Tabla de contenido

1. Introducción 2
2. Objetivo. 2
3. Alcance. 2
4. Definiciones. 2
5. Condiciones y/o políticas específicas de operación. 6
6. Descripción del desarrollo de actividades 8
6.1. CRITERIOS DE SELECCIÓN DE INDICADORES 8
6.2. TIPOLOGIA DE INDICADORES 8
6.2.1. Indicadores de Gestión. 9
6.2.2. Indicadores de cumplimiento. 9
6.2.3. Indicadores de Desempeño. 9
6.2.4. Indicadores Financieros / Estratégicos. 9
6.3. INDICADORES DETALLADOS 10
6.3.1. Indicadores de GESTIÓN. 10
6.3.2. INDICADORES DE CUMPLIMIENTO. 15
6.3.3. INDICADORES DE DESEMPEÑO. 23
6.3.4. INDICADORES FINANCIEROS / ESTRATÉGICOS. 24
6.4. SEGUIMIENTO Y CONTROL 24
7. Documentos y registros relacionados 25
8. Anexos (cuando aplique) 25
9. Control de cambios. 25
10. Responsable. 25
11. Revisión, aprobación y verificación. 25

6.1.1. INTRODUCCIÓN

La Gobernación de Nariño, en cumplimiento de las disposiciones del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), adopta el presente documento de Indicadores de Implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), con el propósito de evaluar y monitorear el avance, eficacia y mejora continua de la gestión de la seguridad de la información en la entidad.

Estos indicadores permiten medir el grado de implementación de los controles, políticas, procedimientos y mecanismos asociados al MSPI, conforme a los lineamientos de la normatividad vigente, la Política de Gobierno Digital, y la Guía de Implementación del MSPI.

6.1.2. OBJETIVO.

Establecer un conjunto de indicadores que permitan evaluar de forma sistemática el nivel de implementación, madurez y efectividad de las acciones del Modelo de Seguridad y Privacidad de la Información (MSPI) en la Gobernación de Nariño, en sus componentes de efectividad, eficiencia y eficacia.

6.1.3. ALCANCE.

Aplica a todas las dependencias, funcionarios, contratistas/proveedores de la Gobernación de Nariño que intervienen en la gestión, tratamiento, protección y administración de los activos de información institucional y los datos personales.

6.1.4. DEFINICIONES.

- **Acceso remoto:** Uso de mecanismos tecnológicos para conectarse a sistemas internos desde ubicaciones externas.

- **Activo de información:** Toda información, elementos, servicios o personas, relacionados con la producción o tratamiento de información, que tengan valor para la entidad, y por lo tanto se deben administrar y proteger.

- **Acuerdo de confidencialidad:** Documento contractual mediante el cual una o ambas partes se comprometen a proteger y no divulgar información sensible o confidencial a la que tengan acceso durante la relación contractual, asegurando su uso exclusivo para los fines establecidos y previniendo accesos no autorizados, conforme a los requisitos legales, normativos y de seguridad de la organización.

- **Acuerdo de nivel de servicio (SLA)(ANS):** Es un contrato formal entre un proveedor de servicios y una entidad, que define claramente qué servicios se prestarán, cómo se medirán (tiempo de actividad, respuesta, resolución), los horarios, responsabilidades y las consecuencias (sanciones/compensaciones) si no se cumplen los objetivos de rendimiento acordados, asegurando expectativas claras y calidad del servicio

- **Amenaza:** Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.

- **Autenticación:** Proceso para validad la identidad de un usuario antes de permitir el acceso a un sistema.

- **Autorización:** Proceso mediante el cual se definen y asignan permisos a un usuario o rol para realizar acciones específicas.

- **Ciberseguridad:** Se entiende como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética, buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio de las interacciones digitales.

- **Confidencialidad:** Propiedad de la información que pretende garantizar que esta sólo es accedida por personas o sistemas autorizados.

- **Control:** Son todas aquellas políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

- **Control de acceso:** Conjunto de medidas, procesos y mecanismos que permiten autorizar, restringir, registrar y supervisar el acceso a la información, sistemas o recursos tecnológicos**.**

- **Correo electrónico institucional:** Es el servicio de correo que le asigna la entidad a cada colaborador para que lo utilice en el desarrollo de sus funciones.

- **Creación de usuario:** Procedimiento por el cual se asigna un usuario y contraseña a funcionarios, contratistas y terceras partes para el ingreso a la red institucional, correo electrónico, sistemas de información e infraestructura tecnológica.

- **Credenciales:** Medios utilizados para autenticar la identidad de un usuario: nombre de usuario, contraseña, tokens, certificados digitales, mfa, entre otros.

- **Dato:** Es una representación simbólica (numérica, alfabética, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.

- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

- **Dato personal privado:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para la persona titular del dato. Ejemplos: libros de los comerciantes, documentos privados, información extraída a partir de la inspección del domicilio.

- **Dato personal semiprivado:** Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato referente al cumplimiento e incumplimiento de las obligaciones financieras o los datos relativos a las relaciones con las entidades de la seguridad social, entre otros.

- **Dato público:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales, y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

- **Dato sensible:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

- **Disponibilidad:** Propiedad de la información que pretende garantizar el acceso y uso de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

- **Inactivación de usuario:** Proceso mediante el cual se suspende de manera temporal o definitiva el acceso del usuario a la red, correo electrónico, infraestructura tecnológica y sistemas de información dependiendo de la solicitud.

