Centro de Especializaciones Noeder

Florida Global University

Diplomado de Especialización

IMPLEMENTADOR Y AUDITOR INTERNO DE SEGURIDAD DE LA INFORMACIÓN ISO 27001

CICLO REGULAR

MÓDULO VI

CLASE 01

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 – CLASE 01

1. Alcance y aplicación de auditoría
2. Definiciones y criterios de auditoría
3. Enfoque e importancia de las auditorías
4. Principios de auditoría
5. Programa general de auditorias

ALCANCE Y APLICACIÓN DE AUDITORIA

Objetivo:

- ✓ Formar auditores internos capaces de evaluar el desempeño del SGSI conforme a ISO 27001.
- ✓ Entender la justificación de las auditorías de SGSI
- ✓ Adquirir los conocimientos necesarios para la planificación y realización de auditorías de SGSI
- ✓ Conocer las técnicas de Auditoria
- ✓ Definir las responsabilidades de los roles.
- ✓ Conocer el proceso de certificación

DEFINICIONES Y CONCEPTOS SOBRE AUDITORIA

Auditoría

Proceso sistemático, independiente y documentado para evaluar conformidad con criterios definidos

Evidencia de la Auditoría

Registros verificables que sustentan hallazgos.

Criterios de Auditoria

Conjunto de políticas, procedimientos o requisitos usados como referencia frente a la cual se compara la evidencia objetiva,

DEFINICIONES Y CONCEPTOS SOBRE AUDITORIA

Hallazgos de Auditoria

Resultados de la evaluación de la evidencia presentadas.

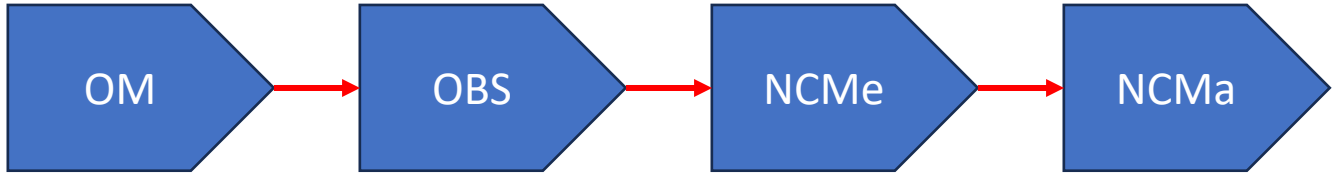
Nota 1: Los hallazgos de la auditoria indican conformidad o no conformidad.

Nota 2: Los hallazgos de la auditoria pueden conducir a la identificación de oportunidades para la mejora o el registro de buenas practicas

Nota 3: Si los criterios de auditoria se seleccionan a partir de requisitos legales o reglamentarios, los hallazgos de auditoria pueden denominarse cumplimiento o no cumplimiento.

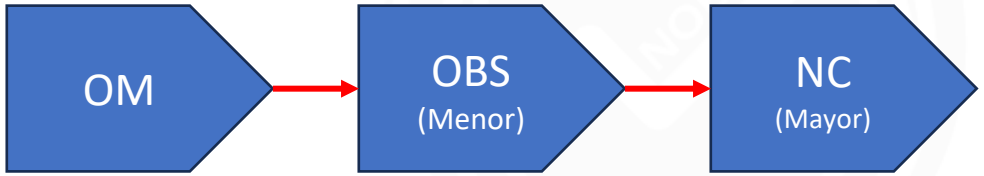
Conclusiones de la auditoria

Resultado global de la auditoría considerando hallazgos y objetivos.

