MARCO de CIBERSEGURIDAD

GUÍA METODOLÓGICA INDICADORES PARA UN SGSI

Uruguay Presidencia

agesic

SEGURIDAD DE LA INFORMACIÓN

Este documento ha sido elaborado por Agesic (Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento).

El Marco de Ciberseguridad es un conjunto de requisitos (requisitos normativos y buenas prácticas) que se entienden necesarios para la mejora de la seguridad de la información y la ciberseguridad.

Objetivo y alcance

Definir indicadores que permitan medir el avance de la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI)

Para poder medir el grado de avance en la implementación de cualquier actividad, es imprescindible definir indicadores, cuando trabajamos en un SGSI también. El definir indicadores es una tarea compleja que debe ser realizada por expertos que además de estar especializados en la temática, deben conocer en profundidad la organización involucrada, así como todos los factores externos que puedan influenciar el proceso.

Este trabajo propone un conjunto de indicadores, los cuales, cumpliendo mínimamente con los requerimientos anteriormente descriptos, pueden servir como una guía general que posibilite en parte conocer el nivel de avance de implementación de un SGSI en una organización.

Actividades asociadas a la implementación del SGSI

Todo proceso de implementación de un “Sistema de Gestión de Seguridad de la Información” involucra el logro de un conjunto de objetivos los cuales son llevados adelante a través de la realización de actividades. Estas actividades están asociadas a las etapas de establecer, implementar, controlar y mantener el SGSI.

El siguiente cuadro muestra las etapas y actividades necesarias para implementar un SGSI.

Etapa	Actividades
ESTABLECER	Definir el Alcance del SGSI
	Definir Activos Críticos
	Definir la organización del SGSI y asignar RRHH
	Definir la Aplicabilidad del SGSI (Definición de objetivos de control y controles seleccionados para el gerenciamiento de los riesgos y justificación de los que no fueron seleccionados).
	Elaborar el Documento de la Política de Seguridad de la Información y Procedimientos
	Evaluar y planificar riesgos
IMPLEMENTAR	Divulgar la Política de Seguridad de la Información
	Implementar controles definidos

CONTROLAR	Realizar auditorías y chequear efectividad de controles
MANTENER	Gestionar los riesgos
	Gestionar incidentes
	Revisar la definición de los activos críticos, políticas y procedimientos.

Tabla 1

Debido a la complejidad que tiene cada una de las etapas, en general cada actividad es completada en base a aproximaciones sucesivas utilizando el modelo de mejora continua de Deming (PLAN-DO-CHECK-ACT). Son muy pocas las actividades que podrían realizarse en un solo paso sin requerir mejoras posteriores, pero pueden existir dependiendo del grado de madurez de la organización.

Por otro lado, el llevar adelante todas las etapas y actividades correspondientes no nos asegura que el SGSI se encuentre implementado totalmente, menos aún por que cada objetivo puede tener o no dependencias de otros.

Indicadores y métricas

A efectos de poder realizar un seguimiento del grado de implementación del SGSI, se proponen a continuación algunos indicadores y métricas que permitirán cuantificar el avance de las actividades para alcanzar los objetivos planteados.

Objetivo	Indicador	Métrica	Peso
ESTABLECER			
Organización del SGSI definida y RRHH asignados.	1- Existencia de estructura organizativa y RRHH designados.	1.1- Resolución de la Dirección del Organismo donde se crea el área. 1.2- Resolución de la Dirección donde se designan las personas.	10
Documento de la Política de Seguridad de la Información.	2- Políticas, procedimientos.	2.1- Documento de Política aprobado por la Dirección. 2.2- Procedimientos de primer nivel aprobados siendo íntegros, completos y apropiados[1].	10

[1] Se entiende como íntegros que, siendo parte de un conjunto general de políticas y procedimientos, no se contradicen entre sí, completos porque abarcan

