Guía de indicadores de gestión para la seguridad de la información

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Guía No. 9

MINTIC vive digital Colombia TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN

HISTORIA

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
2.0	11/30/2011	Documento del Modelo Anterior
3.0	25/05/2015	Ajustes por Restructuración del Modelo

TABLA DE CONTENIDO

1. DERECHOS DE AUTOR

Todas las referencias a los documentos del Modelo de Seguridad y Privacidad de la Información, con derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno en Línea.

Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en la norma técnica colombiana NTC ISO/IEC 27001 e ISO 27004 vigente, así como a los anexos con derechos reservados por parte de ISO/ICONTEC.

2. AUDIENCIA

Entidades públicas de orden nacional y entidades públicas del orden territorial, así como proveedores de servicios de Gobierno en Línea, y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de la información en el marco de la Estrategia de Gobierno en Línea.

3. INTRODUCCIÓN

En esta guía encontrara una serie de indicadores[1] de gestión que podrían ser utilizados al interior de su entidad para medir la efectividad, eficacia y eficiencia de la Seguridad de la Información dentro de la entidad,

[1] **Indicador:** Relación entre variables cuantitativas o cualitativas que permiten observar la situación y las tendencias de cambio con respecto a objetivos, metas trazadas y resultados esperados.

4. OBJETIVO DE LA MEDICION

La creación de indicadores de gestión está orientada principalmente en 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.

5. INDICADORES PROPUESTOS

A continuación se definen una serie de indicadores para medir la gestión[2] y el cumplimiento[3] en el avance de implementación del Nuevo Modelo de Seguridad y Privacidad de la Información, dichos indicadores son:

INDICADOR 01- ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN.					
IDENTIFICADOR	SGIN01				
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 gestio de seguridad de la información, por parte de la alta dirección.					
TIPO DE INDICADOR					
Indicador de Gestión					
DESCRIPCIÓN DE VARIABLES		**FORMULA**		**FUENTE DE INFORMACIÓN**	
VSI01: Número de personas con su respectivo rol definió según el modelo de operación capítulo 2		(VSI01/VSI02)*100		Capítulo 2 de la guía del modelo de operación del marco de seguridad y privacidad de la información	
VSI02: Número de personas con su respectivo rol definió después de un año				Actas de asignación de personal.	
METAS					
MÍNIMA	**75-80%**	**SATISFACTORIA**	80- 90%	**SOBRESALIENTE**	100%
OBSERVACIONES					
De acuerdo a lo establecido en el capítulo 2 de la guía del modelo de operación del marco de seguridad y privacidad de la información, es necesario crear nuevos cargos y asignar responsabilidades en los actuales, por lo tanto, el indicador está enfocado, no solo a la contratación de nuevas personas, sí no 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 su control, dentro del marco de seguridad y privacidad de la información.	

[2] Indicador de Gestión: Los indicadores de gestión están relacionados con las razones que permiten administrar realmente un proceso o un sistema.
[3] Indicador de Cumplimiento: De cumplimiento están relacionados con las razones que indican el grado de consecución de tareas.

INDICADOR 02 - CUBRIMIENTO DEL SGSI EN ACTIVOS DE INFORMACIÓN.					
TIPO DE INDICADOR					
Indicador de Gestión					
DESCRIPCIÓN DE VARIABLES		**FORMULA**		**FUENTE DE INFORMACIÓN**	
VSI03: Número de activos críticos de información incluidos en el alcance de implementación del modelo, incluidos en la zona de riesgo inaceptable y la implementación del control no requiere adquisición de elementos de hardware o software.		(VSI03/VSI04)*100		Alcance del SGSI, Inventario de Activos de información, plan de tratamiento, matriz de riesgos	
VSI04: Número de activos críticos de información incluidos en el alcance de implementación del modelo; activos incluidos en la zona de riesgo inaceptable.				Inventario de Activos de información, nuevos	
METAS					
MÍNIMA	75-80%	**SATISFACTORIA**	80-90%	**SOBRESALIENTE**	100%
OBSERVACIONES					
El indicador de cada proceso debe ser recolectado y promediado para construir un indicador que refleje el estado a nivel empresa. El terminó “incluir un activo” debe ser entendido como realizar la correcta clasificación del activo, tratamiento, evaluación de riesgos sobre el mismo y determinación de controles para minimizar el riesgo calculado. Para este indicador, solo se tienen en cuenta los controles que no implican adquisición de hardware o software.					

