Centro de Especializaciones Noeder

Florida Global University

Diplomado de Especialización

IMPLEMENTADOR Y AUDITOR INTERNO EN SEGURIDAD DE LA INFORMCIÓN ISO 27001

CICLO REGULAR

MÓDULO VI

CLASE 03

FORMACIÓN DE AUDITOR INTERNO EN SEGURIDAD DE LA INFORMACIÓN – ISO 27001

Ing. Johnattan Sifuentes Rojas

MODULO VI – FORMACIÓN DE AUDITORES INTERNOS ISO 27001

CONTENIDO MODULO VI – SESION 04

1. Comunicación de los resultados de auditoria
2. Seguimiento a cumplimiento de planes de mejoramiento
3. Casos de Hallazgos
4. PHVA

COMUNICACIÓN DE RESULTADOS DE LA AUDITORIA

COMUNICACIÓN DE RESULTADOS DE LA AUDITORIA

CARACTERISICAS

- ✓ Conciso y sin “Novedades / sorpresas”
- ✓ Distribuido a la Gerencia / Coordinación y Representante de la Dirección.

CONTENIDO DEL INFORME

- ✓ Alcance y objetivo
- ✓ Itinerario
- ✓ Documentación de referencia
- ✓ Referencia a las listas de verificación
- ✓ Integrantes del equipo auditor
- ✓ Personal Contactado
- ✓ Resumen de hallazgos
- ✓ Descripción de No conformidades

LO QUE NO DEBE INCLUIR

- ✓ Opiniones subjetivas, información confidencial, critica hacia las personas, declaraciones ambiguas, detalles triviales y hallazgos no mencionados en la reunión de cierre.

COMUNICACIÓN DE RESULTADOS DE LA AUDITORIA

CUIDADOS EN LA REDACCIÓN

- ✓ Lenguaje claro, no retorico
- ✓ Emplear el titulo del párrafo de la Norma para presentar una No conformidad
- ✓ Emplear frases de la norma.
- ✓ No utilizar las palabras “Defecto” o “Deficiencia” sino “No Conformidad”
- ✓ No hablar en general: Informe detalladamente
- ✓ No proponer soluciones, es la empresa quien debe hacerlo (Auditoria de 2da y 3ra)
- ✓ No emplear frases “Me parece que…”, “En mi opinión…” que expresan ideas subjetivas

COMUNICACIÓN DE RESULTADOS DE LA AUDITORIA

SEGUIMIENTO A CUMPLIMIENTO DE PLANES

LA GERENCIA RESPONSABLE DEL AREA AUDITADA DEBE:

- ✓ Investigar causas
- ✓ Determinar acciones correctivas
- ✓ Implementar las acciones correctivas

LA ACCION CORRECTIVA DEBE:

- ✓ Corregir el problema.
- ✓ Determinar magnitud del problema
- ✓ Prevenir la repetición de la NC
- ✓ Obtener respuesta del auditado
- ✓ Evaluar la acción correctiva propuesta
- ✓ Confirmar la implementación de la acción correctiva

CLASIFICACIÓN Y REGISTRO DE AUDITORES

COMPETENCIA Y EVALUACION DE AUDITORES

2. * Determinación de las competencias del auditor

1. Generalidades

Al decidir los conocimientos y habilidades apropiados requeridos al auditor, debería considerarse lo siguiente:

- el tamaño, naturaleza y complejidad de la organización que se va a auditar;
- las disciplinas del sistema de gestión que se va a auditar;
- los objetivos y amplitud del programa de auditoría;
- otros requisitos, tales como los impuestos por organismos externos, cuando sea apropiado;
- la función del proceso de auditoría en el sistema de gestión del auditado;
- la complejidad del sistema de gestión que se va a auditar;
- la incertidumbre en el logro de los objetivos de la auditoría.

