Centro de Especializaciones Noeder

Florida Global University

Diplomado de Especialización

IMPLEMENTADOR Y AUDITOR INTERNO DE SEGURIDAD DE LA INFORMACIÓN ISO 27001

CICLO REGULAR

MÓDULO V

CLASE 01

EVALUACIÓN DEL DESEMPEÑO Y MEJORA DEL SGSI

Ing. Johnattan Sifuentes Rojas

MODULO V – EVALUACION DEL DESEMPEÑO Y MEJORA DEL SGSI

CONTENIDO MODULO V

1. Seguimiento y medición del desempeño
2. Indicadores de desempeño
3. Evaluación del cumplimiento legal y normativo
4. Auditorías internas como herramienta de mejora
5. Revisión por la dirección
6. Gestión de no conformidades
7. Acciones correctivas
8. Mejora continua

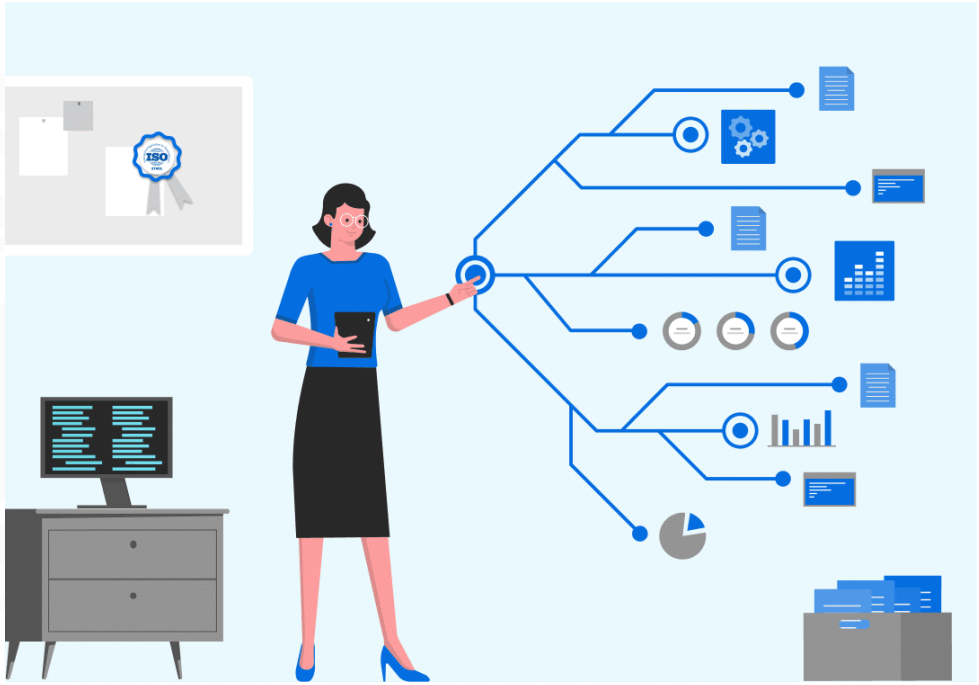
SEGUIMIENTO Y MEDICIÓN DEL DESEMPEÑO DEL SGSI

Objetivo:

Garantizar que el Sistema de Gestión de Seguridad de la Información (SGSI) cumpla con los resultados esperados.

Contenido:

- Métodos de seguimiento: revisiones periódicas, indicadores, auditorías internas y otros.
- Herramientas de medición: métricas, reportes de incidentes de seguridad de la información, cumplimiento de los controles de SI
- Relación con la cláusula 9.1 de la norma ISO 27001.



INDICADORES DE DESEMPEÑO EN SGSI

Objetivo:

Definir y aplicar métricas que permitan evaluar la eficacia del SGSI.