INDICADOR 03 - TRATAMIENTOS DE EVENTOS RELACIONADOS EN MARCO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
IDENTIFICADOR	SGIN03	
DEFINICIÓN		
El indicador permite determinar la eficiencia en el tratamiento de eventos relacionados la seguridad de la información. Los eventos serán reportados por los usuarios o determinadas en las auditorías planeadas para el sistema.		
OBJETIVO		
El objetivo del indicador es reflejar la gestión y evolución del modelo de seguridad y privacidad de la información al interior de una entidad		
TIPO DE INDICADOR		
Indicador de Gestión		
DESCRIPCIÓN DE VARIABLES	**FORMULA**	**FUENTE DE INFORMACIÓN**
VSI05: Número de anomalías cerradas.	(VSI05/VSI06)*100	Auditorías internas, herramientas de monitoreo

INDICADOR 03 - TRATAMIENTOS DE EVENTOS RELACIONADOS EN MARCO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN					
VSI06: Número total de anomalías encontradas.				Auditorías internas, herramientas de monitoreo	
METAS					
MÍNIMA	75-80%	**SATISFACTORIA**	80- 90%	**SOBRESALIENTE**	100%

INDICADOR – PLAN DE SENSIBILIZACIÓN					
IDENTIFICADOR	SGIN04				
DEFINICIÓN					
El indicador permite medir la aplicación de los temas sensibilizados en seguridad de la información por parte de los usuarios finales. Estas mediciones se podrán realizar por medio de auditorías especializadas en el tema o de forma aislada por parte de los responsables de la capacitación y sensibilización.					
OBJETIVO					
El objetivo del indicador es establecer la efectividad de un plan de capacitación y sensibilización previamente definido como medio para el control de incidentes de seguridad.					
TIPO INDICADOR					
Indicador de Gestión					
DESCRIPCIÓN DE VARIABLES		**FORMULA**		**FUENTE DE INFORMACIÓN**	
VSI07: Número de fallas o no cumplimientos encontrados en las sensibilizaciones programadas o eventos realizados para evaluar el tema.		(VSI07/VSI08)*100		Oficial de Seguridad de la Información, auditorías internas, atención al usuario, listas de asistencia	
VSI08: Total de personal a capacitar.				Total de funcionarios de la entidad.	
METAS					
MÍNIMA	75-80%	**SATISFACTORIA**	80- 90%	**SOBRESALIENTE**	100%
OBSERVACIONES					
Para el levantamiento de la información que permita obtener datos para la medición el responsable debe idear planes, laboratorios o actividades periódicas que permitan medir lo capacitado o divulgado.					

INDICADOR – CUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN LA ENTIDAD
IDENTIFICADOR SGIN05
DEFINICIÓN
Cumplimiento de políticas de seguridad de la información en la entidad
OBJETIVO
Busca identificar el nivel de estructuración de los procesos de la entidad orientados a la seguridad de la información.
TIPO INDICADOR
Indicador de Cumplimiento

INDICADOR – CUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN LA ENTIDAD		
DESCRIPCIÓN DE VARIABLES	**FORMULA**	**FUENTE DE INFORMACIÓN**
VSI09: ¿La entidad ha definido una política general de seguridad de la información?	VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	Guía del Modelo de Operación / Usuarios Internos
VSI10: ¿La entidad ha definido una organización interna en términos de personas y responsabilidades con el fin de cumplir las políticas de seguridad de la información y documenta estas actividades?		Guía del Modelo de Operación / Usuarios Internos
VSI11: ¿La entidad cumple con los requisitos legales, reglamentarios y contractuales con respecto al manejo de la información?		Guía del Modelo de Operación / Usuarios Internos
METAS		
CUMPLE 1	**NO CUMPLE**	**0**
OBSERVACIONES		

INDICADOR – IDENTIFICACIÓN DE LINEAMIENTOS DE SEGURIDAD DE LA ENTIDAD		
IDENTIFICADOR	SGIN06	
DEFINICIÓN		
Grado de la seguridad de la información y los equipos de cómputo.		
OBJETIVO		
Busca medir el nivel de preparación del recurso humano y su apropiación en cuanto a la seguridad de la información y los equipos de cómputo.		
TIPO INDICADOR		
Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES	**FORMULA**	**FUENTE DE INFORMACIÓN**
VSI12: ¿La entidad ha definido lineamientos de trabajo a través del comité o responsable de seguridad para que sus funcionarios cumplan las políticas de seguridad y evalúa periódicamente su pertinencia?	VSI0X = 1 (SÍ se evidencia)	Usuarios Internos.
VSI13: ¿La entidad ha definido lineamientos en cuanto a la protección de las instalaciones físicas, equipos de cómputo y su entorno para evitar accesos no autorizados y minimizar riesgos de la información de la entidad?	VSIOX = 0 (NO se evidencia)	Usuarios Internos.
METAS		
CUMPLE 1	**NO CUMPLE**	0
OBSERVACIONES		