- **Indicador de implementación:** Herramienta cuantitativa o cualitativa que mide el progreso y el desempeño de una estrategia, plan o proyecto para asegurar que se están alcanzando los objetivos

- **Información:** Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

- **Información clasificada:** Información cuyo acceso se limita por razones legales, de seguridad, interés público o protección de datos personales.

- **Integridad:** Propiedad de la información que pretende mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

- **Modelo de Seguridad y Privacidad de la Información - MSPI**

- **Privilegios:** Capacidades o permisos concedidos a un usuario para ejecutar funciones dentro de un sistema.

- **Protección de datos personales:** Conjunto de técnicas jurídicas e informáticas encaminadas a garantizar los derechos de las personas sobre el control de su información personal y sobre la confidencialidad, integridad y disponibilidad de esta.

- **Proveedor:** Terceros que suministran bienes o servicios a una organización, incluyendo los que ofrecen servicios especializados de ciberseguridad para proteger los activos de información frente a amenazas y riesgos.

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

- **Roles y perfiles:** Estructura que agrupa permisos y responsabilidades asignadas a usuarios según su función dentro de la organización.

- **Seguridad digital:** Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante, incluye la seguridad de la información (Políticas, Procedimientos y demás controles) y la seguridad informática (Herramientas de seguridad).

- **Sistemas de información:** Es un conjunto de componentes interrelacionados que trabajan juntos para recopilar, procesar, almacenar y difundir información con el fin de apoyar la toma de decisiones y la obtención de objetivos organizacionales.

- **Transferencia de información:** Proceso mediante el cual la información es enviada, recibida o compartida entre personas, áreas, sistemas o terceros, utilizando medios

electrónicos o físicos.

- **Usuario:** Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información, para propósitos propios de su labor.

- **Vulnerabilidad:** Es una debilidad de un activo informático, o sistema de información que puede ser explotada por una o más amenazas para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

6.1.5. CONDICIONES Y/O POLÍTICAS ESPECÍFICAS DE OPERACIÓN.

La creación de indicadores de gestión está orientada principalmente a la medición de efectividad, eficiencia y eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, indicadores que servirán como insumo para el componente de mejora continua, permitiendo adoptar decisiones de mejora.

Los objetivos de estos procesos de medición en seguridad de la información son:

- Evaluar la efectividad de la implementación de los controles de seguridad.
- Evaluar la eficiencia del Modelo de Seguridad y Privacidad de la Información al interior de la entidad.
- Proveer estados de seguridad que sirvan de guía en las revisiones del Modelo de Seguridad y Privacidad de la Información, facilitando mejoras en seguridad de la información y nuevas entradas a auditar.
- Comunicar valores de seguridad al interior de la entidad.
- Servir como insumos al plan de análisis y tratamiento de riesgos.
- Permitir que se cuente con un proceso que demuestre si está siendo eficaz y está llegando a su punto de equilibrio dentro del sistema de gestión de seguridad de la información.

Acorde con la Guía para Diseño, Construcción e Interpretación de Indicadores del DANE, para la construcción de indicadores se debe tener en cuenta un tratamiento adecuado de la información que será la base del proceso de revisión control y mejora, de esta forma, dentro de la elaboración de indicadores se tienen definidos cuatro etapas específicas, como se menciona a continuación:

a. Identificación Del Objeto De La Medición

En este primer paso los encargados de la implementación del MSPI, deben tener en cuenta el Plan de Seguridad de la Información que se ha definido y de esta manera se desarrolla el objeto de medición sobre los aspectos que consideren más relevantes para evaluar, determinar qué tan fácil es recolectar la información asociada y que herramientas estoy empleando para obtener dicha información.

b. Definición De Las Variables

Una vez determinado el objeto de la medición, se definirán los aspectos que precisarán los datos que se recolectarán al levantar la información, así se determinarán los insumos, puntos de control, herramientas usadas y la relación entre estos aspectos o variables de medición.
En este sentido, las variables, una vez identificadas, deben ser definidas con la mayor rigurosidad, asignándole un sentido claro, para evitar que se originen ambigüedades y discusiones sobre sus resultados. Así mismo, se debe tener claridad de quién y cómo produce dicha información para de esta forma mejorar el criterio de confiabilidad.

c. Criterios de selección y calidad de los datos

El punto inicial es determinar si el indicador que se está eligiendo es de interés para la alta dirección, si va a permitir al líder de proyecto (el encargado de la seguridad de la información de la entidad) identificar la efectividad no solo del avance en la implementación, sino que, con esta recolección, medición y seguimiento del proyecto se logra demostrar cómo éste aporta al objetivo misional de la entidad.
Finalmente, es importante que el indicador sea sencillo de expresar, leer e interpretar, y como se menciona en la guía para la Administración del Riesgo y el diseño de controles en entidades públicas del Departamento Nacional de Planeación, debe elaborarse metodológicamente de forma sencilla, automática, sistemática y continua.

d. Diseño Del Indicador

El diseño del indicador implica, además, la realización de ciertas actividades o etapas que deben contemplarse en el proceso definitivo de construcción de indicadores.

Relación con otros marcos de referencia.

A continuación, se detalla una validación de la metodología utilizada con el marco de referencia ISO/IEC 27004:2016 (Gestión de métricas de seguridad de la información) y el marco de referencia de la NIST SP 800-55.