Activos Críticos identificados	3- Identificación de los activos críticos de la organización.	3.1- Mapa de procesos críticos y sus activos asociados, aprobado por los responsables, por todas las áreas de la organización y por la dirección.	10
Riesgos identificados.	4-Identificación de los riesgos que afectan a los procesos y activos críticos.	4.1- Mapa de Riesgos identificados. 4.2- Documento aprobado por la Dirección de la Organización.	10
IMPLEMENTAR			
Planes de implementación de mejoras y controles en sistemas definidos.	5- Definición de controles en función de los riesgos detectados y las mejoras en los sistemas	5.1- Mejoras y controles definidos. Documento aprobado por Gerente de TI y Gerente de Auditoria.	10
Divulgar la PSI.	6- Controlar la capacitación según jerarquías.	6.1- Plan de capacitación definido. 6.2- Actas del Centro de Capacitación de la organización. Porcentaje de personas capacitadas, entrenadas y sensibilizadas. 6.3- Firma de acuerdo de confidencialidad.	20
CONTROLAR			
Realizar auditorías y controles.	7- Revisar el desempeño del sistema.	7.1- Dos auditorías realizadas.	15
MANTENER			
Mantenimiento del SGSI.	8- Controlar que se cumpla el ciclo de mejora continua. Gestionar riesgos e incidentes. Implementar mejoras.	8.1- Revisión de políticas y procedimientos. 8.2- Revisión de activos y mapa de riesgos. (revisiones de acuerdo a lo establecido a la política)	15

Tabla 2

Podemos decir entonces que para completar cada etapa se requiere el cumplimiento de ciertos objetivos, y que el cumplimiento de cada objetivo puede medirse utilizando una métrica como la propuesta en la tabla.

---

todos los aspectos tratados en la norma y apropiados pues deben ser relevantes a la misión de la organización.

De esta manera obtenemos para cada objetivo una medida de cumplimiento la cual puede ser expresada cuantitativa o cualitativamente.

A continuación, se presenta una posible asociación entre ambas medidas utilizando la escala de Likert para las medidas cualitativas.

Nivel de cumplimiento de la métrica	Grado de cumplimiento de la métrica (%)	Medida cualitativa (escala de Likert)	Medida cuantitativa (peso o ponderación)
No cumple	0% – 24 %	totalmente inadecuado	0.2
Cumple mínimamente	25% – 49 %	inadecuado	0.4
Cumple parcialmente	50% – 74%	indiferente (ni adecuado, ni inadecuado)	0.6
Cumple mayoritariamente	75% – 99%	adecuado	0.8
Cumple totalmente	100%	muy adecuado	1.0

Tabla 3

Finalmente, el avance global de la implementación del SGSI se podrá evaluar con la suma del grado de cumplimiento de las distintas etapas considerando las ponderaciones propuestas en la Tabla 2.

Para facilitar el entendimiento de la propuesta anterior, se adjunta un ejemplo en el anexo.

1 Medida de las métricas

Debido a que dependiendo del avance de implementación de un SGSI y de la experiencia que tenga el personal asignado, podrá ser más simple o menos complejo el determinar la medida de las diferentes métricas. Se propone la siguiente tabla que consta de un conjunto de preguntas que pueden ayudar al establecimiento de la medida para cada métrica, teniendo en cuenta que, si se quiere comparar varias organizaciones entre ellas, deberá utilizarse el mismo cuestionario.

Métrica	Cuestionario	Respuesta	Peso o ponde -ración
ESTABLECER			
1.1- Resolución de la Dirección del Organismo donde se crea el área. 1.2- Resolución de la Dirección donde se designan las personas.	1- ¿En la organización hay alguien impulsando las temáticas de seguridad de la información?	NO ni SI ni NO SI	0 5/9 10/9
	2- ¿El impulsor tiene llegada directa a la dirección?	NO ni SI ni NO SI	0 5/9 10/9
	3- ¿La dirección ha participado de reuniones por esta temática?	NO ni SI ni NO SI	0 5/9 10/9
	4- ¿La dirección ha demostrado preocupación por la seguridad de la información? ¿La dirección entiende las necesidades de capacitar RH de la organización para llevar adelante el SGSI?	NO ni SI ni NO SI	0 5/9 10/9
	5- ¿La dirección está trabajando en la preparación de las resoluciones para la creación del área y asignación de personal?	NO ni SI ni NO SI	0 5/9 10/9
	6- ¿La dirección ha entendido los riesgos y los ha asumido o ha encaminado mecanismos para mitigarlos?	NO ni SI ni NO SI	0 5/9 10/9
	7- ¿Se ha realizado alguna consultoría externa para evaluar la seguridad de la información en la organización?	NO ni SI ni NO SI	0 5/9 10/9
	8- ¿Alguna consultora externa ha recomendado establecer un SGSI?	NO ni SI ni NO SI	0 5/9 10/9
	9- ¿La dirección se ha reunido internamente para evaluar la implementación de un SGSI?	NO ni SI ni NO SI	0 5/9 10/9
2.1- Documento de Política aprobado por la Dirección. 2.2- Procedimientos de primer nivel aprobados	1- ¿Existe una planificación para establecer políticas de seguridad de la información a nivel global?	NO ni SI ni NO SI	0 5/9 10/9
	2- ¿Las políticas se han comenzado a documentar?	NO ni SI ni NO SI	0 5/9 10/9
	3- ¿La documentación de las políticas abarca todas las áreas de seguridad? (incluyendo física, lógica,....)	NO ni SI ni NO SI	0 5/9 10/9

