TIC

Lineamientos de Indicadores de Gestión de Seguridad de la Información

Ministerio de tecnologías de la información y las comunicaciones

MSPI

Julián Molina Gómez – Ministro de Tecnologías de la Información y las Comunicaciones
Yeimi Carina Murcia Yela - Viceministra de Transformación Digital
Lucy Elena Urón Rincón - Directora de Gobierno Digital
Luis Clímaco Córdoba Gómez - Subdirector de Estándares y Arquitectura de TI
Danny Alejandro Garzón Aristizábal – Contratista Subdirección de Estándares y Arquitectura de TI
German García Filoth – Contratista Subdirección de Estándares y Arquitectura de TI
Johanna Marcela Forero Varela - Profesional Especializado Subdirección de Estándares y Arquitectura de TI
Julio Andrés Sánchez Sánchez - Contratista Subdirección de Estándares y Arquitectura de TI
Lourdes María Acuña Acuña - Contratista de la Dirección de Gobierno Digital
Tairo Elías Mendoza Piedrahita - Profesional Especializado Dirección de Gobierno Digital
Andrés Díaz Molina- Jefe de la Oficina de Tecnologías de la Información
Nelson Barrios Perdomo – Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Adriana María Pedraza - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Camilo Andrés Jiménez - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Emanuel Elberto Ortiz - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Angela Janeth Cortés Hernández - Oficial de Seguridad y Privacidad de la Información GIT de Seguridad y Privacidad de la Información.

Ministerio de Tecnologías de la Información y las Comunicaciones
Viceministerio de Transformación Digital
Dirección de Gobierno Digital

Versión	**Observaciones**
Versión 5 21/04/2025	Lineamientos de Indicadores De Gestión De Seguridad De La Información Dirigida a las entidades del Estado

Comentarios, sugerencias o correcciones pueden ser enviadas al correo electrónico: gobiernodigital@mintic.gov.co

Tabla de contenido

Listado de Tablas

Lineamientos de Indicadores De Gestión De Seguridad De La Información

1. Objetivo de la medición

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.

Nota: Los objetivos de seguridad deben ser monitoreados, y este monitoreo debe estar disponible como “información documentada”

2. Construcción de indicadores

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:

2.1. 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.

2.2. 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.[5]

2.3. 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.

2.4. 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.

[5] GUÍA PARA LA CONSTRUCCIÓN Y ANÁLISIS DE INDICADORES, Departamento Nacional de Planeación.

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 donde provienen los datos?	Los datos deben ser medidos siempre 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.

Tabla 1 Criterios para selección de indicadores

Fuente: Guía para Diseño, Construcción e Interpretación de Indicadores. Metodología línea base de indicadores, DANE 2009.

3. 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)

Tabla 2 Relación con otros marcos de referencia

Nota. Tener presente que el marco de referencia a utilizar para la definición de indicadores es de acuerdo como lo tenga definido la entidad en su sistema de calidad.

4. Indicadores Propuestos

A continuación, se definen una serie de indicadores para medir la gestión y el cumplimiento en el avance de la implementación del Modelo de Seguridad y Privacidad de la Información.

Estos indicadores son ejemplos que pueden ser adoptados por las entidades o modificados de acuerdo con sus necesidades.

<table>
<tr><td colspan="6">INDICADOR 01- ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN.</td></tr>
<tr><td colspan="2">IDENTIFICADOR</td><td colspan="4">SGIN01</td></tr>
<tr><td colspan="6">DEFINICIÓN</td></tr>
<tr><td colspan="6">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</td></tr>
<tr><td colspan="6">OBJETIVO</td></tr>
<tr><td colspan="6">Hacer un seguimiento a la asignación de recursos y responsabilidades en gestión de seguridad de la información por parte de la alta dirección.</td></tr>
<tr><td colspan="6">TIPO DE INDICADOR</td></tr>
<tr><td colspan="6">Indicador de Gestión</td></tr>
<tr><td colspan="2">DESCRIPCIÓN DE VARIABLES</td><td colspan="2">FORMULA</td><td colspan="2">FUENTE DE INFORMACIÓN</td></tr>
<tr><td colspan="2">VSI01: Número de personas que conforman el equipo de seguridad de la información con su respectivo rol y responsabilidades asignadas.</td><td colspan="2" rowspan="2">(VSI01/VSI02) *100</td><td colspan="2">Lineamientos de roles y responsabilidades.</td></tr>
<tr><td colspan="2">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.</td><td colspan="2">Actas de asignación de personal.</td></tr>
<tr><td colspan="6">METAS</td></tr>
<tr><td>MÍNIMA</td><td>75-80%</td><td>SATISFACTORIA</td><td>80- 90%</td><td>SOBRESALIENTE</td><td>100%</td></tr>
<tr><td colspan="6">OBSERVACIONES</td></tr>
</table>

