis y gestión de riesgos) y demás normas relacionadas.
2. Dar cumplimiento a la Ley ley 1581 de 2012 de protección de datos personales, mediante el diagnóstico y planeación del sistema de gestión y protección de datos personales, aplicación de controles y estrategias de sensibilización en seguridad de la información.
3. Fortalecer el sistema de seguridad informática para minimizar riesgos que afecten la disponibilidad, integridad y confidencialidad de la información existente en la Gobernación de Nariño.
4. Fortalecer la cultura de seguridad de la información de la Gobernación de Nariño, para el uso adecuado y seguro de los recursos tecnológicos y la información por parte de los usuarios de la entidad.
5. Atender las observaciones y hallazgos de las auditorías internas y externas de control.

3. ALCANCE

El plan de seguridad y privacidad de la información, se enfocará en fortalecer la implementación de acciones de acuerdo a los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, orientados a la seguridad informática de la infraestructura tecnológica de la Gobernación de Nariño, dentro de las acciones que realizará la entidad en torno a la seguridad y privacidad de la información institucional, teniendo en cuenta las capacidades y recursos disponibles, para garantizar la confidencialidad, integridad y disponibilidad de la información, minimizando riesgos en todos sus activos.

Su aplicación será a todos los niveles de la Entidad, sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que, debido al cumplimiento de sus funciones, compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los entes de control, entidades relacionadas que accedan, ya sea interna o externamente a cualquier activo de información, independientemente de su ubicación. De igual manera, el plan aplica a toda la información creada, procesada o utilizada, sin importar el medio, formato o presentación o lugar en el cual se encuentre.

4. TERMINOS Y DEFINICIONES

- 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.

- Amenaza: Es la causa potencial de un daño a un activo de información.

- Anexo SL: Nuevo esquema definido por International Organization for Standardization - ISO para todos los Sistemas de Gestión acorde al nuevo formato llamado “Anexo SL”, que proporciona una estructura uniforme como el marco de un sistema de gestión genérico.

- Análisis de riesgos: Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

- 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).

- Causa: Razón por la cual el riesgo sucede.

- Ciberiesgo o riesgo cibernético: Posibles resultados negativos derivados de fallas en la seguridad de los sistemas tecnológicos o asociados a ataques cibernéticos. [CE 007 de 2018 SFC].

- Ciberseguridad: Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de FINDETER. [CE 007 de 2018 SFC].

- 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 comprueban 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)

- 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.

- PSE: Proveedor de Servicios Electrónicos, es un sistema centralizado por medio del cual las empresas brindan a los usuarios la posibilidad de hacer sus pagos por Internet.

- 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.

- Responsables del Activo: Personas responsables del activo de información.

- 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.

- Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

- Riesgo Residual: Nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo.

- 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).

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

5. MODELO DE SEGURIDAD

5.1. CICLO OPERACIÓN

El modelo de seguridad de la información de la Gobernación de Nariño, se estableció teniendo en cuenta las cinco (5) fases definidas en el ciclo de operación del Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno en Línea[1]:

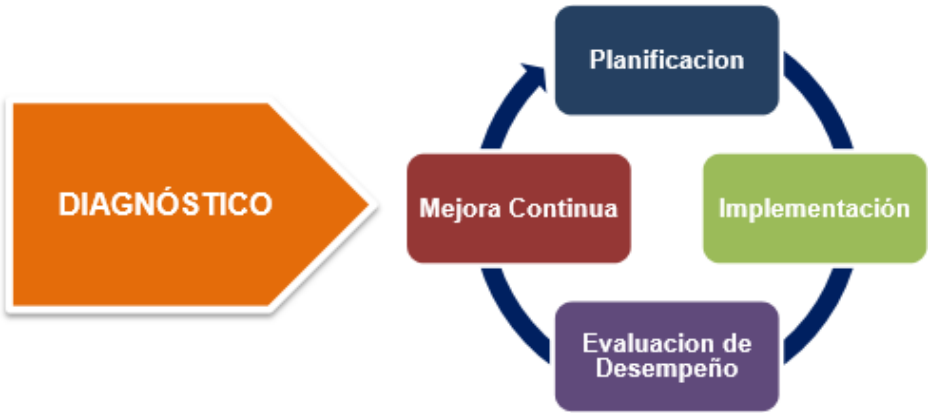

Figura 1. Ciclo de operación Modelo de Seguridad y Privacidad de la información
Fuente: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