Aspecto	Guía del DANE	ISO/IEC 27004:2016	NIST SP 800-55 Rev.1
Propósito	Diseñar y construir indicadores de gestión institucional	Medir la eficacia del SGSI conforme a ISO/IEC 27001	Evaluar desempeño de controles de seguridad de la información
Enfoque	Evaluación de gestión pública y política basada en indicadores	Evaluación de controles y procesos dentro del SGSI	Evaluación de desempeño técnico, operacional y de impacto
Tipo de indicadores	Resultado, Producto, Eficiencia, Calidad, Impacto	Desempeño, Eficacia, Cumplimiento	Implementación, Eficacia, Eficiencia, Impacto
Ciclo de medición	Definir → Diseñar → Recolectar → Analizar → Interpretar	Planear > Medir > Analizar > Mejorar	Seleccionar → Desarrollar → Implementar → Analizar > Usar
Nivel de especificidad técnica	Media, orientada a procesos organizacionales y gestión institucional	Alta, con métricas alineadas a controles ISO/IEC 27001	Alta, orientada a sistemas de TI y operaciones de seguridad
Estructura del indicador	Nombre, definición, unidad, fórmula, frecuencia, fuente, interpretación	Objetivo, medida, fórmula, unidad, frecuencia, responsable, interpretación	Atributo, medida, fórmula, fuente, periodicidad, nivel de impacto
Marco normativo asociado	CONPES, Ley 87, Sistema de Gestión (MIPG)	ISO/IEC 27001 (SGSI)	NIST SP 800-53 (controles de seguridad)

6.1.6. DESCRIPCIÓN DEL DESARROLLO DE ACTIVIDADES

6.2. CRITERIOS DE SELECCIÓN DE INDICADORES

CRITERIO DE SELECCIÓN	PREGUNTA A TENER EN CUENTA	OBJETIVO
PERTINENCIA	¿El indicador expresa qué se quiere medir de forma clara y precisa?	Busca que el indicador permita describir la situación o fenómeno determinado, objeto de la acción.
FUNCIONALIDAD	¿El indicador es monitoreable?	Verifica que el indicador sea medible, operable y sensible a los cambios registrados en la situación inicial.
DISPONIBILIDAD	¿La información del indicador está disponible?	Los indicadores deben ser construidos a partir de variables sobre las cuales exista información estadística de tal manera que puedan ser consultados cuando sea necesario.
CONFIABILIDAD	¿De dónde provienen los datos?	Los datos deben ser medidos bajo ciertos estándares y la información requerida debe poseer atributos de calidad estadística.
UTILIDAD	¿El indicador es relevante con lo que se quiere medir?	Que los resultados y análisis permitan tomar decisiones.

6.3. TIPOLOGIA DE INDICADORES

6.3.1. INDICADORES DE GESTIÓN.

Corresponde a una medida que relaciona variables del proceso y permite administrar y hacer seguimiento real a un proceso o sistema de seguridad de la información, evaluando la efectividad, eficiencia y eficacia en la implementación de los controles y actividades definidos en el MSPI.

6.3.2. INDICADORES DE CUMPLIMIENTO.

Métricas diseñadas para medir el grado en que la entidad ha adoptado, desarrollado y puesto en funcionamiento el modelo de seguridad y privacidad de la información (MSPI)**,** definido por el ministerio tic para todas las entidades del estado. Miden qué tanto la Entidad ha implementado los controles, lineamientos, políticas y prácticas del MSPI, según lo exige el marco normativo de gobierno digital, para garantizar la confidencialidad, integridad y disponibilidad de la información, basándose en estándares internacionales como ISO 27001.

6.3.3. INDICADORES DE DESEMPEÑO.

Medida cuantitativa o cualitativa utilizada para evaluar el grado de avance, eficacia y cumplimiento de las actividades, controles y requisitos establecidos por el Modelo de Seguridad y Privacidad de la Información (MSPI).

Estos indicadores permiten monitorear cómo la entidad adopta, mantiene y mejora los procesos de seguridad y privacidad, identificando brechas, midiendo resultados y facilitando la toma de decisiones para garantizar la protección de los activos de información.

6.3.4. INDICADORES FINANCIEROS / ESTRATÉGICOS.

Son métricas diseñadas para medir **el** nivel de inversión, sostenibilidad económica y alineación estratégica que la Entidad realiza para implementar adecuadamente el modelo de seguridad y privacidad de la información (MSPI).

En esencia permiten responder a tres preguntas clave:

- ¿La entidad está destinando suficientes recursos para implementar el MSPI?
- ¿La inversión está alineada con la estrategia institucional y los riesgos identificados?
- ¿El gasto en seguridad de la información es eficiente, efectivo y sostenible en el tiempo?

6.4. INDICADORES DETALLADOS

6.4.1. INDICADORES DE GESTIÓN.

- **INDICADOR 01- ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN**

Definición: El indicador permite determinar y hacer seguimiento, al compromiso de la dirección, en cuanto a seguridad de la información, en lo relacionado con la asignación de personas y responsabilidades relacionadas a la seguridad de la información al interior de la entidad.

Objetivo: Hacer un seguimiento a la asignación de recursos y responsabilidades en gestión de seguridad de la información por parte de la alta dirección.

Descripción de variables:

VSI01: Número de personas que conforman el equipo de seguridad de la información con su respectivo rol y responsabilidades asignadas.
Fuente de Información: Lineamientos de roles y responsabilidades

VSI02: Número de personas que deberían conformar el equipo de seguridad de la información según la estructura definida por la entidad y que tengan responsabilidades de seguridad de la información definidas.
Fuente de Información: Actas de asignación de personal

Formula= (VSI01/VSI02) *100

Metas:

- **MÍNIMA:** 75-80%
- **SATISFACTORIA:** 80- 90%
- **SOBRESALIENTE: 100%**

Según los lineamientos establecidos en la sección de Roles y responsabilidades, hay que crear nuevos cargos y asignar responsabilidades en los actuales, por lo que el indicador está enfocado, no solo a la contratación de nuevas personas, sino a la asignación de responsabilidades.