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.					
IDENTIFICADOR	SGIN02				
DEFINICIÓN					
El indicador permite determinar y hacer seguimiento al cubrimiento que se realiza a nivel de activos **críticos** 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.					
TIPO DE INDICADOR					
Indicador de Gestión					
DESCRIPCIÓN DE VARIABLES		FORMULA		FUENTE DE INFORMACIÓN	
VSI03: Número de activos de información críticos incluidos en la gestión de riesgos de seguridad de la información con controles identificados.		(VSI03/VSI04) *100		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.				Inventario de Activos de información.	
METAS					
MÍNIMA	75-80%	SATISFACTORIA	80-90%	SOBRESALIENTE	100%
OBSERVACIONES					
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					
IDENTIFICADOR	SGIN03				
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.					
TIPO DE INDICADOR					
Indicador de Gestión					
DESCRIPCIÓN DE VARIABLES		FORMULA		FUENTE DE INFORMACIÓN	
VSI05: Número de eventos o incidentes cerrados dentro del tiempo objetivo.		(VSI05/VSI06) *100		Auditorías internas, herramientas de atención de servicios	
VSI06: Número total de eventos o incidentes reportados o detectados.				Auditorías internas, herramientas de atención de servicios	
METAS					
MÍNIMA	75-80%	SATISFACTORIA	80- 90%	SOBRESALIENTE	100%
OBSERVACIONES					
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					
IDENTIFICADOR	SGIN04				
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.					
TIPO INDICADOR					
Indicador de Gestión					
DESCRIPCIÓN DE VARIABLES		FORMULA		FUENTE DE INFORMACIÓN	
VSI07: Número de usuarios evaluados que aplicaron correctamente los contenidos sensibilizados.		(VSI07/VSI08) *100		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.				Total, de funcionarios de la entidad.	
METAS					
MÍNIMA	75-80%	SATISFACTORIA	80-90%	SOBRESALIENTE	100%
OBSERVACIONES					
La evaluación debe incluir actividades prácticas, simulaciones o pruebas que midan la apropiación y aplicación de los contenidos sensibilizados.					

INDICADOR 05 – CUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
IDENTIFICADOR SGIN05
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.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		FORMULA	FUENTE DE INFORMACIÓN
VSI09: ¿Existe una política general de seguridad de la información formalizada y vigente?		(VSI09 + VSI10 + VSI11) / 3 * 100	Usuarios Internos
VSI10: ¿Existe una estructura organizativa con roles y responsabilidades claras?			Usuarios Internos
VSI11: ¿Se da cumplimiento a requisitos legales, reglamentarios y contractuales en el tratamiento de la información?			Usuarios Internos
METAS CUMPLE SI / NO CUMPLE NO			
MÍNIMA 75-80%	**SATISFACTORIA** 80-90%	SOBRESALIENTE	100%
OBSERVACIONES			
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	
IDENTIFICADOR	SGIN06
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.	
TIPO INDICADOR	
Indicador de Cumplimiento	

DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
VSI12: Evidencia de lineamientos aplicados por funcionarios y contratistas que contribuyen a minimizar los riesgos sobre los activos de información.	(VSI12 / VSI13) * 100	lineamientos formales, encuestas a funcionarios
VSI13: Evidencia de lineamientos definidos para cumplir las políticas de seguridad de la información.		lineamientos formales, encuestas a funcionarios

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

OBSERVACIONES
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	
IDENTIFICADOR	SGIN07
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.	
TIPO INDICADOR	
Indicador de Cumplimiento	

DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
VSI14: Número de accesos no autorizados detectados	VSI14/VSI15 * 100	Revisión documental de políticas y procedimientos, entrevistas con responsables de TI, y evidencia de difusión o implementación.