Los tipos, niveles de riesgos, y oportunidades abordados por el sistema de gestión;
otros requisitos, tales como aquellos impuestos por entes externos, cuando sea apropiado;

CLASIFICACIÓN Y REGISTRO DE AUDITORES

COMPETENCIA Y EVALUACION DE AUDITORES

7.2.2 Comportamiento personal

Los auditores deberían poseer las cualidades necesarias que les permitan actuar de acuerdo con los principios de la auditoría. Los auditores deberían demostrar un comportamiento profesional durante el desempeño de las actividades de auditoría, incluyendo ser:

- Ético, es decir, imparcial, sincero, honesto y discreto;
- De mentalidad abierta, es decir, dispuesto a considerar ideas o puntos de vista alternativos;
- Diplomático, es decir, con tacto en las relaciones con las personas;
- Observador, es decir, activamente consciente del entorno físico y las actividades;
- Perceptivo, es decir, consciente y capaz de entender las situaciones;
- Versátil, es decir, capaz de adaptarse fácilmente a diferentes situaciones;
- Tenaz, es decir, persistente y orientado hacia el logro de los objetivos;

CLASIFICACIÓN Y REGISTRO DE AUDITORES

COMPETENCIA Y EVALUACION DE AUDITORES

7.2.3.2 Conocimientos y habilidades genéricos de los auditores de sistemas de gestión

Los auditores deberían tener conocimientos y habilidades de las áreas señaladas a continuación.

a) Principios, procedimientos y métodos de auditoría

b) Sistema de gestión y documentos de referencia

c) Contexto de la organización

d) Requisitos legales y contractuales aplicables y otros requisitos que aplican al auditado

Entender los tipos de riesgo y oportunidades asociados a la auditoría, así como los principios del enfoque basado en el riesgo para la auditoría.