- **INDICADOR 02 - CUBRIMIENTO DEL SGSI EN ACTIVOS DE INFORMACIÓN.**

Definición: El indicador permite determinar y hacer seguimiento al cubrimiento que se realiza a nivel de activos **c**ríticos de información de una entidad y los controles aplicados.

Objetivo: Hacer un seguimiento a la inclusión de nuevos activos críticos de información y sus controles, dentro del marco de seguridad y privacidad de la información.

Descripción de variables:

VSI03: Número de activos de información críticos incluidos en la gestión de riesgos de seguridad de la información con controles identificados
Fuente de Información: Alcance del SGSI, Inventario de Activos de información, plan de tratamiento, matriz de riesgos

VSI04: Número de activos de información críticos identificados en el inventario de activos de información.
Fuente de Información: Inventario de Activos de información

Formula= (VSI03/VSI04) *100

Metas:

- **MÍNIMA:** 75-80%
- **SATISFACTORIA:** 80- 90%
- **SOBRESALIENTE: 100%**

Los indicadores de cada proceso deben recolectarse y promediarse para construir un indicador que refleje el estado general de la entidad.

'Incluir un activo' implica gestionar su ciclo completo: clasificarlo, evaluar sus riesgos, definir controles para mitigarlos y aplicar el tratamiento correspondiente.

Este indicador mide la proporción de activos de información que han sido identificados como críticos (según el procedimiento de identificación, clasificación y valoración de activos de la entidad) y que están cubiertos por controles de seguridad.

- **INDICADOR 03 - TRATAMIENTO DE EVENTOS O INCIDENTES DE SEGURIDAD RELACIONADOS EN MARCO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Definición: Mide la eficiencia en la resolución de eventos e incidentes de seguridad de la información, reportados o detectados, con base en su cierre dentro del tiempo objetivo establecido por la entidad.

Objetivo: Evaluar la capacidad de la entidad para gestionar y resolver oportunamente los eventos e incidentes de seguridad de la información.

Descripción de variables:

VSI05: Número de eventos o incidentes cerrados dentro del tiempo objetivo.
Fuente de Información: Auditorías internas, herramientas de atención de servicios.

VSI06: Número total de eventos o incidentes reportados o detectados.

Fuente de Información: Auditorías internas, herramientas de atención de servicios.

Formula= (VSI05/VSI06) *100

Metas:

- **MÍNIMA:** 75-80%
- **SATISFACTORIA:** 80- 90%
- **SOBRESALIENTE: 100%**

La clasificación y priorización de los eventos e incidentes de seguridad se realiza conforme a los criterios establecidos en el procedimiento de gestión de incidentes de seguridad de la información de la entidad.

- **INDICADOR 04 – CUMPLIMIENTO DEL PLAN DE SENSIBILIZACIÓN**

Definición: El indicador permite medir cuántos usuarios aplican correctamente lo aprendido en las actividades de sensibilización en seguridad de la información.

Objetivo: El indicador pretende establecer la efectividad del plan de sensibilización en seguridad de la información y determinar si los usuarios finales aplican correctamente los conocimientos adquiridos en las actividades de sensibilización, como evidencia de la efectividad del plan.

Descripción de variables:

VSI07: Número de usuarios evaluados que aplicaron correctamente los contenidos sensibilizados.
Fuente de Información: Oficial de Seguridad de la Información, auditorías internas, atención al usuario, listas de asistencia, resultados de evaluaciones realizadas

VSI08: Total de personal capacitado durante el periodo evaluado.
Fuente de Información: Total, de funcionarios de la entidad
Formula= (VSI07/VSI08) *100

Metas:

- **MÍNIMA:** 75-80%
- **SATISFACTORIA:** 80- 90%
- **SOBRESALIENTE: 100%**

La evaluación debe incluir actividades prácticas, simulaciones o pruebas que midan la apropiación y aplicación de los contenidos sensibilizados.

- **INDICADOR 16 – PORCENTAJE DE IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN**

Definición: Mide el grado de avance en la implementación de los controles de seguridad establecidos en el plan de tratamiento de riesgos de la entidad, en el marco del Sistema de Gestión de Seguridad de la Información de la entidad.

Objetivo: Determinar el nivel de cumplimiento del plan de tratamiento de riesgos a través de la ejecución efectiva de los controles de seguridad definidos, permitiendo hacer seguimiento a la madurez de la gestión de riesgos de la entidad.

Descripción de variables:

VSI32: Número de controles implementados efectivamente, según evidencia técnica y documental.
Fuente de Información: Plan de tratamiento de riesgos, informes de auditoría.

VSI33: Número total de controles definidos para ser implementados en el periodo evaluado.
Fuente de Información: Plan de Tratamiento de riesgos.

Formula= (VSI032/VSI33) *100

Metas:

- **MÍNIMA:** 75-80%
- **SATISFACTORIA:** 80- 90%
- **SOBRESALIENTE: 100%**

La validación debe hacerse con base en el seguimiento al plan de tratamiento de riesgos, revisión de evidencia documental de implementación, informes técnicos o auditorías internas. La medición debe realizarse trimestral o semestralmente según el ciclo de implementación definido por la entidad.

- **INDICADOR 18 - IMPLEMENTACIÓN DE MECANISMOS DE INTELIGENCIA DE AMENAZAS**

Definición: Mide el grado de implementación de fuentes y mecanismos que permitan anticiparse a posibles amenazas mediante el análisis proactivo de datos internos y externos.