siendo íntegros, completos y apropiados.	4- ¿La documentación de políticas cuenta con información de versionado, ha sido revisada y aprobada por el responsable de su definición?	NO ni SI ni NO SI	0 5/9 10/9
	5- ¿La documentación ha sido presentada a la dirección?	NO ni SI ni NO SI	0 5/9 10/9
	6- ¿La dirección ha confirmado entender que su revisión y aprobación es imprescindible para llevar adelante este proceso en la organización?	NO ni SI ni NO SI	0 5/9 10/9
	7- ¿Existe una planificación para la definición y elaboración de los procedimientos?	NO ni SI ni NO SI	0 5/9 10/9
	8- ¿Se han definido los procedimientos de primer nivel? ¿Han sido documentados?	NO ni SI ni NO SI	0 5/9 10/9
	9- ¿Se han revisado teniendo en cuenta su integridad, completitud y adecuación?	NO ni SI ni NO SI	0 5/9 10/9
3.1- Mapa de procesos críticos y/o activos críticos, aprobado por los responsables, por todas las áreas involucradas de la organización en el SGSI y por la Dirección.	1- ¿La dirección alguna vez ha encaminado un relevamiento de procesos críticos y/o activos críticos (mapa de procesos - activos)?	NO ni SI ni NO SI	0 5/8 10/8
	2- ¿Dicho relevamiento se encuentra documentado?	NO ni SI ni NO SI	0 5/8 10/8
	3- ¿Se cuenta con un catálogo de servicio de la organización documentado?	NO ni SI ni NO SI	0 5/8 10/8
	4- ¿Se encuentra en conocimiento de las gerencias que componen la organización?	NO ni SI ni NO SI	0 5/8 10/8
	5- ¿Se entiende necesario tener la certeza de que las gerencias de la organización deben estar en conocimiento del mapa de procesos críticos y/o activos asociados?	NO ni SI ni NO SI	0 5/8 10/8
	6- ¿Se cuenta con un organigrama actualizado de la organización?	NO ni SI ni NO SI	0 5/8 10/8
	7- ¿Se ha definido un mecanismo para confirmar que las gerencias están en conocimiento?	NO ni SI ni NO SI	0 5/8 10/8
	8- Para el caso de que el SGSI abarque en forma parcial a la organización: ¿Está planificado poner en conocimiento los procesos y/o activos	NO ni SI ni NO SI	0 5/8 10/8