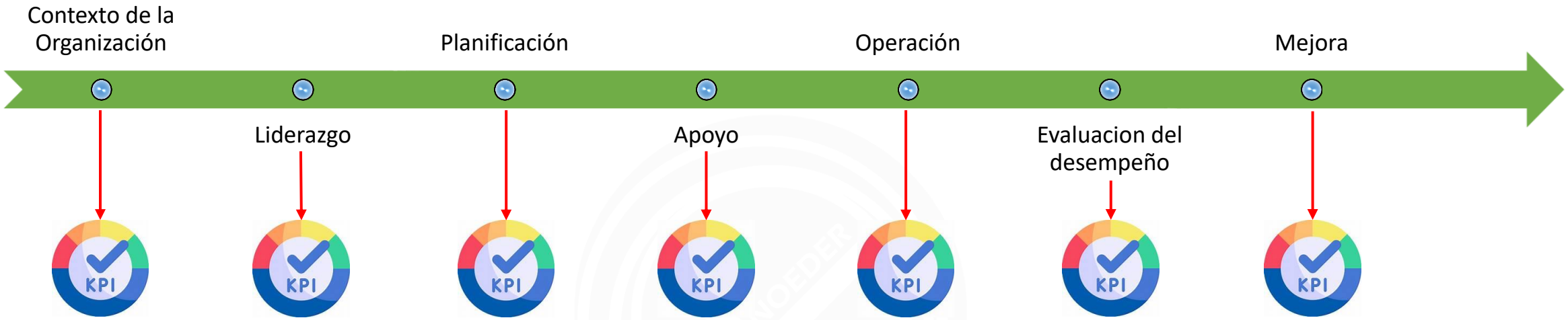
Contenido:

Definir métricas que midan la capacidad de la organización para responder, recuperarse y mejorar frente a incidentes disruptivos.
Características de un buen indicador (SMART: específico, medible, alcanzable, relevante, temporal).

Ejemplos prácticos:

- Número de incidentes de seguridad de la información..
- Nivel de concienciación del personal
- Cumplimiento de controles de seguridad.
- Cumplimiento de requisitos legales y normativos

INDICADORES DE DESEMPEÑO EN SGSI



Nº	TIPO	Objetivos del Sistema de Gestión	Nombre del Indicador	Algoritmo	Meta	Fuente	Frecuencia de Monitoreo (Cada Q)	Plazo para alcanzar la meta	Responsable	Valor mínimo	Valor Intermedio	Valor Óptimo
1	SGSI	Medir la implementación efectiva de los controles definidos en el SGSI.	Porcentaje de controles implementados y verificados.	(Controles implementados y verificados/Controles planificado) ×100	Meta: ≥ 90%.	SoA	Trimestral	Semestral	ISO	[0% a 50%>	[50% a 89%]	[90% a 100%]
2	SGSI	Evaluar la capacidad de respuesta ante incidentes de seguridad.	Porcentaje de incidentes gestionados dentro del tiempo establecido.	(Incidentes cerrados en plazo/Total de incidentes)×100	Meta: ≥ 90%.	Procedimiento de Incidentes de SI	Trimestral	Anual	ISM	[0% a 50%>	[50% a 89%]	[90% a 100%]
3	SGSI	Medir la efectividad de las capacitaciones en seguridad de la información.	Porcentaje de colaboradores que aprueban evaluaciones de concienciación.	(Colaboradores aprobados/Total de colaboradores evaluados) ×100	Meta: ≥ 85%.	Plan de capacitación	Trimestral	Anual	RH	[0% a 50%>	[50% a 84%]	[85% a 100%]
4	SGSI	Verificar la conformidad del SGSI con leyes y regulaciones aplicables.	Porcentaje de requisitos legales cumplidos.	(Requisitos cumplidos/Total de requisitos aplicables)×100	Meta: ≥ 90%.	Procedimiento Cumplimiento Legal	Trimestral	Anual	Legal	[0% a 50%>	[50% a 89%]	[90% a 100%]

INDICADORES DE DESEMPEÑO EN SGSI

25 indicadores para transformar la evaluación, los informes y las inversiones en ciberseguridad

- Tiempo de contención de incidentes
- Tiempo de remediación de incidentes
- Pruebas de continuidad con terceros
- Participación en la gestión del riesgo de terceros
- Terceros sin evaluar
- Sistemas ciberfísicos
- Cobertura de protección de terminales
- Frecuencia de actualización de parches del sistema operativo
- Soluciones alternativas ante inactividad por ransomware
- Simulacro de recuperación ante ataques de ransomware
- Autenticación multifactor
- Tiempo de eliminación de accesos
- Gestión de accesos privilegiados
- Higiene de cuentas con privilegios
- Autenticación de confianza cero
- Tasa de notificación de phishing
- Tasa de clics en simulaciones de phishing
- Formación en concienciación sobre seguridad
- Cobertura de seguridad en la nube
- Visibilidad en tiempo de ejecución en la nube
- TI en la sombra
- Excepciones de políticas vencidas
- Deuda tecnológica
- Evaluación de riesgos de IA
- Clasificación de datos

AUDITORIAS INTERNAS COMO HERRAMIENTA DE MEJORA

Objetivo:

Usar la auditoría interna como mecanismo de retroalimentación y mejora continua.

