



Centro de  
Especializaciones  
Noeder



Florida  
Global  
University

Diplomado de Especialización

# **IMPLEMENTADOR Y AUDITOR INTERNO DE SEGURIDAD DE LA INFORMACIÓN ISO 27001**

**CICLO INTENSIVO**

**MÓDULO VI**

**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

1. Alcance y aplicación de auditoría
2. Definiciones y conceptos de auditoría
3. Principios de auditoría
4. Requisitos para una auditoria
5. Etapas de una auditoria
6. Responsabilidades y competencias del personal responsable
7. Riesgos del programa de auditoria
8. Funciones y responsabilidades del equipo auditor



# ALCANDE Y APLICACIÓN DE AUDITORIA

## Objetivo:

- ✓ Entender la justificación de las auditorías de SGSI
- ✓ Adquirir los conocimientos necesarios para la planificación y realización de auditorías de SGSI
- ✓ Conocer tanto las técnicas como la metodología en las SGSI
- ✓ Definir las responsabilidades de las personas implicadas
- ✓ Conocer el proceso de certificación





# DEFINICIONES Y CONCEPTOS SOBRE AUDITORIA

## Auditoria

Proceso sistemático, independiente y documentado, destinado a obtener evidencias objetivas y evaluarlas de manera imparcial, con el propósito de determinar el grado de cumplimiento respecto a los criterios de auditoría

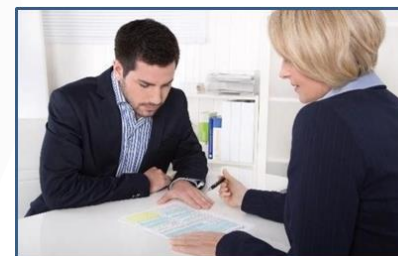


## Evidencia de la Auditoria

Registros, declaraciones de hechos u otra información pertinente a los criterios de auditoría, que sea verificable y permita demostrar objetivamente el cumplimiento.

## Criterios de Auditoria

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



## Hallazgos de Auditoria

Resultados de la evaluación de la evidencia de auditoría recopilada frente a los criterios de auditoría.

## Conclusiones de la auditoria

Resultado de una auditoria, tras considerar los objetivos de la auditoria y todos los hallazgos de la auditoria.





# PRINCIPIOS DE AUDITORIA

## Cómo se clasifican según la relación entre auditor y auditado

### 1 Primera parte



La organización se audita a sí misma.

- ✓ Auditoría interna
- ✓ Evalúa el propio sistema
- ✓ Busca mejora y control

### 2 Segunda parte



Un cliente o parte interesada audita a un proveedor.

- ✓ Relación cliente-proveedor
- ✓ Verifica requisitos contractuales
- ✓ Evalúa capacidad y confianza

### 3 Tercera parte



Un organismo independiente audita para certificar.

- ✓ Auditoría de certificación
- ✓ Ente imparcial
- ✓ Otorga o mantiene certificación