- **Fase Diagnóstico**: Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.
- **Fase Planificación (P**lanear**):** En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.
- **Fase Implementación (H**acer**):** En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.
- **Fase Evaluación de desempeño (V**erificar**):** Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.
- **Fase Mejora Continua (A**ctuar**):** Se analizan los resultados de las acciones implementadas y si éstas no cumplen los objetivos definidos, se analizan las causas de las desviaciones y se generan los respectivos planes de acciones.

[1] Modelo de Seguridad y Privacidad, MINTIC, Pág. 1-2

5.2. ALINEACIÓN NORMA ISO 27001:2013 Y CICLO DE OPERACIÓN

Aunque en la norma ISO 27001:2013 no se determina un modelo de mejora continua (PHVA) como requisito para estructurar los procesos del Sistema de Gestión de Seguridad de la Información, la nueva estructura de esta versión se puede alinear con el ciclo de mejora continua de las modelos de gestión de la siguiente forma:

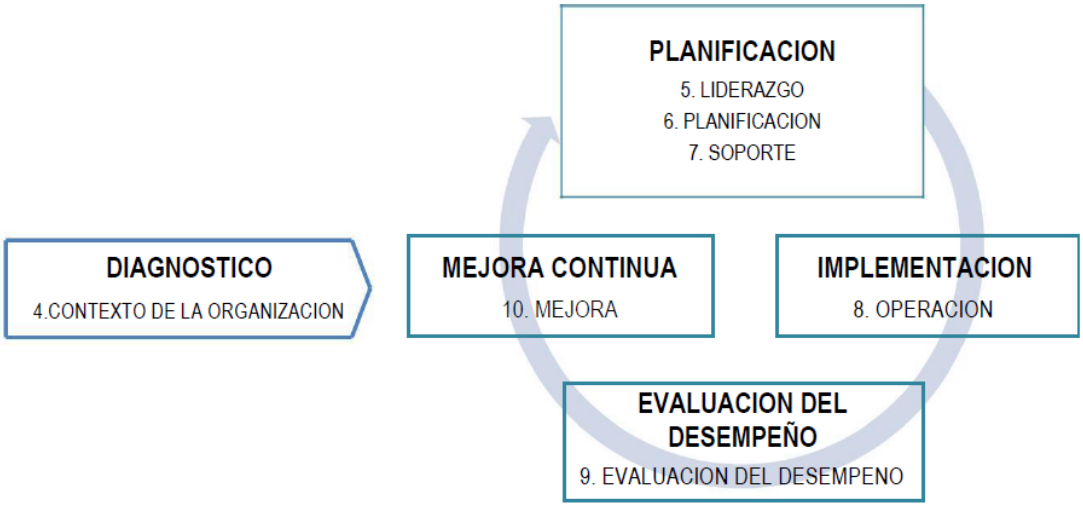

Figura 2. Norma ISO 27001:2013 alineado al Ciclo de mejora continua
Fuente: Elaborada con base en la información publicada en la página web *http://www.welivesecurity.com/la-es/2013/10/09/publicada-iso-270002013-cambios-en-la-norma-para- gestionar-la-seguridad-de-la-informacion/*

A continuación, se muestra la relación entre las fases del ciclo de operación del Modelo de Seguridad y Privacidad de la Información (Diagnóstico, Planificación, Implementación, Evaluación, Mejora Continua) y la estructura de capítulos y numerales de la norma ISO 27001:2013:

Fase	Capitulo ISO 27001:2013[2]
Diagnóstico	4. Contexto de la Organización
Planificación	5. Liderazgos 6. Planificación 7. Soporte
Implementación	8. Operación
Evaluación de desempeño	9. Evaluación de desempeño
Mejora Continua	10. Mejora

Tabla 1. Fases Ciclo Operación vs Estructura ISO 27001:2013

FASE I. DIAGNÓSTICO:

En la norma ISO 27001:2013. En el capítulo 4 - Contexto de la organización de la norma ISO 27001:2013, se determina la necesidad de realizar un análisis de las cuestiones externas e internas de la organización y de su contexto, con el propósito de incluir las necesidades y expectativas de las partes interesadas de la organización en el alcance del modelo de seguridad de la información.