Contenido:

- ✓ Planificación de auditorías internas (ISO 27001 cláusula 9.2).
- ✓ Competencias del auditor: independencia, objetividad, conocimiento técnico.
- ✓ Técnicas de auditoría: entrevistas, revisión documental, pruebas de cumplimiento.
- ✓ Elaboración de hallazgos: conformidades, no conformidades, oportunidades de mejora

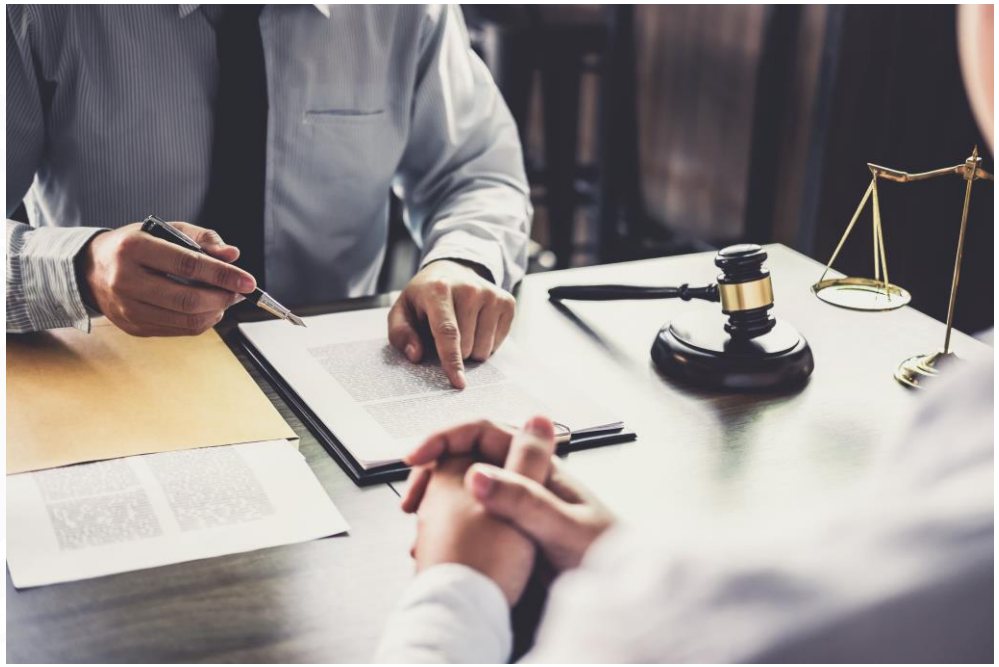
EVALUACION DEL CUMPLIMIENTO LEGAL Y NORMATIVO

Objetivo:

Verificar que la organización cumpla con leyes, regulaciones y requisitos contractuales aplicables.

Contenido:

- Identificación de requisitos legales (protección de datos, ciberseguridad, propiedad intelectual).
- Mecanismos de evaluación: matrices de cumplimiento, revisiones periódicas, auditorías externas.
- Evidencias requeridas: registros, contratos, políticas internas.
- Riesgos asociados al incumplimiento.



KPI

Nº	TIPO	Objetivos del Sistema de Gestión	Nombre del Indicador	Algoritmo	Meta	Fuente	Frecuencia de Monitoreo (Cada Q)	Plazo para alcanzar la meta	Responsable	Valor mínimo	Valor Intermedio	Valor Óptimo
1	SGSI	Verificar la conformidad del SGSI con leyes y regulaciones aplicables.	Porcentaje de requisitos legales cumplidos.	(Requisitos cumplidos/Total de requisitos aplicables)×100	Meta: ≥ 90%.	Procedimiento Cumplimiento Legal	Trimestral	Anual	Legal	[0% a 50%>	[50% a 89%]	[90% a 100%]

REVISION POR LA DIRECCIÓN

Objetivo:

Asegurar el compromiso de la alta dirección en la mejora del SGSI.

Contenido:

- Elementos clave de la revisión (ISO 27001 cláusula 9.3)
- Estado de acciones correctivas.
- Resultados de auditorías internas y externas.
- Retroalimentación de partes interesadas.
- Desempeño de indicadores.
- Importancia de la toma de decisiones basada en evidencia.
- Ejemplo: acta de revisión con compromisos de mejora.