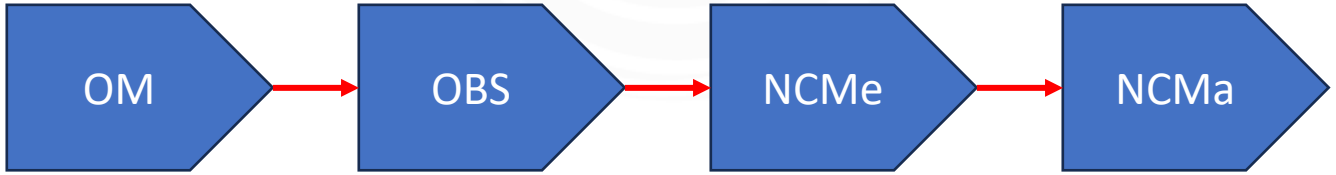


NCMa> “Paralización del proceso de Certificación”
AENOR > 4 NCMa
IRAM > 6 NCMa

9001: 2008



9001: 2015



AENOR / IRAM> 60 días calendario

AENOR /IRAM > 30 días calendario

PRINCIPIOS DE AUDITORIA

Auditorias de 1ra Parte

Son auditorias realizadas por la organización a su propio Sistema de Gestión

Auditorias de 2da Parte

Son auditorias realizadas por la organización a sus proveedores para evaluar su adecuación y rendimiento

Auditorias de 3ra Parte

Son auditorias realizadas por un organismo que es comercial y contractualmente independiente de la organización, sus proveedores y clientes, con el objetivo de determinar que el Sistema de Gestión esta documentador e implementando de acuerdo a los requisitos específicos en la norma aplicable

PLANIFICACION AUDITORIA

Responsabilidades del gestor del programa

- ✓ La persona debería:
  - Establecer el alcance del programa de auditoria
  - Identificar y evaluar los riesgos del programa de auditoria
  - Establecer las responsabilidades de la auditoria
  - Establecer los procedimientos para los programas de auditoria
  - Determinar los recursos necesarios
  - Asegurar la implementación del programa de auditoria.
  - Asegurar que se gestionan y mantienen los registros del programa de auditoria
  - Hacer seguimiento, revisión y mejora al programa de auditoria.

PLANIFICACION AUDITORIA

Competencias requeridas

- ✓ La persona responsable de la gestión del programa de auditoria debería poder gestionar el programa y sus riesgos asociados de manera eficaz y eficiente y tener conocimiento y habilidades en las siguientes áreas:

  - Principios, procedimientos y métodos de auditoria.
  - Norma de sistema de gestión y documentos de referencia
  - Actividades, productos y procesos del auditado
  - Requisitos legales y otros requisitos aplicables pertinentes a las actividades y productos del auditado.
  - Cuando se aplique, debe tener conocimiento de clientes, proveedores y partes interesadas del auditado.

ETAPA DE AUDITORIA

Con fines didácticos la gestión del programa de auditorias lo dividimos en las siguientes etapas:

PLANEACION DE LA AUDITORIA

PROGRAMA GENERAL DE AUDITORIA

Implementación del programa de auditoria

- ✓ Selección de métodos de auditoria:
  - La responsabilidad de la aplicación eficaz de los métodos de auditoria para cualquier auditoria dad en la etapa de planificación recae en la persona responsable de gestionar el programa de auditoria o en el líder del equipo auditor. El líder del equipo auditor es responsable de realizar las actividades de auditoria.

- ✓ Selección de los miembros del equipo auditor
  - Las personas responsables de la gestión del programa de auditoria deberían designar a los miembros del equipo auditor, incluyendo al líder del equipo y a cualquier experto técnico que pueda requerirse, de ser necesario.
  - El equipo auditor debería seleccionase teniendo en cuenta las competencias necesarias para alcanzar los objetivos de las auditoria individual dentro del alcance definido, Si no cubren todas las competencias necesarias, deberían incluirse en el equipo expertos técnicos con competencias adicionales, pero no deben actuar como auditores.

PROGRAMA GENERAL DE AUDITORIA

Funciones y responsabilidades de:

Auditor Líder

- ✓ Participa en la elección del equipo auditor
- ✓ Prepara el plan de auditoria
- ✓ Representan al equipo auditor ante el auditado
- ✓ Brinda instrucciones al equipo auditor.
- ✓ Informa sobre cualquier obstáculo importante encontrado en el curso del auditoria.
- ✓ Es el responsable final de todas las fases de la auditoria
- ✓ Presenta el informe de auditoria.

Auditor

- ✓ Apoya al auditor líder y sigue sus instrucciones
- ✓ Recoger y analiza las evidencias suficientes para determinar los hallazgos
- ✓ Documentar los hallazgos de la auditoria.
- ✓ Colabora en la redacción del informe de auditoria.
- ✓ Intercambia información con el equipo auditor.