Objetivo	Identificar el estado de la Entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información

Figura 3. Fase de Diagnóstico modelo de seguridad
Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

[2] NTC-ISO-IEC 27001:2013, Pág. 1-12

Metas	Actividades \ Instrumentos \ Resultados
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la entidad	Diagnóstico de la situación actual de la entidad con relación a la gestión de seguridad de la información. Diagnóstico nivel de cumplimiento de la entidad frente a los objetivos de control y controles establecidos en el Anexo A de la norma ISO 27001:2013. Valoración estado actual de la gestión de seguridad de la entidad con base en el Instrumento de Evaluación MSPI de MINTIC.
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad.	Valoración del nivel de estratificación de la entidad frente a la seguridad de la información con base en el método planteado en el documento '*ANEXO 3: ESTRATIFICACIÓN DE ENTIDADES*' del modelo seguridad de la información para la estrategia de Gobierno en Línea 2.0. Valoración del nivel de madurez de seguridad y privacidad de la información en la entidad de acuerdo con los lineamientos establecidos en el capítulo '*MODELO DE MADUREZ*' del documento Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea.
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Ejecución prueba de vulnerabilidades con el fin de identificar el nivel de seguridad y protección de los activos de información de la entidad y definición de planes de mitigación.

Para la recolección de la información, en esta fase se utilizarán mecanismo como:

- Diligenciamiento de cuestionarios con el objetivo de determinar el nivel de cumplimiento de la entidad, con relación a los dominios de la norma ISO/IEC 27001:2013.
- Documentación existente en el sistema de calidad de la entidad relacionada con la información de las partes interesadas de la entidad, los roles y funciones asociadas a la seguridad de la información.
- Fuentes externas, como las guías de autoevaluación, encuesta y estratificación dispuestas por la estrategia de gobierno en línea Ministerio de Tecnologías de la Información y las Comunicaciones.

FASES II. PLANIFICACIÓN:

En la norma ISO 27001:2013. En el capítulo 5 - Liderazgo, se establece las responsabilidades y compromisos de la Alta Dirección respecto al Sistema de Gestión de Seguridad de la Información, y entre otros aspectos, la necesidad de que la Alta Dirección establezca una política de seguridad de la información adecuada al propósito de la organización, asegure la asignación de los recursos para la seguridad de la información y que las responsabilidades y roles pertinentes a la seguridad de la información se asignen y comuniquen.
En el capítulo 6 - Planeación, se establece los requerimientos para la valoración y tratamiento de riesgos de seguridad, y para la definición de objetivos viables de seguridad de la información y planes específicos para su cumplimiento.

En el capítulo 7 - Soporte se establece que la organización debe asegurar los recursos necesarios para el establecimiento, implementación y mejora continua del modelo de seguridad de la Información.

Objetivo	Definir la estrategia metodológica, que permita establecer el alcance, objetivos, procesos y procedimientos, pertinentes a la gestión del riesgo y mejora de seguridad de la información, en procura de los resultados que permitan dar cumplimiento con las metas propuestas del SGSI.