KPI:

Nº	TIPO	Objetivos del Sistema de Gestión	Nombre del Indicador	Algoritmo	Meta	Fuente	Frecuencia de Monitoreo (Cada Q)	Plazo para alcanzar la meta	Responsable	Valor mínimo	Valor Intermedio	Valor Óptimo
1	SGSI	Evaluar la eficacia de la revisión por la dirección y el seguimiento de las decisiones tomadas.	Porcentaje de acciones de revisión implementadas en el plazo acordado.	(Acciones implementadas en plazo / Total de acciones definidas en revisión)×100	Realizar implementaciones dentro del plazo ≥ 90%	Revisión por la Dirección	Trimestral	Anual	CISO	[0% a 50%>	[50% a 89%]	[90% a 100%]

GESTION DE NO CONFORMIDADES

Objetivo:

Identificar, registrar y gestionar desviaciones respecto a los requisitos del SGSI.

Contenido:

- ✓ Definición de no conformidad.
- ✓ Proceso de gestión: detección → análisis → registro → tratamiento.
- ✓ Herramientas: sistema para registrar los incidentes SI, matrices de seguimiento, etc.
- ✓ Ejemplo: no conformidad por falta de implementar los controles de SI.

KPI:

Nº	TIPO	Objetivos del Sistema de Gestión	Nombre del Indicador	Algoritmo	Meta	Fuente	Frecuencia de Monitoreo (Cada Q)	Plazo para alcanzar la meta	Responsable	Valor mínimo	Valor Intermedio	Valor Óptimo
1	SGSI	Evaluar la eficacia del sistema en la gestión y resolución de no conformidades detectadas en auditorías o revisiones.	Porcentaje de no conformidades cerradas dentro del plazo establecido.	(No conformidades cerradas en plazo / Total de no conformidades detectadas)×100	Cierre oportuno de no conformidades ≥ 90%	No Conformidades	Trimestral	Anual	CISO	[0% a 50%>	[50% a 89%]	[90% a 100%]

ACCIONES CORRECTIVAS

Objetivo:

Eliminar la causa raíz de las no conformidades para evitar su recurrencia.

Contenido:

- Diferencia entre acción correctiva y acción preventiva.
- Metodologías de análisis de causa raíz (Ishikawa, 5 porqués)
- Documentación de acciones correctivas: plan, responsable, plazo, evidencia.
- Seguimiento y verificación de eficacia.

KPI:

Nº	TIPO	Objetivos del Sistema de Gestión	Nombre del Indicador	Algoritmo	Meta	Fuente	Frecuencia de Monitoreo (Cada Q)	Plazo para alcanzar la meta	Responsable	Valor mínimo	Valor Intermedio	Valor Óptimo
1	SGSI	Medir la capacidad del sistema para resolver las causas raíz de las no conformidades y evitar su recurrencia.	Porcentaje de acciones correctivas implementadas y verificadas como eficaces dentro del plazo establecido.	(Acciones correctivas implementadas y verificadas / Total de acciones correctivas definidas)×100	Eficacia en la implementación de acciones correctivas ≥ 90%	Acciones Correctiva	Trimestral	Anual	CISO	[0% a 50%>	[50% a 89%]	[90% a 100%]

MEJORA CONTINUA DEL SGSI

Objetivo:

Mantener el SGSI actualizado y alineado con los cambios del entorno.

Contenido:

- ✓ Ciclo PDCA (Plan-Do-Check-Act) aplicado al SGSI.
- ✓ Fuentes de mejora: auditorías, incidentes de SI, cambios tecnológicos, retroalimentación de usuarios, etc.

Ejemplos de mejora continua:

- ✓ Implementación de nuevas tecnologías de monitoreo.
- ✓ Actualización de políticas frente a nuevas amenazas.
- ✓ Programas de capacitación periódica.

KPI

Nº	TIPO	Objetivos del Sistema de Gestión	Nombre del Indicador	Algoritmo	Meta	Fuente	Frecuencia de Monitoreo (Cada Q)	Plazo para alcanzar la meta	Responsable	Valor mínimo	Valor Intermedio	Valor Óptimo
1	SGSI	Evaluar la capacidad del SGSI para incorporar aprendizajes de incidentes de SI y revisiones de la dirección, asegurando su evolución sistemática.	Porcentaje de mejoras implementadas que generan reducción de riesgos o hallazgos repetidos.	(Mejoras implementadas con impacto comprobado / Total de mejoras implementadas)×100	Efectividad de la mejora continua ≥ 85%	Mejora Continua	Trimestral	Anual	CISO	[0% a 50%>	[50% a 84%]	[85% a 100%]

¡Gracias!

Centro de
Especializaciones
Noeder

Conéctate con nuestra comunidad