Centro de Especializaciones Noeder

Florida Global University

Diplomado de Especialización

IMPLEMENTADOR Y AUDITOR INTERNO DE SEGURIDAD DE LA INFORMACIÓN ISO 27001

CICLO INTENSIVO

MÓDULO V

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 del SGSI
2. Indicadores de desempeño en seguridad de la información
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 del SGSI

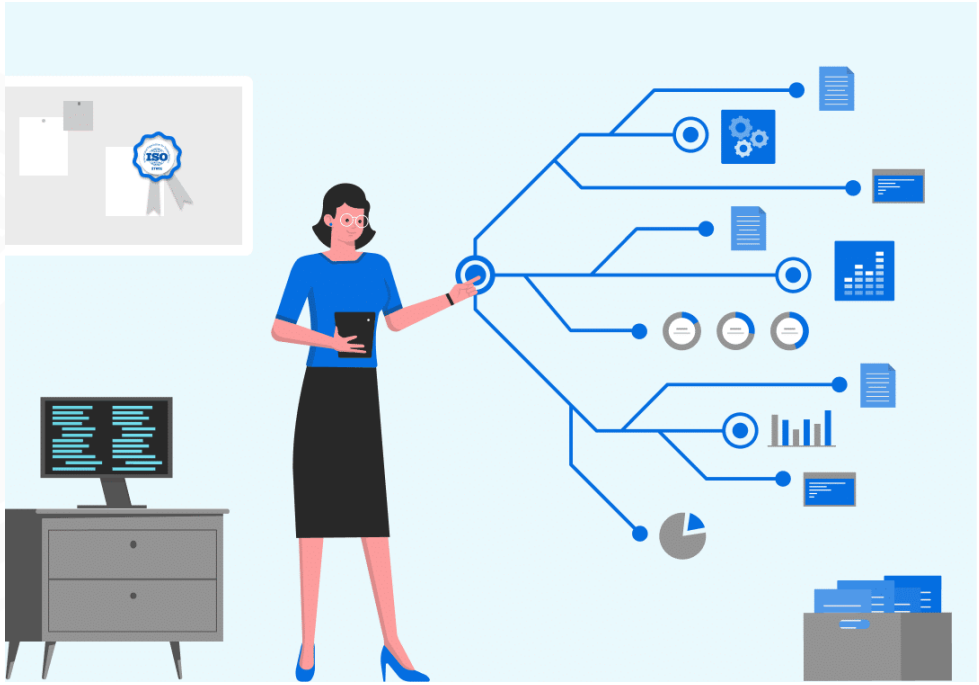
SEGUIMIENTO Y MEDICIÓN DEL DESEMPEÑO DEL SGSI

Objetivo:

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

Contenido:

- Concepto de desempeño en un SGSI.
- Métodos de seguimiento: revisiones periódicas, indicadores, auditorías internas.
- Herramientas de medición: encuestas, métricas técnicas, reportes de incidentes.
- Relación con la cláusula 9.1 de la norma ISO 27001.



INDICADORES DE DESEMPEÑO EN SEGURIDAD DE LA INFORMACON

Objetivo:

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

Contenido:

Tipos de indicadores:

- ✓ Operativos: número de incidentes, tiempos de respuesta, disponibilidad de sistemas.
- ✓ Estratégicos: nivel de cumplimiento de objetivos de seguridad, percepción de clientes.

Características de un buen indicador (SMART: específico, medible, alcanzable, relevante, temporal).

Ejemplos prácticos:

- % de cumplimiento en controles de acceso.
- Tiempo promedio de resolución de incidentes.
- Nivel de concienciación del personal en seguridad.

EVALUACION DEL CUMPLIMIENTO LEGAL Y NORMATIVO

Objetivo:

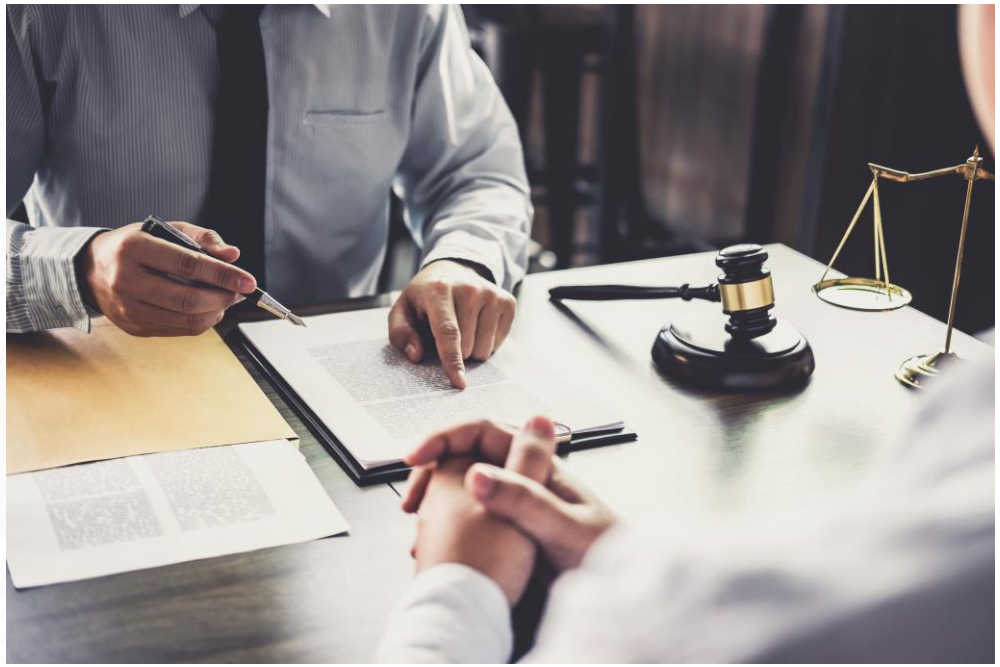
Verificar que la organización cumple con leyes, regulaciones y requisitos contractuales aplicables.

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.



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

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.

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 de tickets, matrices de seguimiento.
- ✓ Ejemplo: no conformidad por falta de actualización en políticas de acceso.

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.

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, cambios tecnológicos, retroalimentación de usuarios.

Ejemplos de mejora continua:

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

¡Gracias!

Centro de
Especializaciones
Noeder

Conéctate con nuestra comunidad