INDICADOR – VERIFICACIÓN DEL CONTROL DE ACCESO	
IDENTIFICADOR	SGIN07
DEFINICIÓN	
Grado control de acceso en la entidad.	
OBJETIVO	

INDICADOR – VERIFICACIÓN DEL CONTROL DE ACCESO		
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: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar el acceso de los usuarios a sus servicios de Gobierno en línea y a sus redes de comunicaciones?	VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	Usuarios Internos.
VSI15: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar el uso y el acceso a los sistemas de información, las aplicaciones y los depósitos de información con las que cuenta la entidad? VSI16: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar las terminales móviles y accesos remotos a los recursos de la entidad?		Usuarios Internos.
METAS		
CUMPLE	1	**NO CUMPLE** 0
OBSERVACIONES		

INDICADOR – ASEGURAMIENTO EN LA ADQUISICIÓN Y MANTENIMIENTO DE SOFTWARE		
IDENTIFICADOR	SGIN08	
DEFINICIÓN		
Grado de protección de los servicios de la entidad.		
OBJETIVO		
Busca identificar la existencia de lineamientos, normas o estándares en cuanto a la adquisición o desarrollo de aplicaciones.		
TIPO INDICADOR		
Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES	**FORMULA**	**FUENTE DE INFORMACIÓN**
VSI17: ¿La entidad ha definido lineamientos, normas y/o estándares para el desarrollo o adquisición de software, sistemas y aplicaciones?		Usuarios Internos.

INDICADOR – ASEGURAMIENTO EN LA ADQUISICIÓN Y MANTENIMIENTO DE SOFTWARE			
VSI18: ¿La entidad ha definido lineamientos, normas y/o estándares para la gestión de incidentes relacionados con el servicio?		VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	Usuarios Internos.
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

INDICADOR – IMPLEMENTACIÓN DE LOS PROCESOS DE REGISTRO Y AUDITORÍA			
IDENTIFICADOR	SGIN09		
DEFINICIÓN			
Grado de existencia de lineamientos, normas o estándares en cuanto registro y auditoría para la seguridad de la información.			
OBJETIVO			
Busca identificar la existencia de lineamientos, normas o estándares en cuanto registro y auditoría para la seguridad de la información.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE DE INFORMACIÓN**
VSI19: ¿La entidad ha definido lineamientos, normas y/o estándares para el registro y control de eventos que sucedan sobre sus sistemas, redes y servicios?			Usuarios Internos.
VSI20: ¿La entidad verifica de manera interna y/o a través de terceros, periódicamente sus procesos de seguridad de la información y sistemas para asegurar el cumplimiento del modelo?		VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	Usuarios Internos.
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			
INDICADOR – DETECCIÓN DE ANOMALÍAS EN LA PRESTACIÓN DE LOS SERVICIOS DE LA ENTIDAD			
IDENTIFICADOR			

<table>
<tr><th colspan="4">INDICADOR – IMPLEMENTACIÓN DE LOS PROCESOS DE REGISTRO Y AUDITORÍA</th></tr>
<tr><td colspan="2">DEFINICIÓN</td><td colspan="2">SGIN10</td></tr>
<tr><td colspan="4">Grado de implementación de los mecanismos encaminados a la detección de anomalías e irregularidades.</td></tr>
<tr><td colspan="4">OBJETIVO</td></tr>
<tr><td colspan="4">Busca medir el nivel de mecanismos encaminados a la detección de anomalías e irregularidades</td></tr>
<tr><td colspan="4">TIPO INDICADOR</td></tr>
<tr><td colspan="4">Indicador de Cumplimiento</td></tr>
<tr><td colspan="4">DESCRIPCIÓN DE VARIABLES</td></tr>
<tr><td colspan="2">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?</td><td>FORMULA</td><td colspan="2">FUENTE DE INFORMACIÓN</td></tr>
<tr><td colspan="2"></td><td rowspan="2"></td><td colspan="2">Usuarios Internos, No Conformidades</td></tr>
<tr><td colspan="2">METAS</td><td colspan="2"></td></tr>
<tr><td colspan="4">CUMPLE</td></tr>
<tr><td>OBSERVACIONES</td><td>1</td><td>NO CUMPLE</td><td>0</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4"></td></tr>
</table>