## ¿Qué cambia entre ellas?



Quién audita



Para qué se audita



Qué resultado se espera



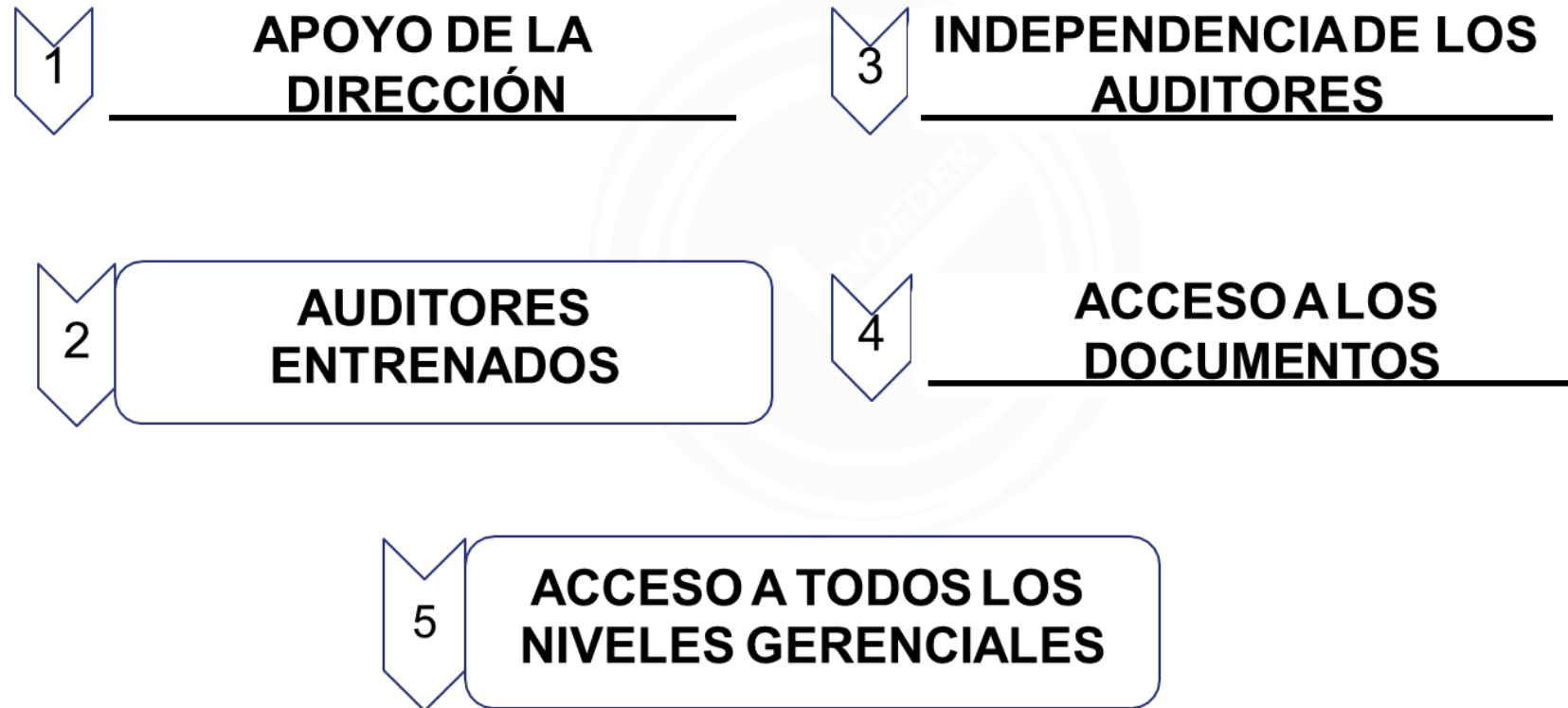
### Clave profesional

No toda auditoría persigue lo mismo: cambia el propósito, la relación entre las partes y el nivel de formalidad.



# REQUISITOS PARA UNA AUDITORIA

## Requisitos fundamentales para una auditoria efectiva





# ETAPA DE AUDITORIA

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



Programa  
general de  
auditorías



Planeación  
de la auditoría



Ejecución  
de la auditoría



Comunicación  
de resultados de  
la auditoría



Seguimiento a  
cumplimiento  
de planes de  
mejoramiento



# PLANIFICACION AUDITORIA

## Programa de Auditoria

- ✓ Conjunto de una o más auditorías planificadas para un periodo determinado y orientadas a un propósito específico.
- ✓ Un programa de auditoría puede incluir una o varias auditorías, según el tamaño, la naturaleza y la complejidad de la organización auditada.
- ✓ Las personas responsables de la gestión del programa de auditoría deben establecerlo, implementarlo, darle seguimiento, revisarlo y mejorarlo, así como identificar los recursos necesarios y garantizar su disponibilidad.

| Nº | AREA                     | FECHA PREVISTA    | FECHA REAL | ALCANCE/OBSERVACIONES                                                                                                                                                            |
|----|--------------------------|-------------------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Auditoria Intema SGSI    | Marzo T1-2014     |            | Auditoria y comprobación del SGSI actual por una empresa externa especializada independiente <b>Realización:</b> Unidad de auditoria interna/Contratación de una empresa externa |
| 2  | Auditoria de Seguimiento | Junio 2 T2-2014   |            | Revisión del cumplimiento del certificado ISO27001 <b>Realización:</b> AENOR                                                                                                     |
| 3  | Auditoria ISO27002       | Noviembre T4-2014 |            | Revisión del cumplimiento de la norma ISO27002 por la comunidad europea <b>Realización:</b> Unidad de auditoria interna Contratación de una empresa externa                      |



# PLANIFICACION AUDITORIA

## Responsabilidades de la persona que gestiona el programa de auditoria

- ✓ La persona responsable del programa de auditoria debería:
  - Definir el alcance del programa de auditoría.
  - Identificar y evaluar los riesgos asociados al programa de auditoría.
  - Asignar las responsabilidades de la auditoría.
  - Establecer los procedimientos aplicables al programa de auditoría.
  - Determinar los recursos necesarios y garantizar su disponibilidad.
  - Asegurar la implementación efectiva del programa de auditoría.
  - Gestionar y mantener los registros del programa de auditoría.
  - Realizar seguimiento, revisión y mejora continua del programa de auditoría.