PROGRAMA GENERAL DE AUDITORIA

Funciones y responsabilidades de:

ISO 19011

5.4.4 Selección de los miembros del equipo auditor

Si los auditores del equipo auditor no cubren todas las competencias necesarias, deberían incluirse en el equipo expertos técnicos con competencias adicionales. Los expertos técnicos deberían operar bajo la dirección de un auditor, pero no deberían actuar como auditores.

Experto Técnico

- ✓ Persona que aporta conocimientos o experiencia específicos al equipo auditor
- ✓ Nota 1: El conocimiento o experiencia específicos son los relacionados con la organización, el proceso o la actividad a auditar, el idioma o la orientación cultural.
- ✓ Nota 2: Un experto técnico no actúa como un auditor en el equipo auditor.

Auditado

- ✓ Informa a sus empleados de la auditoria
- ✓ Elije el personal que acompañara al auditor
- ✓ Facilita al equipo auditor los recursos necesarios
- ✓ Facilita accesos a instalaciones y evidencias materiales a petición de auditores.
- ✓ Coopera con auditores para alcanzar los objetivos
- ✓ Determina e inicia acciones correctivas del informa final.

PROGRAMA GENERAL DE AUDITORIA

Programa de Auditoria

- ✓ Conjunto de una o mas auditorias planificadas para un periodo de tiempo determinado y dirigidas hacia un propósito especifico.
- ✓ Un programa de auditoria puede incluir una o mas auditorias, dependiendo del tamaño, la naturaleza y la complejidad de la organización que va a ser auditada.
- ✓ Las personas a cargo de la gestión de la auditoria deberían: Establecer, implementar, realizar el seguimiento, revisar y mejorar el programa de auditoria e Identificar los recursos necesarios y asegurarse de que se proporcionan.

Generalidades del programa					
Programa No.	1	Duración:	Distribuidas durante todo el año 2018, ver cronograma	No. de Auditorías	25
Objetivos:	Vigilar, Mantener y Mejorar permanentemente el sistema de calidad y sus procesos. Ejemplos de objetivos de un programa de auditoría: — contribuir con la mejora del sistema de gestión y su desempeño; — cumplir con requisitos externos, ej. Certificación de una norma de sistema de gestión; — verificar conformidad con requisitos contractuales; — obtener y mantener confianza en la capacidad de un proveedor; — determinar la efectividad del sistema de gestión; — evaluar la compatibilidad y alineación de los objetivos del sistema de gestión con la política del sistema de gestión y los objetivos generales de la organización.				
Alcance:	Aplica a todos los procesos dentro del alcance del Sistema de Gestión de Calidad, así como todos los niveles y gerencias de la organización.				
Tipo de auditorías:	Según su forma		Según su alcance		
	Únicas:	X	Internas o de primera parte:	X	
	Combinadas:		Externas o de segunda parte:		
	Conjuntas:		Externas de certificación o de tercera parte:		

No.	Requisitos/Proceso/Actividad	Criterios	Equipo auditor	Mes										
				1	2	3	4	5	6	7	8	9	10	11
1	Sistema de Gestión de Calidad	ISO 9001:2015	Equipo A	■										
2	Reclutamiento y Selección de Personal (prs)	ISO 9001:2015 (7.1.2)	Equipo B	■										
3	Entrenamiento y Competencia del Personal (pec)	ISO 9001:2015 (7.2,7.3)	Equipo C	■										
4	Nómina y Servicios al Personal (pns)	ISO 9001:2015 (7.1.1,7.1.2)	Equipo D		■									
5	Contabilidad (pct)	ISO 9001:2015 (7.1.1,7.1.2)	Equipo E		■									
6	Cuentas por Pagar (pcp)	ISO 9001:2015 (7.1.1,7.1.2)	Equipo F			■								
7	Demanda de Mercado (pdm)	ISO 9001:2015 (5.1.2,8.2)	Equipo G			■								
8	Compras y Proveedores (pco)	ISO 9001:2015 (8.4)	Equipo A				■							
9	Recolección (pre)	ISO 9001:2015 (8.5)	Equipo B				■							
10	Recepción y Almacén (pra)	ISO 9001:2015 (8.5)	Equipo C					■						

¡Gracias!

Centro de
Especializaciones
Noeder

Conéctate con nuestra comunidad