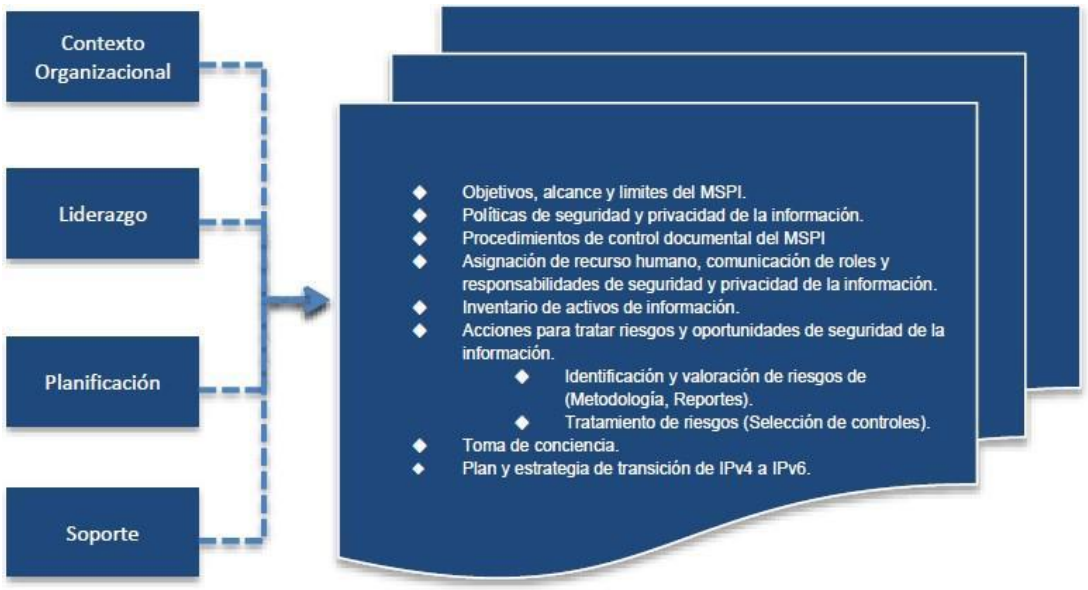

Figura 4. Fase de Planificación modelo de seguridad
Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

Metas	Actividades \ Instrumentos \ Resultados
Realizar un análisis de Contexto y factores externos e internos de la entidad en torno a la seguridad de la información.	Realizar un Análisis de Contexto de la entidad entorno a la seguridad de la información teniendo en cuenta el capítulo 4. CONTEXTO DE LA ORGANIZACIÓN de la norma ISO 27001:2013, con el fin de poder determinar las cuestiones externas e internas de la organización que son pertinentes para la implementación del Sistema de Gestión de Seguridad de la Información.
Definir el alcance del SGSI de la entidad	Definir el alcance del Sistema de Gestión de Seguridad de la Información de la entidad aprobado por la Alta Dirección y socializado al interior de la Entidad. Definir el alcance del Sistema de Gestión de Seguridad de la Información, en el cual se establece los límites y la aplicabilidad del sistema.
Definir Roles, Responsables y Funciones de seguridad y privacidad de la información	Adicionar las funciones de seguridad de la información, al Comité de Riesgos de la entidad y formalizar mediante acto administrativo. Establecer el Rol de Oficial de Seguridad de la información. Definir un marco de gestión que contemple roles y responsabilidades para la implementación, administración, operación y gestión de la seguridad de la información en la entidad. Definir la estructura organizacional de la Entidad que contendrá los roles y responsabilidad pertinentes a la seguridad de la información.
Definir la metodología de riesgos de seguridad de la información	Definir Metodología de Valoración de Riesgos de Seguridad. Integrar la metodología definida con la metodología de riesgos operativos de la entidad. Implementar un sistema de información para la administración y gestión de los riesgos de seguridad de la entidad.
Elaborar las políticas de seguridad y privacidad de la información de la entidad	Actualizar Política General de Seguridad y Privacidad la cual debe ser aprobada por la Alta Dirección y socializada al interior de la Entidad. Elaborar el manual de Políticas de Seguridad y Privacidad de la Información, que corresponde a un documento que contiene las políticas y los lineamientos que se implementaran en la Entidad con el objetivo de proteger la disponibilidad, integridad y confidencialidad de la información. Estas políticas deben ser aprobadas por la Alta Dirección y socializadas al interior de la Entidad.