Objetivo: Evaluar la adopción de fuentes, procesos y herramientas que permitan anticiparse a posibles amenazas de seguridad mediante el análisis proactivo de información técnica y contextual.

Descripción de variables:

VSI36: Número de fuentes activas de inteligencia de amenazas utilizadas.

Fuente de Información: Plan de ciberinteligencia, boletines de CERT, CSIRT, SIEM, informes del área de seguridad.

VSI37: Número total de fuentes planeadas.
Fuente de Información: Plan de ciberinteligencia, boletines de CERT, CSIRT, SIEM informes del área de seguridad

Formula= (VSI032/VSI33) *100

Metas:

- **MÍNIMA:** 75-80%
- **SATISFACTORIA:** 80- 90%
- **SOBRESALIENTE: 100%**

Se deben considerar tanto amenazas técnicas como de ingeniería social. Evaluar semestralmente.

- **INDICADOR 20 – PORCENTAJE DE CANALES CRÍTICOS CON CONTROLES ACTIVOS DE PREVENCIÓN DE FUGA DE DATOS**

Definición: Mide el nivel de protección aplicado a los canales de comunicación críticos mediante controles de prevención de fuga de datos (DLP).

Objetivo: Medir la cobertura de las soluciones y medidas de prevención de pérdida de datos (DLP) implementadas en los canales utilizados para la transmisión, almacenamiento o compartición de información crítica.

Descripción de variables:

VSI39: Número de canales críticos protegidos por controles DLP.
Fuente de Información: Informes técnicos de herramientas DLP, matrices de canales críticos, configuraciones de seguridad, políticas de uso.

VSI40: Total de canales identificados como críticos.
Fuente de Información: Informes técnicos de herramientas DLP, matrices de canales críticos, configuraciones de seguridad, políticas de uso.

Formula= (VSI039/VSI40) *100

Metas:

- **MÍNIMA:** 75-80%
- **SATISFACTORIA:** 80- 90%
- **SOBRESALIENTE: 100%**

Los canales incluyen correo, almacenamiento externo, nube, impresoras, etc. La revisión debe hacerse al menos cada seis meses o tras un incidente relevante.

6.4.2. INDICADORES DE CUMPLIMIENTO.

- **INDICADOR 05 – CUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Definición: Mide el grado de cumplimiento de las políticas de seguridad y privacidad de la información en la entidad, con base en criterios definidos relacionados con existencia de política, organización interna y cumplimiento normativo.

Objetivo: Determinar si la entidad ha definido e implementado adecuadamente las políticas de seguridad de la información, y si cumple con los aspectos organizativos y normativos requeridos.

Descripción de variables:

VSI09: ¿Existe una política general de seguridad de la información formalizada y vigente?
Fuente de Información: Usuarios Internos

VSI10: ¿Existe una estructura organizativa con roles y responsabilidades claras?
Fuente de Información: Usuarios Internos

VSI11: ¿Se da cumplimiento a requisitos legales, reglamentarios y contractuales en el tratamiento de la información?
Fuente de Información: Usuarios Internos

Formula= (VSI09 + VSI10 + VSI11) / 3 * 100

Metas:

METAS CUMPLE SI / NO CUMPLE NO

- **MÍNIMA:** 75-80%
- **SATISFACTORIA:** 80- 90%
- **SOBRESALIENTE: 100%**

La validación de este indicador debe hacerse mediante revisión documental y entrevistas con responsables del SGSI, conforme a los lineamientos del Modelo de Operación de la Entidad. Se recomienda su actualización anual o tras cambios normativos o estructurales.

- **INDICADOR 06 - CUMPLIMIENTO DE LINEAMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Definición: Mide el nivel de cumplimiento de los lineamientos establecidos por la entidad para la gestión de la seguridad y privacidad de la información, considerando tanto su definición formal como su aplicación efectiva.

Objetivo: Evaluar si la entidad cuenta con lineamientos definidos y aplicados en materia de seguridad y privacidad de la información, y si estos son conocidos y adoptados por los funcionarios y contratistas como parte de sus responsabilidades.

Descripción de variables:

VSI12: Evidencia de lineamientos aplicados por funcionarios y contratistas que contribuyen a minimizar los riesgos sobre los activos de información.
Fuente de Información: lineamientos formales, encuestas a funcionarios.

VSI13: Evidencia de lineamientos definidos para cumplir las políticas de seguridad de la información.
Fuente de Información: lineamientos formales, encuestas a funcionarios.

Formula= (VSI12 / VSI13) * 100

Metas:

- **MÍNIMA:** 75-80%
- **SATISFACTORIA:** 80- 90%
- **SOBRESALIENTE: 100%**

La verificación debe realizarse mediante revisión documental de los lineamientos institucionales, encuestas o entrevistas a funcionarios y contratistas, y observación directa de medidas implementadas para proteger la información. Se recomienda realizar esta evaluación al menos una vez al año o cuando se actualicen las políticas de seguridad y privacidad de la información de la entidad.

- **INDICADOR 07 – EFECTIVIDAD OPERATIVA DEL CONTROL DE ACCESO**

Definición: Mide la efectividad de los controles de acceso implementados, con base en la detección y gestión de accesos no autorizados o intentos de acceso fallidos

Objetivo: Busca identificar la existencia de lineamientos, normas o estándares en cuanto al control de acceso en la entidad.

Descripción de variables:

VSI14: Número de accesos no autorizados detectados.

Fuente de Información: Revisión documental de políticas y procedimientos, entrevistas con responsables de TI, y evidencia de difusión o implementación.