	identificados al resto de los mandos de la organización?		
4.1- Mapa de Riesgos identificados. Documento aprobado por la Dirección de la Organización.	1- ¿Se cuenta con personal capacitado para la realización de un análisis de riesgos?	NO ni SI ni NO SI	0 5/9 10/9
	2- ¿Se ha definido un grupo de trabajo estable para llevar adelante el análisis?	NO ni SI ni NO SI	0 5/9 10/9
	3- ¿Se ha contratado a una empresa externa para realizar el análisis de riesgos? ¿Se cuenta con un análisis de riesgo previo?	NO ni SI ni NO SI	0 5/9 10/9
	4- Entre el personal afectado al análisis, ¿se encuentra personal con un conocimiento profundo del negocio, procesos críticos y activos asociados?	NO ni SI ni NO SI	0 5/9 10/9
	5- ¿Se ha definido un plan de trabajo?	NO ni SI ni NO SI	0 5/9 10/9
	6- ¿Se ha definido una metodología para cuantificar los riesgos?	NO ni SI ni NO SI	0 5/9 10/9
	7- ¿La metodología elegida ha sido aprobada por la dirección?	NO ni SI ni NO SI	0 5/9 10/9
	8- ¿Como parte del análisis se ha incluido la identificación de amenazas, vulnerabilidades e impacto?	NO ni SI ni NO SI	0 5/9 10/9
	9- ¿Se han definido acciones para los diferentes niveles de riesgo (aceptarlo, mitigarlo, etc.)?	NO ni SI ni NO SI	0 5/9 10/9
IMPLEMENTAR			
5.1- Mejoras y controles definidos. Documento aprobado por Gerente de TI y Gerente de Auditoria.	1- ¿Se han identificado los procesos y activos que requieren algún tipo de mejora o control?	NO ni SI ni NO SI	0 5/10 10/10
	2- ¿Se han documentado las mejoras?	NO ni SI ni NO SI	0 5/10 10/10
	3- ¿Se ha contactado a la gerencia de TI anticipadamente informando de esta iniciativa de mejora?	NO ni SI ni NO SI	0 5/10 10/10
	4- ¿La gerencia de TI ha participado en la elaboración de los planes de mejora?	NO ni SI ni NO SI	0 5/10 10/10

	5- ¿La gerencia de TI entiende la necesidad de realizar las mejoras propuestas? ¿ha entendido importante destinar RRHH Y RRMM a las mismas?	NO ni SI ni NO SI	0 5/10 10/10
	6- ¿Existe un mapa de aplicaciones que relacione los procesos del negocio con los sistemas e infraestructura de TI?	NO ni SI ni NO SI	0 5/10 10/10
	7- ¿La gerencia de Auditoría ha llevado adelante en el pasado revisiones de seguridad?	NO ni SI ni NO SI	0 5/10 10/10
	8- ¿La gerencia de Auditoría ha participado en la elaboración de los planes de mejora?	NO ni SI ni NO SI	0 5/10 10/10
	9- ¿Se elaboró un plan futuro de controles?	NO ni SI ni NO SI	0 5/10 10/10
	10- ¿La gerencia de Auditoría tiene personal capacitado o prevista la contratación de servicios externos para llevar adelante las auditorías técnicas?	NO ni SI ni NO SI	0 5/10 10/10
6.1- Plan de capacitación definido. 6.2- Actas del Centro de Capacitación de la organización. Porcentaje de personas capacitadas, entrenadas y sensibilizadas. 6.3- Firma de acuerdo de confidencialidad.	1- ¿Se han identificado y clasificado las necesidades en cuanto a capacitación en seguridad en la organización?	NO ni SI ni NO SI	0 10/10 20/10
	2- ¿Se han definido los objetivos de la capacitación en seguridad en la organización?	NO ni SI ni NO SI	0 10/10 20/10
	3- ¿Se tiene un presupuesto reservado para la capacitación en seguridad?	NO ni SI ni NO SI	0 10/10 20/10
	4- ¿Se definió el temario, contenido, agenda e instructores de la capacitación en seguridad?	NO ni SI ni NO SI	0 10/10 20/10
	5- ¿El temario de la capacitación en seguridad fue aprobado por la dirección de la organización?	NO ni SI ni NO SI	0 10/10 20/10
	6- ¿Se hizo público de alguna forma dentro de la organización la existencia de capacitación en seguridad?	NO ni SI ni NO SI	0 10/10 20/10
	7- ¿La capacitación tiene en cuenta los distintos roles de los miembros dentro de la organización?	NO ni SI ni NO SI	0 10/10 20/10