INDICADOR – POLÍTICAS DE PRIVACIDAD Y CONFIDENCIALIDAD			
IDENTIFICADOR	SGIN11		
DEFINICIÓN			
Grado de implementación de políticas privacidad y confidencialidad de la entidad.			
OBJETIVO			
Busca identificar el nivel de implementación de políticas privacidad y confidencialidad de la entidad.			
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?		VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	Usuarios Internos.
VSI23: ¿La entidad ha implementado lineamientos, normas y/o estándares para proteger la información privada de las entidades que utilicen sus servicios?			Usuarios Internos.
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

INDICADOR – VERIFICACIÓN DE LAS POLÍTICAS DE INTEGRIDAD DE LA INFORMACIÓN			
IDENTIFICADOR	SGIN12		
DEFINICIÓN			
Grado de implementación de mecanismos para la integridad de la información de la entidad.			
OBJETIVO			
Busca identificar el nivel de implementación de políticas privacidad y confidencialidad de la entidad.			
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)	Usuarios Internos.
VSI25: ¿La entidad ha implementado lineamientos, normas y/o estándares para recuperar información en caso de modificación o pérdida intencional o accidental?			Usuarios Internos.
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

INDICADOR – VERIFICACIÓN DE LAS POLÍTICAS DE INTEGRIDAD DE LA INFORMACIÓN

INDICADOR – POLÍTICAS DE DISPONIBILIDAD DEL SERVICIO Y LA INFORMACIÓN			
IDENTIFICADOR	SGIN13		
DEFINICIÓN			
Grado de cumplimiento de las políticas de disponibilidad del servicio y la información.			
OBJETIVO			
Busca identificar el nivel de implementación de políticas de disponibilidad del servicio y la información.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE DE INFORMACIÓN**
VSI26: ¿La entidad verifica que los lineamientos, normas y/o estándares orientados a la continuidad en la prestación de los servicios se cumplan?		VSI0X = 1 (SÍ se evidencia)	Usuarios Internos.
VSI27: ¿La entidad ha implementado mecanismos para que los servicios de Gobierno en línea tengan altos índices de disponibilidad?		VSIOX = 0 (NO se evidencia)	Usuarios Internos.
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

INDICADOR – ATAQUES INFORMÁTICOS A LA ENTIDAD.			
IDENTIFICADOR	SGIN14		
DEFINICIÓN			
Porcentaje de ataques informáticos recibidos en la entidad que impidieron la prestación de alguno de sus servicios.			
OBJETIVO			
Busca conocer el número de ataques informáticos que recibe la entidad			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE DE INFORMACIÓN**
VSI28: ¿Cuántos ataques informáticos recibió la entidad en el último año?		VSI0X = 1 (SÍ se evidencia)	Herramientas de Monitoreo/Usuarios Internos.
VSI29: ¿Cuántos ataques recibió la entidad en el último año que impidieron la prestación de algunos de los servicios que la entidad ofrece a los ciudadanos y empresas?		VSIOX = 0 (NO se evidencia)	Herramientas de Monitoreo/Usuarios Internos.
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

INDICADOR – PORCENTAJE DE DISPONIBILIDAD DE LOS SERVICIO DE GOBIERNO EN LÍNEA QUE PRESTA LA ENTIDAD			
IDENTIFICADOR	SGIN15		
DEFINICIÓN			
Porcentaje de disponibilidad de los servicios que presta la entidad			
OBJETIVO			
Busca identificar el nivel de disponibilidad del servicio y la información.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE DE INFORMACIÓN**
VSI30: La entidad tiene definidos ANS para los servicios de Gobierno en Línea que presta		VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	Usuarios Internos.
VSI31: Porcentaje de disponibilidad de los servicio de Gobierno en línea que presta la entidad en base a los ANS del punto anterior.			Usuarios Internos.
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

INDICADOR – PORCENTAJE DE IMPLEMENTACIÓN DE CONTROLES					
IDENTIFICADOR	SGIN16				
DEFINICIÓN					
grado de avance en la implementación de controles de seguridad					
OBJETIVO					
Busca identificar el grado de avance en la implementación de controles de seguridad					
TIPO INDICADOR					
Indicador de Gestión					
DESCRIPCIÓN DE VARIABLES		**FORMULA**		**FUENTE DE INFORMACIÓN**	
VSI32: Número de Controles Implementados		(VSI032/VSI33)*100		Plan de tratamiento de riesgos	
VSI33: Número de Controles que se planearon implementar				Plan de Tratamiento de riesgos.	
METAS					
MÍNIMA	75-80%	**SATISFACTORIA**	80- 90%	**SOBRESALIENTE**	100%