VSI15: Total de intentos de acceso.
Fuente de Información: Revisión documental de políticas y procedimientos, entrevistas con responsables de TI, y evidencia de difusión o implementación.

Formula= VSI14/VSI15 * 100

Metas:

- **MÍNIMA:** 75-80%
- **SATISFACTORIA:** 80- 90%
- **SOBRESALIENTE: 100%**

La verificación debe realizarse mediante revisión documental de políticas y procedimientos, entrevistas con responsables de TI, y evidencia de difusión o implementación. Se recomienda su evaluación anual.

- **INDICADOR 08– CUMPLIMIENTO DE LINEAMIENTOS PARA EL ASEGURAMIENTO EN LA ADQUISICIÓN Y MANTENIMIENTO DE SOFTWARE**

Definición: Mide el nivel de cumplimiento de la entidad en cuanto a la existencia de lineamientos, normas o estándares que aseguren la incorporación de criterios de seguridad de la información en el desarrollo, adquisición y mantenimiento de software y servicios tecnológicos.

Objetivo: Verificar si la entidad ha definido e implementado lineamientos formales que aseguren la protección de los servicios tecnológicos en las fases de adquisición, desarrollo y mantenimiento de software, incluyendo la gestión de incidentes asociados.

Descripción de variables:

VSI17: ¿La entidad ha definido y documentado lineamientos, normas o estándares para el desarrollo o adquisición segura de software, sistemas y aplicaciones?
Fuente de Información: Usuarios Internos / Documentación técnica.

VSI18: ¿La entidad ha establecido lineamientos para la gestión de incidentes relacionados con fallas o vulnerabilidades en los servicios de software?
Fuente de Información: Usuarios Internos / Procedimientos.

Formula= (VSI17 + VSI18) / 2 * 100

Metas:

- **CUMPLIMIENTO TOTAL: 10**0%
- **CUMPLIMIENTO PARCIAL: 5**0%
- **NO CUMPLE: 0%**

La verificación debe realizarse mediante revisión documental de lineamientos sobre desarrollo/adquisición de software, análisis de contratos o convenios, entrevistas con responsables de TI y revisión de reportes de incidentes relacionados con software. La evaluación debe actualizarse al menos anualmente o cuando se implementen nuevos servicios.

- **INDICADOR 09 – CUMPLIMIENTO DE LINEAMIENTOS DE REGISTRO Y AUDITORÍA EN SEGURIDAD DE LA INFORMACIÓN**

Definición: Mide el cumplimiento de la entidad en cuanto a la definición e implementación de lineamientos, normas y/o estándares relacionados con el registro de eventos y auditorías de seguridad de la información.

Objetivo: Verificar si la entidad cuenta con directrices formalizadas para registrar eventos de seguridad y auditar periódicamente sus sistemas, con el fin de garantizar trazabilidad y mejora continua del modelo de seguridad.
Descripción de variables:

VSI19: ¿La entidad ha definido y aplica lineamientos o estándares para el registro y control de eventos en sus sistemas, redes y servicios?
Fuente de Información: Documentación institucional, revisión de logs, entrevistas.

VSI20: ¿La entidad realiza auditorías internas o externas periódicas sobre sus procesos y controles de seguridad de la información?
Fuente de Información: Informes de auditoría, cronogramas de verificación.

Formula= (VSI19 + VSI20) / 2 * 100

Metas:

- **CUMPLIMIENTO TOTAL: 10**0%
- **CUMPLIMIENTO PARCIAL: 5**0%
- **NO CUMPLE: 0%**

La verificación debe realizarse mediante revisión de lineamientos internos, políticas, bitácoras o registros de eventos, y evidencia de auditorías internas o de terceros. Es recomendable evaluar al menos una vez al año y cada vez que se actualicen los sistemas críticos.

- **INDICADOR 10 – IMPLEMENTACIÓN DE MECANISMOS PARA LA DETECCIÓN DE ANOMALÍAS EN LA INFRAESTRUCTURA Y SERVICIOS DE INFORMACIÓN**

Definición: Mide el nivel de implementación de mecanismos y herramientas en la entidad para detectar de manera proactiva vulnerabilidades, fallas o comportamientos anómalos que puedan afectar la seguridad en su infraestructura tecnológica, redes, sistemas, aplicaciones y servicios.

Objetivo: Verificar si la entidad ha adoptado e implementado mecanismos de monitoreo y análisis que permitan identificar oportunamente anomalías o vulnerabilidades en la prestación de sus servicios de información.

Descripción de variables:

VSI21: VAPRSG005: ¿La entidad ha implementado mecanismos para detectar periódicamente vulnerabilidades de seguridad en el funcionamiento de:

a) su infraestructura,
b) redes,
c) sistemas de información,
d) aplicaciones y/o
e) uso de los servicios?

Fuente de Información: Informes técnicos, reportes de monitoreo, hallazgos de no conformidades.

Formula= VSI0X = 1 (SÍ se evidencia)
VSIOX = 0 (NO se evidencia)

Metas:

- **CUMPLE: 1**
- **NO CUMPLE: 0**

Se puede descomponer la variable en subcomponentes (VSI21a–e) si se desea medir de forma más granular cada ámbito, en este caso la fórmula sería ((VSI21a + VSI21b + VSI21c + VSI21d + VSI21e) / 5) * 100.

La verificación debe realizarse mediante revisión de evidencias técnicas (reportes de escaneo de vulnerabilidades, alertas de monitoreo, sistemas SIEM, logs de eventos), entrevistas al equipo de TI, y validación de hallazgos registrados en auditorías o no conformidades. Se recomienda evaluación semestral o posterior a cambios significativos en infraestructura.