Elaborar documentación de operación (formatos de procesos, procedimientos y documentos debidamente definidos y establecidos) del sistema de seguridad de la información.	Elaborar los documentos de operación del sistema de seguridad de la información, tales como: • Declaración de aplicabilidad • Procedimiento y/o guía de identificación y clasificación de activos de información. • Procedimiento Continuidad del Negocio, Procedimientos operativos para gestión de TI • Procedimiento para control de documentos (SGI) • Procedimiento para auditoría interna (SGI) • Procedimiento para medidas correctivas (SGI) • Procedimiento para la gestión de eventos e incidentes de seguridad de la información • Procedimiento para la gestión de vulnerabilidades de seguridad de la información. • Entre otros.
Identificar y valorar activos de información	Realizar la identificación y valoración de los activos de información de la entidad de acuerdo con su nivel de criticidad y el alcance del modelo de seguridad. Documentar el inventario de los activos de información de la entidad.
Identificar, valorar y tratar los riesgos de seguridad de la información de la entidad	Realizar la identificación y valoración de los riesgos transversales de seguridad de la información y definir los respectivos planes de tratamiento. Realizar la valoración de riesgos de seguridad de la información. Definir los planes de acción que incluya los controles a implementar con el objetivo de mitigar los riesgos identificados en el proceso de valoración de riesgos. Para la seleccionar de los controles, se tomará como base los objetivos de control y los controles establecidos en el Anexo A de la norma ISO/IEC 27001:2013.
Establecer plan de capacitación, comunicación y sensibilización de seguridad de la información.	Elaborar plan anual de capacitación y sensibilización sobre de seguridad de la información.

FASES III. IMPLEMENTACIÓN:

En la norma ISO 27001:2013. En el capítulo 8 - Operación de la norma ISO 27001:2013, se indica que la organización debe planificar, implementar y controlar los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información.

Objetivo	Llevar a cabo la implementación de la fase de planificación del SGSI, teniendo en cuenta para esto los aspectos más relevantes en los procesos de implementación del Sistema de Gestión de Seguridad de la Información de la entidad.

Figura 5. Fase de Implementación modelo de seguridad
Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

Metas	Actividades \ Instrumentos \ Resultados
Establecer el plan de implementación de seguridad de la información	Ejecutar el plan de implementación del modelo de seguridad y privacidad de la información el cual debe ser revisado y aprobado por el comité de riesgos.
Ejecutar el plan de tratamiento de riesgos	Ejecutar el plan de tratamiento de los riesgos transversales de seguridad de la información, identificados en la fase de planificación que fue presentado en el comité de riesgos.
Ejecutar del plan y estrategia de transición de IPv4 a IPv6.	Ejecutar y realizar seguimiento al plan de transición a IPv6 y elaborar informe de implementación.
Establecer indicadores de gestión de seguridad	Definir los indicadores para medir la gestión del modelo de seguridad y establecer los mecanismos para su medición. Estos indicadores deben permitir verificar la eficacia y efectividad de los controles implementados para mitigar los riesgos de seguridad de la entidad.
Implementar procedimiento de gestión de eventos e incidentes de seguridad	Implementar el procedimiento y los mecanismos para la gestión de los eventos e incidentes de seguridad de la información.
Implementar procedimiento de gestión de vulnerabilidades	Implementar el procedimiento y los mecanismos para la gestión de vulnerabilidades de seguridad de la información.