7.2.3.3 Debe contar también con conocimientos y habilidades especificas de la disciplina o sector que se va a auditar.

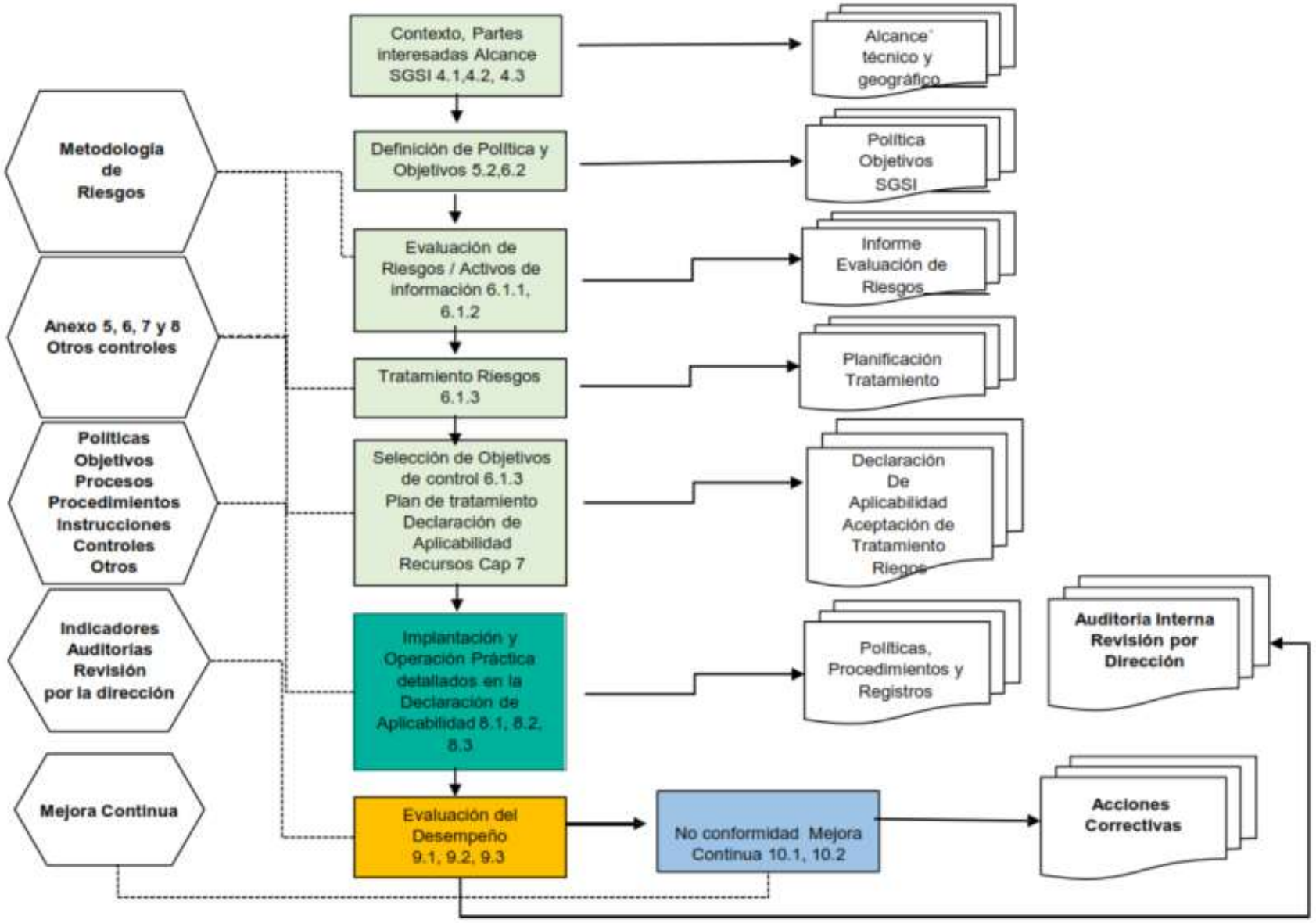
HALLAZGOS

Ref. N.C.	DESCRIPCIÓN DE LA NO CONFORMIDAD	Apdo. Norma 9001	Apdo. Norma 22301	Apdo. Norma 20000-1	Apdo. Norma 27001	Categoría N. C.
01	En contra de lo establecido en el requisito 6.1.3 de la norma: No se tiene evidencia de la aprobación de los planes de tratamiento y aceptación del riesgo residual por parte de los propietarios de los riesgos (f). Casos: RSI001, RSI004 con propietario del riesgo Soporte IT.	--	--	--	6.1.3	Menor

HALLAZGOS

Ref. N.C.	DESCRIPCIÓN DE LA NO CONFORMIDAD	Apdo. Norma 9001	Apdo. Norma 22301	Apdo. Norma 20000-1	Apdo. Norma 27001	Categoría N. C.
02	En contra a lo establecido en el requisito 8.1 "La organización deberá planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de la seguridad de la información"; no se evidencia que se cumpla con el siguiente control: a) La información almacenada en los sistemas y dispositivos de información debe ser eliminada cuando ya no sea necesaria. Caso: REQ 2026-001757 baja de usuario del 31/03/2026 en el cual no hay detalle de las actividades relacionadas a la baja entre ellas la eliminación de información según lo establecido en la PL-21 Borrado Seguro sección 5 Procedimientos operativos de IT para baja de equipos. Se escala a NC la OBS-06 de revisión previa. (Anexo A 8.10 Borrado de información) b) Las configuraciones, incluidas las de seguridad, del hardware, el software, los servicios y las redes deben establecerse, documentarse, aplicarse, supervisarse y revisarse. Garantizar que el hardware, el software, los servicios y las redes funcionen correctamente con los ajustes de seguridad requeridos, y que la configuración no se vea alterada por cambios no autorizados o incorrectos. Casos: No hay evidencia documentada de las configuraciones de firewall, servidores que son utilizados en la organización (Anexo A 8.9 Gestión de la configuración)	--	--	--	8.1	Menor

P-H-V-A ISO 27001



¡Gracias!

Centro de
Especializaciones
Noeder

Conéctate con nuestra comunidad