- **INDICADOR 11 – IMPLEMENTACIÓN DE POLÍTICAS DE PRIVACIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN**

Definición: Mide el nivel de implementación de políticas, lineamientos y controles relacionados con la privacidad de los datos personales y la confidencialidad de la información procesada por la entidad.

Objetivo: Verificar si la entidad ha establecido e implementado mecanismos que garanticen la protección de la información personal de los ciudadanos y la confidencialidad de los datos que gestionan o transfieren otras entidades a través de sus servicios.

Descripción de variables:

VSI22: ¿La entidad ha implementado lineamientos, normas y/o estándares para proteger la información personal y privada de los ciudadanos que utilicen sus servicios, en cumplimiento de la Ley 1581 de 2012 y demás normas aplicables?
Fuente de Información: Políticas institucionales, registros de cumplimiento, entrevistas.

VSI23: ¿La entidad ha implementado lineamientos, normas y/o estándares para proteger la información confidencial compartida por otras entidades?
Fuente de Información: Documentación técnica, acuerdos de confidencialidad, revisión de procesos.

Formula= VSI0X = 1 (SÍ se evidencia)
VSIOX = 0 (NO se evidencia)

Metas:

- **CUMPLE: 1**
- **NO CUMPLE: 0**

La validación debe realizarse mediante revisión de políticas de privacidad y confidencialidad definidas en la entidad, verificación de medidas técnicas y administrativas de protección de datos personales, entrevistas con responsables de tratamiento de la información y análisis de cumplimiento con el régimen legal aplicable en Colombia. Se recomienda evaluación anual o posterior a cambios normativos.

- **INDICADOR 12 – IMPLEMENTACIÓN DE POLÍTICAS Y MECANISMOS PARA LA INTEGRIDAD DE LA INFORMACIÓN**

Definición: Mide el nivel de implementación de políticas, lineamientos y controles orientados a garantizar la integridad de la información de la entidad, previniendo su alteración, pérdida o destrucción accidental o maliciosa.

Objetivo: Verificar si la entidad ha implementado mecanismos para prevenir, detectar y recuperar información ante eventos que comprometan su integridad, ya sean accidentales o intencionales.

Descripción de variables:

VSI24: ¿La entidad ha implementado lineamientos contra modificación o pérdida accidental de información?
Fuente de Información: Políticas institucionales, evidencias técnicas, entrevistas.

VSI25: ¿La entidad ha definido mecanismos de recuperación ante eventos que afecten la integridad de la información, tanto intencionales como accidentales?
Fuente de Información: Planes de contingencia, pruebas de restauración, revisión de procesos.

Formula= VSI0X = 1 (SÍ se evidencia)
VSIOX = 0 (NO se evidencia)

Metas:

- **CUMPLE: 1**
- **NO CUMPLE: 0**

La verificación debe realizarse a través de revisión documental de políticas de integridad, planes de respaldo, registros de restauración de datos, entrevistas a responsables de TI y pruebas de los mecanismos de control y recuperación. La evaluación debe realizarse al menos una vez al año.

- **INDICADOR 13 – IMPLEMENTACIÓN DE POLÍTICAS Y MECANISMOS PARA LA DISPONIBILIDAD DEL SERVICIO Y LA INFORMACIÓN**

Definición: Mide el nivel de implementación de políticas, normas y mecanismos orientados a garantizar la disponibilidad continua de los servicios de la entidad y el acceso oportuno a la información, especialmente en el contexto de servicios digitales.

Objetivo: Verificar si la entidad cuenta con lineamientos y controles implementados para garantizar la continuidad operativa y la alta disponibilidad de sus servicios de información, incluyendo servicios digitales esenciales.

Descripción de variables:

VSI26: ¿La entidad verifica el cumplimiento de lineamientos y estándares orientados a la continuidad del servicio y recuperación ante interrupciones?
Fuente de Información: Procedimientos, políticas de continuidad, evidencias de pruebas.

VSI27: ¿La entidad ha implementado mecanismos para que los servicios de Gobierno Digital tengan altos índices de disponibilidad?
Fuente de Información: Reportes de disponibilidad, herramientas de monitoreo, sistemas de respaldo.

Formula= VSI0X = 1 (SÍ se evidencia)
VSIOX = 0 (NO se evidencia)

Metas:

- **CUMPLE: 1**
- **NO CUMPLE: 0**

La verificación debe incluir revisión de políticas de continuidad, registros de pruebas de recuperación, reportes de monitoreo de disponibilidad, y entrevistas con responsables de TI. La evaluación se recomienda de forma semestral o posterior a incidentes que afecten la operación.

- **INDICADOR 14 – PROPORCIÓN DE ATAQUES INFORMÁTICOS CON IMPACTO EN LA CONTINUIDAD DEL SERVICIO**

Definición: Mide el porcentaje de ataques informáticos que, durante un periodo determinado, generaron interrupciones o afectaciones en la prestación de los servicios institucionales ofrecidos a ciudadanos o terceros.

Objetivo: Identificar el impacto real de los ataques informáticos en la operación de la entidad, evaluando la capacidad de los controles de seguridad para mitigar o contener amenazas que puedan comprometer la continuidad de los servicios.

Descripción de variables:

VSI28: Número total de ataques informáticos recibidos por la entidad en el último año.
Fuente de Información: Herramientas de monitoreo, reportes técnicos.