VSI15: Total de intentos de acceso			Revisión documental de políticas y procedimientos, entrevistas con responsables de TI, y evidencia de difusión o implementación.
METAS			
MÍNIMA 75-80%	SATISFACTORIA 80-90%	SOBRESALIENTE	100%
OBSERVACIONES			
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			
IDENTIFICADOR	SGIN08		
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.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		FORMULA	FUENTE DE INFORMACIÓN
VSI17: ¿La entidad ha definido y documentado lineamientos, normas o estándares para el desarrollo o adquisición segura de software, sistemas y aplicaciones?		(VSI17 + VSI18) / 2 * 100	Usuarios Internos / Documentación técnica

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

METAS			
CUMPLIMIENTO TOTAL	100%	CUMPLIMIENTO PARCIAL 50%	NO CUMPLE 0%

OBSERVACIONES

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		
IDENTIFICADOR	SGIN09	
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.		
TIPO INDICADOR		
Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
VSI19: ¿La entidad ha definido y aplica lineamientos o estándares para el registro y control de eventos en sus sistemas, redes y servicios?	(VSI19 + VSI20) / 2 * 100	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?			Informes de auditoría, cronogramas de verificación
METAS			
CUMPLIMIENTO TOTAL	100%	CUMPLIMIENTO PARCIAL 50%	NO CUMPLE 0%
OBSERVACIONES			
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			
IDENTIFICADOR			
DEFINICIÓN	SGIN10		
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.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		FORMULA	FUENTE DE INFORMACIÓN
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		VSI0X = 1 (SÍ se evidencia)	Informes técnicos, reportes de monitoreo, hallazgos de no conformidades

e) uso de los servicios?		VSIOX = 0 (NO se evidencia)	
METAS			
CUMPLE	1	NO CUMPLE	0
OBSERVACIONES			
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			
IDENTIFICADOR	SGIN11		
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.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		FORMULA	FUENTE DE INFORMACIÓN
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?			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?	VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	Documentación técnica, acuerdos de confidencialidad, revisión de procesos

METAS			
CUMPLE	1	NO CUMPLE	0

OBSERVACIONES

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	
IDENTIFICADOR	SGIN12

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.

TIPO INDICADOR

Indicador de Cumplimiento

DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
VSI24: ¿La entidad ha implementado lineamientos contra modificación o pérdida accidental de información?	VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	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?		Planes de contingencia, pruebas de restauración, revisión de procesos

METAS			
CUMPLE	1	NO CUMPLE	0
OBSERVACIONES			
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			
IDENTIFICADOR	SGIN13		
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.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		FORMULA	FUENTE DE INFORMACIÓN
VSI26: ¿La entidad verifica el cumplimiento de lineamientos y estándares orientados a la continuidad del servicio y recuperación ante interrupciones?		VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	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?			Reportes de disponibilidad, herramientas de monitoreo, sistemas de respaldo
METAS			
CUMPLE	1	NO CUMPLE	0
OBSERVACIONES			
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			
IDENTIFICADOR	SGIN14		
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.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		FORMULA	FUENTE DE INFORMACIÓN
VSI28: Número total de ataques informáticos recibidos por la entidad en el último año		(VSI29 / VSI28) * 100	Herramientas de monitoreo, reportes técnicos
VSI29: Número de ataques informáticos que causaron interrupción o afectación en la prestación de servicios			Herramientas de Monitoreo/Usuarios Internos.
METAS			
CUMPLE	1	NO CUMPLE	0
OBSERVACIONES			
La fórmula indica el porcentaje de ataques exitosos o con impacto, que es una métrica de desempeño operativo.			

INDICADOR 15 – PORCENTAJE DE DISPONIBILIDAD DE LOS SERVICIOS EN LÍNEA DE LA ENTIDAD	
IDENTIFICADOR	SGIN15
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.			
TIPO INDICADOR			
Indicador de Desempeño			
DESCRIPCIÓN DE VARIABLES		FORMULA	FUENTE DE INFORMACIÓN
VSI30: Tiempo total que el servicio en línea estuvo disponible durante el periodo evaluado		(VSI30/VSI31)*100	Logs del sistema, herramientas de monitoreo
VSI31: Tiempo total esperado de disponibilidad del servicio en ese mismo periodo			SLA, planificación técnica
METAS			
MÍNIMA 75-80%	**SATISFACTORIA** 80-90%	SOBRESALIENTE	100%
OBSERVACIONES			
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).			

INDICADOR 16 – PORCENTAJE DE IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN	
IDENTIFICADOR	SGIN16
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.	