# PLANIFICACION AUDITORIA

## Identificación y evaluación de riesgos al elaborar un programa de auditoria

- ✓ La persona responsable de la gestión del programa de auditoría debe administrar el programa y sus riesgos asociados de manera eficaz y eficiente, contando con conocimientos y habilidades en las siguientes áreas:
  - Principios, procedimientos y métodos de auditoría.
  - Normas de sistemas de gestión y documentos de referencia.
  - Actividades, productos y procesos del auditado.
  - Requisitos legales y otros requisitos aplicables relacionados con las actividades y productos del auditado.
  - Cuando corresponda, conocimiento de clientes, proveedores y partes interesadas del auditado.





# PLANIFICACION AUDITORIA

## Implementación del programa de auditoria

### ✓ Selección de métodos de auditoria:

- La responsabilidad de aplicar de manera eficaz los métodos de auditoría durante la etapa de planificación recae en la persona encargada de gestionar el programa de auditoría o en el líder del equipo auditor.
- El líder del equipo auditor es responsable de ejecutar las actividades de auditoría.

### ✓ Selección de los miembros del equipo auditor

- "Las personas responsables de la gestión del programa de auditoría deben designar a los miembros del equipo auditor, incluyendo al líder del equipo y, cuando sea necesario, a los expertos técnicos requeridos.
- La selección del equipo auditor debe realizarse considerando las competencias necesarias para alcanzar los objetivos de cada auditoría dentro del alcance definido.
- Si el equipo no cubre todas las competencias requeridas, se deben incorporar expertos técnicos con conocimientos adicionales; sin embargo, estos no deben actuar como auditores..



# PLANEACION DE LA AUDITORIA

## Ciclo de las Auditorías Internas





# PLANEACION DE LA AUDITORIA

1. Definición del equipo auditor y del auditor líder.
2. Análisis preliminar de la documentación:
  - Verificación de la adecuación a la norma.
  - Comprensión del producto o servicio.
  - Confirmación de la última versión del procedimiento.
3. Revisión de los registros de auditorías anteriores.
4. Preparación del plan de auditoría.
5. Elaboración de la lista de verificación:
  - Herramienta de apoyo.
  - Documento de trabajo y registro de la auditoría.



*La eficiencia y efectividad de la auditoria comienza con preparar adecuadamente la auditoria.*



# PLANEACION DE LA AUDITORIA

## CONTENIDO DEL PLAN DE AUDITORIA

- Objetivo y alcance
- Documentos de referencia
- Equipo Auditor
- Lugar y fecha
- Itinerario de la auditoria
- Programación de la reunión de apertura y cierre

|  |                                                              | Qreamo<br>Plan de Auditoria                    |                         |                                          |                       |                            |                                           | <br>Código<br>Versión<br>Emisión |  |
|------------------------------------------------------------------------------------|--------------------------------------------------------------|------------------------------------------------|-------------------------|------------------------------------------|-----------------------|----------------------------|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------|--|
| Proceso a Auditar                                                                  |                                                              | Planeación Estratégica                         | Área                    | Oficina de Planeación                    | Lider del proceso     | Jefe Oficina de Planeación | Equipo Auditor                            | Juan David Pedro Pablo                                                                                              |  |
| Objetivo de la Auditoria                                                           |                                                              | Verificar el cumplimiento de la Norma ISO 9001 | Alcance de la Auditoria | Actividades desarrolladas en el año 2014 |                       | Criterio de la Auditoria   | Norma ISO 9001, Manual de Calidad, Normas |                                                                                                                     |  |
| N                                                                                  | Actividades                                                  | Fecha                                          | Hora Inicia             | Hora Final                               | Lugar                 | Equipo auditor             | Recursos                                  |                                                                                                                     |  |
| 1                                                                                  | Reunión de Apertura                                          | 14/09/2015                                     | 08:00 a.m               | 08:30 a.m                                | Oficina de Planeación | Juan David Pedro Pablo     | Portátil Video beam                       |                                                                                                                     |  |
| 2                                                                                  | Revisión de los compromisos de la dirección. 5.1             | 14/09/2015                                     | 08:30 a.m               | 09:30 a.m                                | Oficina de Planeación | Juan David Pedro Pablo     | Portátil Papelería                        |                                                                                                                     |  |
| 3                                                                                  | Auditoria al enfoque al cliente. 5.2                         | 14/09/2015                                     | 09:30 a.m               | 10:30 a.m                                | Oficina de Planeación | Juan David Pedro Pablo     | Portátil Papelería                        |                                                                                                                     |  |
| 4                                                                                  | Revisión de la Política de Calidad 5.3                       | 14/09/2015                                     | 10:30 a.m               | 11:00 a.m                                | Oficina de Planeación | Juan David Pedro Pablo     | Portátil Papelería                        |                                                                                                                     |  |
| 5                                                                                  | Revisión de la Planificación 5.4                             | 14/09/2015                                     | 11:00 a.m               | 12:00 m                                  | Oficina de Planeación | Juan David Pedro Pablo     | Portátil Papelería                        |                                                                                                                     |  |
| 6                                                                                  | Revisión de la Responsabilidad, Autoridad y Comunicación 5.5 | 14/09/2015                                     | 02:00 p.m               | 03:00 p.m                                | Oficina de Planeación | Juan David Pedro Pablo     | Portátil Papelería                        |                                                                                                                     |  |
| 7                                                                                  | Auditoria a la Revisión por la dirección 5.6                 | 14/09/2015                                     | 03:00 p.m               | 04:00 p.m                                | Oficina de Planeación | Juan David Pedro Pablo     | Portátil Papelería                        |                                                                                                                     |  |
| 8                                                                                  | Reunión de Cierre                                            | 14/09/2015                                     | 05:00 p.m               | 06:00 p.m                                | Oficina de Planeación | Juan David Pedro Pablo     | Portátil Video beam                       |                                                                                                                     |  |
| Firma de Auditor Líder                                                             |                                                              | Juan David                                     |                         | Firma de Auditado                        |                       | Jefe Oficina de Planeación | Fecha                                     | 07/09/2015                                                                                                          |  |