Ejecutar plan de capacitación y sensibilización de seguridad	Ejecutar el plan anual de capacitación, socialización y sensibilización de seguridad de la información.
Ejecutar pruebas anuales de vulnerabilidades e intrusión	Ejecutar el plan anual de pruebas de vulnerabilidades e intrusión, con el objetivo de identificar el nivel de protección de los activos de información de la entidad. Para tal efecto, se deberá tener en cuenta los respectivos requerimientos de seguridad relacionados con pruebas de vulnerabilidades establecidos en la circular externa 029 de 2014 de la Superfinanciera de Colombia o la circular que las reemplacen.
Ejecutar pruebas de Ethical Hacking	Ejecutar pruebas anuales de Ethical Hacking orientadas a poder determinar los niveles de riesgo y exposición de la organización ante atacantes internos o externos, que puedan comprometer activos críticos de la entidad y con esto generar interrupción en los servicios, afectar la continuidad del negocio y/o acceder de forma no autorizada a la información sensible o clasificada de la entidad o de carácter personal de los trabajadores o terceros que laboren para la entidad.
Ejecutar pruebas de Ingeniería Social	Ejecutar pruebas anuales de ingeniería social orientadas a verificar aspectos como: (i) los protocolos internos de seguridad, (ii) el nivel de concientización de los funcionarios y terceros que laboren en la entidad sobre temas de seguridad de la información, (iii) el conocimiento y/o cumplimiento de las políticas de seguridad y privacidad de la información de la entidad y (iv) el nivel de exposición de la información publicada en internet de la entidad y de sus empleados.

FASES IV. EVALUACIÓN DE DESEMPEÑO:

En la norma ISO 27001:2013. En el capítulo 9 - Evaluación del desempeño, se define los requerimientos para evaluar periódicamente el desempeño de la seguridad de la información y eficacia del sistema de gestión de seguridad de la información.

Objetivo	Evaluar el desempeño y la eficacia del SGSI, a través de instrumentos que permitan determinar la efectividad de la implantación del SGSI.

Figura 6. Fase de Evaluación de desempeño modelo de seguridad
Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

Metas	Actividades \ Instrumentos \ Resultados
Ejecución de auditorías de seguridad de la información	Ejecución de auditorías del modelo de seguridad y de temas normativos y de cumplimiento de seguridad de la información aplicables a la entidad, de acuerdo con el plan de auditoría revisado y aprobado por la Alta Dirección. Las auditorías internas se deberán llevar a cabo para la revisión del modelo de seguridad de la información y ciberseguridad implementado en la entidad, con la finalidad de verificar que los objetivos de control, controles, procesos y procedimientos del modelo de seguridad cumplan con los requisitos establecidos en la norma ISO 27002:2013.
Plan de seguimiento, evaluación y análisis de SGSI	Elaboración documento con el plan de seguimiento, evaluación y análisis del modelo de seguridad revisado y aprobado por el Comité de Riesgos.

FASES V: MEJORA CONTINUA:

En la norma ISO 27001:2013. En el capítulo 10 - Mejora, se establece para el proceso de mejora del modelo de seguridad de la Información, que a partir de las no-conformidades que ocurran, las organizaciones deben establecer las acciones más efectiva para solucionarlas y evaluar la necesidad de acciones para eliminar las causas de la no conformidad con el objetivo de que no se repitan.

Objetivo	Consolidar los resultados obtenidos del componente de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el modelo de seguridad.

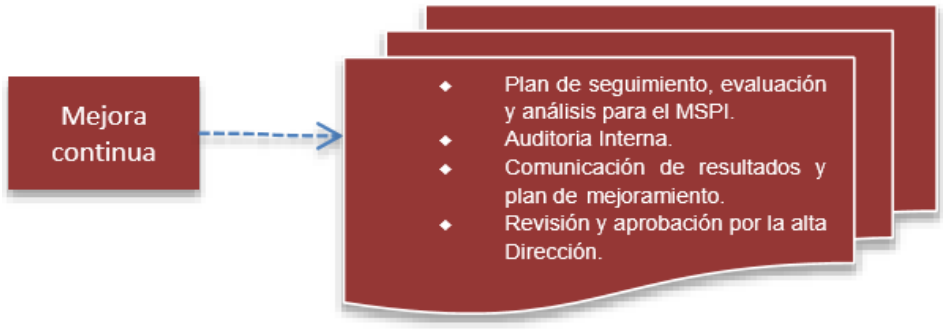

Figura 7. Fase de Mejora Continua modelo de seguridad
Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

Metas	Actividades \ Instrumentos \ Resultados
Diseñar plan de mejoramiento	Diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el Sistema de Gestión de Seguridad de la Información.