TIPO INDICADOR					
Indicador de Gestión					
DESCRIPCIÓN DE VARIABLES		FORMULA		FUENTE DE INFORMACIÓN	
VSI32: Número de controles implementados efectivamente, según evidencia técnica y documental		(VSI032/VSI33) *100		Plan de tratamiento de riesgos, informes de auditoría.	
VSI33: Número total de controles definidos para ser implementados en el periodo evaluado				Plan de Tratamiento de riesgos.	
METAS					
MÍNIMA	75-80%	SATISFACTORIA	80-90%	SOBRESALIENTE	100%
OBSERVACIONES					
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 17 – PROPORCIÓN DE INVERSIÓN EN SEGURIDAD DE LA INFORMACIÓN RESPECTO AL PRESUPUESTO GENERAL DE LA ENTIDAD		
IDENTIFICADOR	SGIN17	
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.		
TIPO INDICADOR		
Indicador Financiero / Estratégico		
DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
VSI34: Monto total invertido por la entidad en iniciativas de seguridad de la información (proyectos, servicios,	(VSI34 / VSI35) * 100	Plan de adquisiciones

personal, infraestructura, consultorías, etc.)					
VSI35: Total del presupuesto ejecutado por la entidad en el mismo periodo				Plan de adquisiciones	
METAS					
MÍNIMA	< 2%	SATISFACTORIA	2–4.9%	SOBRESALIENTE	≥ 5%
OBSERVACIONES					
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 directamente con seguridad. Se recomienda evaluar este indicador anualmente, alineado con el ciclo presupuestal.					

INDICADOR 18 - IMPLEMENTACIÓN DE MECANISMOS DE INTELIGENCIA DE AMENAZAS		
IDENTIFICADOR	SGIN18	
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.		
TIPO INDICADOR		
Indicador de Gestión		
DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
VSI36: Número de fuentes activas de inteligencia de amenazas utilizadas	(VSI032/VSI33) *100	Plan de ciber inteligencia, boletines de CERT, CSIRT, SIEM, informes del área de seguridad.
VSI37: Número total de fuentes planeadas		Plan de ciber inteligencia, boletines de CERT, CSIRT, SIEM,

				informes del área de seguridad.	
METAS					
MÍNIMA	75-80%	SATISFACTORIA	80- 90%	SOBRESALIENTE	100%
OBSERVACIONES					
Se deben considerar tanto amenazas técnicas como de ingeniería social. Evaluar semestralmente.					

INDICADOR 19 - PORCENTAJE DE SERVICIOS EN LA NUBE CON CONTROLES DE SEGURIDAD EVALUADOS Y DOCUMENTADOS					
IDENTIFICADOR SGIN19					
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.					
TIPO DE INDICADOR					
Indicador de Cumplimiento					
DESCRIPCIÓN DE VARIABLES		FORMULA		FUENTE DE INFORMACIÓN	
VSI37 Servicios en la nube con evaluación de seguridad documentada		(VSI37 / VSI38) *100		Contratos con proveedores, informes técnicos de seguridad, matrices de riesgo, auditorías internas.	
VSI38 Total de servicios en la nube utilizados					
MINIMA	75-80%	**SATISFACTORIA**	80- 90%	**SOBRESALIENTE**	100%
OBSERVACIONES					
Considerar servicios SaaS, PaaS o IaaS. Verifica si los controles incluyen cifrado, acceso seguro, respaldo, trazabilidad, etc. Se recomienda actualización anual.					

<table>
<tr><td colspan="6">INDICADOR 20 – PORCENTAJE DE CANALES CRÍTICOS CON CONTROLES ACTIVOS DE PREVENCIÓN DE FUGA DE DATOS</td></tr>
<tr><td colspan="2">IDENTIFICADOR</td><td colspan="4">SGIN20</td></tr>
<tr><td colspan="6">DEFINICIÓN</td></tr>
<tr><td colspan="6">Mide el nivel de protección aplicado a los canales de comunicación críticos mediante controles de prevención de fuga de datos (DLP).</td></tr>
<tr><td colspan="6">OBJETIVO</td></tr>
<tr><td colspan="6">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.</td></tr>
<tr><td colspan="6">TIPO INDICADOR</td></tr>
<tr><td colspan="6">Indicador de Gestión</td></tr>
<tr><td colspan="2">DESCRIPCIÓN DE VARIABLES</td><td colspan="2">FORMULA</td><td colspan="2">FUENTE DE INFORMACIÓN</td></tr>
<tr><td colspan="2">VSI39: Número de canales críticos protegidos por controles DLP</td><td colspan="2" rowspan="2">(VSI039/VSI40) *100</td><td colspan="2">Informes técnicos de herramientas DLP, matrices de canales críticos, configuraciones de seguridad, políticas de uso.</td></tr>
<tr><td colspan="2">VSI40: Total de canales identificados como críticos</td><td colspan="2">Informes técnicos de herramientas DLP, matrices de canales críticos, configuraciones de seguridad, políticas de uso.</td></tr>
<tr><td colspan="6">METAS</td></tr>
<tr><td>MÍNIMA</td><td>75-80%</td><td>SATISFACTORIA</td><td>80-90%</td><td>SOBRESALIENTE</td><td>100%</td></tr>
<tr><td colspan="6">OBSERVACIONES</td></tr>
<tr><td colspan="6">Los canales incluyen correo, almacenamiento externo, nube, impresoras, etc. La revisión debe hacerse al menos cada seis meses o tras un incidente relevante.</td></tr>
</table>