VSI29: Número de ataques informáticos que causaron interrupción o afectación en la prestación de servicios.
Fuente de Información: Herramientas de Monitoreo/Usuarios Internos.

Formula= (VSI29 / VSI28) * 100

Metas:

- **CUMPLE: 1**
- **NO CUMPLE: 0**

La fórmula indica el porcentaje de ataques exitosos o con impacto, que es una métrica de desempeño operativo.

- **INDICADOR 19 - PORCENTAJE DE SERVICIOS EN LA NUBE CON CONTROLES DE SEGURIDAD EVALUADOS Y DOCUMENTADOS**

Definición: Mide el porcentaje de servicios en la nube que han sido revisados formalmente en cuanto a cumplimiento de requisitos de seguridad de la información.

Objetivo: Verificar que los servicios en la nube utilizados por la entidad han sido formalmente evaluados en cuanto a riesgos de seguridad, cumplimiento normativo y controles asociados

Descripción de variables:

VSI37: Servicios en la nube con evaluación de seguridad documentada.
Fuente de Información: Contratos con proveedores, informes técnicos de seguridad, matrices de riesgo, auditorías internas.

VSI38: Total de servicios en la nube utilizados.

Formula= (VSI37 / VSI38) *100

Metas:

- **MÍNIMA:** 75-80%
- **SATISFACTORIA:** 80- 90%
- **SOBRESALIENTE: 100%**

Considerar servicios SaaS, PaaS o IaaS. Verifica si los controles incluyen cifrado, acceso seguro, respaldo, trazabilidad, etc. Se recomienda actualización anual.

6.4.3. INDICADORES DE DESEMPEÑO.

- **INDICADOR 15 – PORCENTAJE DE DISPONIBILIDAD DE LOS SERVICIOS EN LÍNEA DE LA ENTIDAD**

Definición: Mide el porcentaje de tiempo durante el cual los servicios en línea de la entidad estuvieron disponibles para los usuarios en un periodo determinado, en relación con el tiempo total esperado de funcionamiento.

Objetivo: Evaluar el desempeño operativo de los servicios en línea ofrecidos por la entidad, identificando su nivel de disponibilidad efectiva y permitiendo la mejora de la continuidad del servicio.

Descripción de variables:

VSI30: Tiempo total que el servicio en línea estuvo disponible durante el periodo evaluado.
Fuente de Información: Logs del sistema, herramientas de monitoreo.

VSI31: Tiempo total esperado de disponibilidad del servicio en ese mismo periodo.
Fuente de Información: SLA, planificación técnica.

Formula= (VSI30/VSI31)*100

Metas:

- **MÍNIMA:** 75-80%
- **SATISFACTORIA:** 80- 90%
- **SOBRESALIENTE: 100%**

Este indicador debe ser calculado con base en datos registrados por herramientas de monitoreo de infraestructura o reportes automáticos de uptime. Se recomienda una evaluación mensual o trimestral. Puede incluirse un umbral mínimo de disponibilidad definido por los SLA (acuerdos de nivel de servicio).

6.4.4. INDICADORES FINANCIEROS / ESTRATÉGICOS.

- **INDICADOR 17 – PROPORCIÓN DE INVERSIÓN EN SEGURIDAD DE LA INFORMACIÓN RESPECTO AL PRESUPUESTO GENERAL DE LA ENTIDAD**

Definición: Mide la proporción del presupuesto institucional que es destinada específicamente a actividades, servicios, soluciones y proyectos relacionados con la seguridad de la información, en comparación con el presupuesto total ejecutado por la entidad durante un periodo determinado.

Objetivo: Evaluar el nivel de inversión financiera orientada a la protección de los activos de información, permitiendo analizar la prioridad institucional otorgada a la seguridad de la información frente a otras áreas.

Descripción de variables:

VSI34: Monto total invertido por la entidad en iniciativas de seguridad de la información (proyectos, servicios, personal, infraestructura, consultorías, etc.).
Fuente de Información: Plan de adquisiciones.

VSI35: Total del presupuesto ejecutado por la entidad en el mismo periodo.
Fuente de Información: Plan de adquisiciones.

Formula= (VSI30/VSI31)*100

Metas:

- **MÍNIMA:** < 2%
- **SATISFACTORIA: 2- 4.9%**
- **SOBRESALIENTE: >=5%**

La inversión debe incluir gastos directos en seguridad de la información (infraestructura, capacitación, auditorías, herramientas tecnológicas, personal especializado), y excluir los gastos generales de TI no relacionados con seguridad. Se recomienda evaluar este indicador anualmente, alineado con el ciclo presupuestal.

6.5. SEGUIMIENTO Y CONTROL

Los resultados de los indicadores serán revisados en las sesiones del equipo de seguridad y gobierno digital y socializado en Comité Institucional de gestión y desempeño, con el fin de:

- Analizar avances y desviaciones.
- Definir acciones correctivas.
- Actualizar indicadores según las prioridades del MSPI en la Entidad.

7. Documentos y registros relacionados

Guía de implementación MSPI MinTIC.

8. Anexos

Indicadores de implementación MSPI V1 - Gobernación de Nariño

9. Control de cambios.

Versión	Fecha de versión	Descripción del cambio	Responsable
01	15/12/2025	Creación del documento	

10. Responsable.

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

11. Revisión, Aprobación y Verificación.

Revisión:	Aprobación:	Verificación:
Jonnathan Huertas Salas	Jonnathan Huertas Salas	Armando Rosero García
Secretario TIC, Innovación y Gobierno Abierto	Secretario TIC, Innovación y Gobierno Abierto	Secretario de Planeación