6. CRONOGRAMA PLAN DE SEGURIDAD DE LA INFORMACIÓN 2023

El plan de seguridad y privacidad de la información para le vigencia 2023 será ejecutado con recursos propios a través del proyecto **“**Diseño de un Sistema de Gestión de Seguridad de la Información en la Gobernación de Nariño” registrado en el Banco de Proyectos de la entidad mediante código BPIN 2021003520221.

ACTIVIDADES	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic
Identificar y documentar el estado actual de la gestión de seguridad y privacidad de la información en la Entidad, utilizando la herramienta de diagnóstico de MSPI.												
Determinar y documentar el nivel de madurez de los controles de seguridad de la información aplicados actualmente en la entidad.												
Identificar y documentar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.												
Identificar y documentar el uso de buenas prácticas en ciberseguridad.												
Aplicar Análisis de vulnerabilidad – Hacking ético (2 Servidores).												
Elaborar la política de seguridad y privacidad de la información, la cual debe contener una declaración general por parte de la administración, donde se especifique sus objetivos, alcance, nivel de cumplimiento.												
Desarrollar y formalizar procedimientos que permitan gestionar la seguridad de la información en el proceso definido por la secretaría TIC, Innovación y Gobierno Abierto, para la gestión de sistemas de información automatizados en la entidad.												
Definir y documentar los roles y responsabilidades de seguridad de la información en los diferentes niveles (Directivo, de procesos y operativos), y el equipo de gestión de seguridad de la información teniendo en cuenta el perfil estratégico, táctico, operativo y población participante, que permitan la correcta toma de decisiones y una adecuada gestión para el cumplimiento de los objetivos de la entidad en seguridad de la información y tratamiento de datos personales..												

Desarrollar una metodología de gestión de activos de la información, para elaboración de un inventario de activos de información exacto, actualizado y consistente, que permita definir la criticidad de los mismos, sus propietarios, custodios, usuarios, su clasificación y valoración.												
Actualizar el inventario de activos de la información correspondiente a la infraestructura tecnológica de la entidad a cargo de la Secretaría TIC, Innovación y Gobierno Abierto correspondiente al edificio central de la entidad y sus sedes externas (9 sedes): hardware, software, sistemas de información, Datacenter, redes de comunicaciones, dispositivos de red y centros de cableado, usando la matriz definida por MinTIC, debidamente documentada con la identificación, valoración y clasificación de activos de información. Incluir el inventario de activos de información correspondiente de bases de datos de información personal de la Gobernación de Nariño, según información identificada en la Secretaría TIC, Innovación y Gobierno Abierto. Este inventario hace parte del inventario general de activos de la información, usando la matriz definida por MinTIC.												
Actualizar inventario de activos de información de las dependencias de la entidad, con la participación de las mismas.												
Desarrollar una metodología de gestión del riesgo enfocada a procesos, que le permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos, así como la declaración de aplicabilidad, según norma ISO, lineamientos de MinTIC y guía de tratamiento de riesgos emitida por el DAFP.												
Actualizar la Matriz de análisis y evaluación de riesgos sobre inventario de activos de información construido.												
Actualizar el Plan de tratamiento de riesgos de seguridad de la información sobre												

inventario de activos de información construido.												
Actualizar la Declaración de Aplicabilidad sobre inventario de activos de información construido, debidamente documentada, aprobada por el comité institucional de gestión y desempeño.												
Elaborar un Plan de comunicaciones, sensibilización y capacitación que incluya la estrategia para que la seguridad de la información y tratamiento de datos personales, se convierta en cultura organizacional, al generar competencias y hábitos en el personal de la entidad para todos los niveles (directivo, funcionarios, contratistas, terceros).												
Aplicar el Plan de sensibilización mediante videos y piezas publicitarias, hacia el personal de la entidad.												
Actualizar el Plan de seguridad y privacidad de la información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo, teniendo como insumo la información construida en las etapas anteriores en el Diagnóstico y Planificación.												
Monitoreo permanente a los dispositivos de seguridad y firewall de nueva generación, aplicación de correctivos según vulnerabilidades detectadas.												