TIC

Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética Nacional

Ministerio de tecnologías de la información y las comunicaciones

MSPI

Julián Molina Gómez – Ministro de Tecnologías de la Información y las Comunicaciones
Yeimi Carina Murcia Yela - Viceministra de Transformación Digital
Lucy Elena Urón Rincón - Directora de Gobierno Digital
Luis Clímaco Córdoba Gómez - Subdirector de Estándares y Arquitectura de TI
Danny Alejandro Garzón Aristizábal – Contratista Subdirección de Estándares y Arquitectura de TI
German García Filoth – Contratista Subdirección de Estándares y Arquitectura de TI
Johanna Marcela Forero Varela - Profesional Especializado Subdirección de Estándares y Arquitectura de TI
Julio Andrés Sánchez Sánchez - Contratista Subdirección de Estándares y Arquitectura de TI
Lourdes María Acuña Acuña - Contratista de la Dirección de Gobierno Digital
Tairo Elías Mendoza Piedrahita - Profesional Especializado Dirección de Gobierno Digital
Andrés Díaz Molina- Jefe de la Oficina de Tecnologías de la Información
Nelson Barrios Perdomo – Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Adriana María Pedraza - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Camilo Andrés Jiménez - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Emanuel Elberto Ortiz - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Angela Janeth Cortés Hernández - Oficial de Seguridad y Privacidad de la Información GIT de Seguridad y Privacidad de la Información.

Ministerio de Tecnologías de la Información y las Comunicaciones
Viceministerio de Transformación Digital
Dirección de Gobierno Digital

Versión	**Observaciones**
Versión 5 21/04/2025	Documento Maestro del Modelo de Seguridad y Privacidad de la Información Dirigida a las entidades del Estado

Comentarios, sugerencias o correcciones pueden ser enviadas al correo electrónico: gobiernodigital@mintic.gov.co

Modelo de Seguridad y Privacidad de la Información
Documento Maestro V 5.0

Tabla de contenido

Listado de Tablas

Gestión inventario clasificación de activos e infraestructura critica Cibernética

El presente documento detalla los lineamientos básicos que se deben tener en cuenta para realizar una adecuada identificación, gestión y clasificación de activos de información e infraestructura critica cibernética de cada entidad.

- Establecer las responsabilidades de los funcionarios y contratistas de la entidad con los activos de información.
- Garantizar que los activos de información de la entidad reciban un adecuado nivel de protección de acuerdo con su valoración.
- Proporcionar una herramienta que visualice de manera fácil los activos de información de la entidad.
- Sensibilizar y promover la importancia de los activos de información de la entidad.
- Proveer las pautas requeridas y necesarias para la adecuada identificación, clasificación y valoración de los activos de información de la entidad.
- Cumplir con la organización y publicación de los activos de información, respetando tanto las normas como los procedimientos que se deben cumplir.

El inventario y clasificación de activos hace parte de las actividades más relevantes e importantes del Modelo de Seguridad y Privacidad de la Información y está compuesta por las fases:

- **Identificación y Tipificación de los Activos de Información**: Corresponde a la etapa en donde la dependencia como propietario y custodio de la información, identifica y clasifica la información producida, de acuerdo con: Activos de información puros, de Tecnologías de la Información, de Talento humano y Servicios.
- **Clasificación de los activos de Información**: Corresponde a la etapa en donde la dependencia como propietario y custodio de la información califica los activos de información teniendo en cuenta los criterios de confidencialidad, integridad y disponibilidad, conforme a los principios de seguridad de la información. Adicionalmente, los debe alinear con la Ley 1712 de 2014 sobre acceso a la información pública y la Ley 1581 de 2012 sobre protección de datos personales, garantizando un tratamiento diferencial según el tipo de activo clasificado.
- **Revisión y Aprobación**: Corresponde a la etapa en donde se valida la clasificación y valoración dada a los activos de información, para la presentación y aprobación por parte del dueño o responsable de los activos.

- **Publicación de los Activos de Información**: Corresponde a la etapa de publicación de la información en la página web de la entidad, Link de transparencia y acceso a la Información Pública, Portal de Datos Abiertos del estado colombiano o el sitio que lo modifique o sustituya.