	8- ¿Ya se elaboró el material con el que se brindara la capacitación en seguridad?	NO ni SI ni NO SI	0 10/10 20/10
	9- ¿Se definió la forma en que se evaluara a los miembros de la organización en cuanto a la comprensión de la capacitación brindada?	NO ni SI ni NO SI	0 10/10 20/10
	10- ¿Existe un acuerdo de confidencialidad estándar aprobado por la dirección y por las áreas legales de la organización?	NO ni SI ni NO SI	0 10/10 20/10
CONTROLAR			
7.1- Dos auditorías. (Auditorías realizadas por la GSI)	1- ¿Existe planificación para realizar auditorías con el fin de controlar el SGSI?	NO ni SI ni NO SI	0 7/3 15/3
	2- ¿Se cuenta con recursos humanos para llevar a cabo las mismas?	NO ni SI ni NO SI	0 7/3 15/3
	3- ¿Existe personal capacitado?	NO ni SI ni NO SI	0 7/3 15/3
MANTENER			
8.1- Revisión de políticas y procedimientos. 8.2- Revisión de activos y mapa de riesgos.	1- ¿Se ha establecido un plan para la revisión de políticas y procedimientos?	NO ni SI ni NO SI	0 7/8 15/8
	2- ¿Se cuenta con la documentación suficiente para comenzar a gestionar los riesgos?	NO ni SI ni NO SI	0 7/8 15/8
	3- ¿Existe planificación para la gestión de riesgos?	NO ni SI ni NO SI	0 7/8 15/8
	4- ¿Se ha definido un software para la gestión de incidentes?	NO ni SI ni NO SI	0 7/8 15/8
	5- ¿Se ha definido qué significa un incidente de seguridad para la organización?	NO ni SI ni NO SI	0 7/8 15/8
	6- ¿Se ha definido qué significa un evento de seguridad para la organización?	NO ni SI ni NO SI	0 7/8 15/8
	7- ¿Se han clasificado los diferentes tipos de incidentes de seguridad?	NO ni SI ni NO	0 7/8

		SI	15/8
	8- ¿Se cuenta con personal capacitado para la gestión de incidentes?	NO ni SI ni NO SI	0 7/8 15/8

Tabla 4

Nota: La ponderación propuesta para cada respuesta es lineal respecto a la cantidad de preguntas para cada objetivo (ver tabla 2), correspondiéndose con la fracción de <ponderación-del-objetivo> / <cantidad-de-preguntas-para-el-objetivo> a fin de obtener la ponderación máxima del objetivo al responder afirmativamente todas las preguntas del cuestionario.

2 Ejemplos

Para facilitar el entendimiento de los indicadores propuestos se presentan a continuación dos ejemplos.

El primero utilizando la escala de Likert para la determinación del cumplimiento de cada objetivo y finalizando con el nivel de avance de implementación del SGSI.

El segundo ejemplo, no utiliza la escala de Likert sino que se basa en medidas cuantitativas asociadas al cuestionario de cada métrica, obteniéndose el porcentaje de avance de la implementación del SGSI.
Ambos métodos son equivalentes, será necesario determinar cuál se aplica mejor al público objetivo al cual se apunta.

2.1 Ejemplo 1

Paso 1: Para cada objetivo y basado en las métricas propuestas en la tabla 2, se registra el estado actual de cumplimiento utilizando la escala de Likert.

Objetivo	cumplimiento (Likert)
ESTABLECER	
1- Organización del SGSI definida y RRHH asignados.	indiferente
2- Documento de la Política de Seguridad de la Información.	adecuado
3- Activos Críticos identificados.	Inadecuado
4- Riesgos identificados.	Inadecuado
IMPLEMENTAR	
5- Planes de implementación de mejoras y controles en sistemas definidos.	inadecuado

6- Divulgar la PSI.	indiferente
CONTROLAR	
7- Realizar auditorías y controles.	inadecuado
MANTENER	
8- Mantenimiento del SGSI.	indiferente

Paso 2: Teniendo en cuenta las ponderaciones definidas en la tabla 3 asociadas a cada nivel de Likert, se construye la siguiente tabla donde se asocia a cada objetivo un nivel cuantitativo de cumplimiento, que finalmente ponderado con el peso del objetivo y sumados, se obtiene el nivel de cumplimiento de la implementación del SGSI en su globalidad (el cual puede ser traducido a un grado en la escala de Likert utilizando nuevamente la tabla 3).

Objetivo	Cumplimiento (Likert)	Peso escala Likert	Peso objetivo	% Implementación
1- Organización del SGSI definida y RRHH asignados.	indiferente	0.6	10	6
2- Documento de la Política de Seguridad de la Información.	adecuado	0.8	10	8
3- Activos Críticos identificados.	inadecuado	0.4	10	4
4- Riesgos identificados.	inadecuado	0.4	10	4
5- Planes de implementación de mejoras y controles en sistemas definidos.	inadecuado	0.4	10	4
6- Divulgar la PSI.	indiferente	0.6	20	12
7- Realizar auditorías y controles.	inadecuado	0.4	15	6
8- Mantenimiento del SGSI.	indiferente	0.6	15	9
Porcentaje de implementación				53 % Indiferente (ni adecuado, ni inadecuado)

2.2 Ejemplo 2

Paso 1: Relevar el cumplimiento para cada una de las preguntas del cuestionario de la tabla 4, asociados a los objetivos propuestos.

Paso 2: Sumar los valores a fin de obtener el porcentaje de implementación, y si es deseado convertirlo a la escala de Likert.

Objetivo	Métrica	Pregunta	Repuesta	Ponderación	% Implementación
1- Organización del SGSI definida y RRHH asignados.	1.1 y 1.2	1	Si	10/9	6,11
		2	Si	10/9	
		3	ni SI ni NO	5/9	
		4	ni SI ni NO	5/9	
		5	NO	0	
		6	NO	0	
		7	Si	10/9	
		8	Si	10/9	
		9	ni SI ni NO	5/9	
2- Documento de la Política de Seguridad de la Información.	2.1 y 2.2	1	ni SI ni NO	5/9	4,44
		2	ni SI ni NO	5/9	
		3	ni SI ni NO	5/9	
		4	Si	10/9	
		5	Si	10/9	
		6	NO	0	
		7	ni SI ni NO	5/9	
		8	NO	0	
		9	NO	0	
3- Activos Críticos identificados.	3.1	1	ni SI ni NO	5/8	3,75
		2	ni SI ni NO	5/8	
		3	NO	0	
		4	ni SI ni NO	5/8	
		5	ni SI ni NO	5/8	
		6	Si	10/8	
		7	NO	0	
		8	NO	0	
4- Riesgos identificados	4.1 y 4.2	1	Si	10/9	3,33
		2	NO	0	
		3	ni SI ni NO	5/9	
		4	NO	0	
		5	ni SI ni NO	5/9	
		6	ni SI ni NO	5/9	
		7	NO	0	
		8	ni SI ni NO	5/9	
		9	NO	0	
5- Planes de implementación de mejoras y	5.1	1	ni SI ni NO	1/2	3,00
		2	ni SI ni NO	1/2	
		3	ni SI ni NO	1/2	

controles en sistemas definidos.		4	ni SI ni NO	1/2	
		5	ni SI ni NO	1/2	
		6	ni SI ni NO	1/2	
		7	NO	0	
		8	NO	0	
		9	NO	0	
		10	NO	0	
6- Divulgar la PSI.	6.1, 6.2 y 6.3	1	Si	2	7,00
		2	Si	2	
		3	NO	0	
		4	ni SI ni NO	1	
		5	ni SI ni NO	1	
		6	ni SI ni NO	1	
		7	NO	0	
		8	NO	0	
		9	NO	0	
		10	NO	0	
7- Realizar auditorías y controles.	7.1	1	NO	0	0,00
		2	NO	0	
		3	NO	0	
8- Mantenimiento del SGSI.	8.1 y 8.2	1	ni SI ni NO	7/8	1,75
		2	ni SI ni NO	7/8	
		3	NO	0	
		4	NO	0	
		5	NO	0	
		6	NO	0	
		7	NO	0	
		8	NO	0	
Porcentaje de implementación					29,39 Inadecuado

Glosario

Objetivo: Es lo que se quiere alcanzar.

Meta: Es lo que se desea alcanzar en un periodo de tiempo.

Indicador: Provee una visión en cuanto al logro de un objetivo o meta a alcanzar.

Métrica: Es una interpretación de la medida.

ref: IEEE Standard Glossary of Software Terminology