# PLANEACION DE LA AUDITORIA

## La lista de verificación

- Preparadas para cada actividad del sistema de gestión
- Registrar el cumplimiento o incumplimiento
- Oportunidad de resumir y sintetizar las observaciones

### Objetivo:

- ✓ Administrar el tiempo
- ✓ Uniformizar el proceso de auditoria

## Preparación de las listas de verificación

- ¿Qué desea confirmar?
- ¿Cuáles son las metas de cada miembro de la auditoria?
- ¿Qué problemas u oportunidades de mejora existen?

### Objetivo:

- ✓ Que, cuando, como, donde, por qué
- ✓ Evitar el seguimiento de información no esencial



# PLANEACION DE LA AUDITORIA

## La lista de verificación ISO 27001

Índice

Índice

☐ Cambios con respecto al año anterior y que puedan afectar al sistema de gestión

☐ Revisión de nc del año pasado (en caso de ser renovación revisar todas las del ciclo)

☐ 4 Contexto de la organización

☐ 5 Liderazgo

☐ 6 Planificación

☐ 7 Soporte

☐ 8 Operación

☐ 9 Evaluación del desempeño

☐ 10 Mejora

☐ 5 CONTROLES DE LA ORGANIZACIÓN

- ☐ 5.1 Políticas de seguridad de la información
- ☐ 5.2 Roles y responsabilidades en seguridad de la información
- ☐ 5.3 Segregación de tareas
- ☐ 5.4 Responsabilidades de la dirección
- ☐ 5.5 Contacto con las autoridades
- ☐ 5.6 Contacto con grupos especiales de información
- ☐ 5.7 Inteligencia de amenazas
- ☐ 5.8 Seguridad de la información en la gestión de proyectos
- ☐ 5.9 Inventario de información y otros activos asociados
- ☐ 5.10 Uso aceptable de la información y activos asociados
- ☐ 5.11 Devolución de activos
- ☐ 5.12 Clasificación de la información
- ☐ 5.13 Etiquetado de la información
- ☐ 5.14 Transferencia de la información
- ☐ 5.15 Control de acceso
- ☐ 5.16 Gestión de Identidad
- ☐ 5.17 Información de autenticación
- ☐ 5.18 Derechos de acceso
- ☐ 5.19 Seguridad de la información en las relaciones con los proveedores
- ☐ 5.20 Abordar la seguridad de la información dentro de los acuerdos con los proveedores
- ☐ 5.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC

- ☐ 5.28 Recopilación de evidencias
- ☐ 5.29 Seguridad de la información durante la interrupción
- ☐ 5.30 Preparación para las TIC para la continuidad del negocio
- ☐ 5.31 Identificación de los requisitos legales, reglamentarios y contractuales
- ☐ 5.32 Derechos de propiedad intelectual (DPI)
- ☐ 5.33 Protección de los registros
- ☐ 5.34 Privacidad y protección de datos de carácter personal (DCP)
- ☐ 5.35 Revisión independiente de la seguridad de la información
- ☐ 5.36 Cumplimiento de las políticas y normas de seguridad de la información
- ☐ 5.37 Documentación de procedimientos operacionales

☐ 6 CONTROLES DE LAS PERSONAS

- ☐ 6.1 Comprobación
- ☐ 6.2 Términos y condiciones de contratación
- ☐ 6.3 Concienciación, educación y formación en seguridad de la información
- ☐ 6.4 Proceso disciplinario
- ☐ 6.5 Responsabilidad ante la finalización o cambio
- ☐ 6.6 Acuerdos de confidencialidad o no divulgación
- ☐ 6.7 Teletrabajo
- ☐ 6.8 Notificación de los eventos de seguridad de la información

☐ 7 CONTROLES FÍSICOS

- ☐ 7.1 Perímetro de Seguridad física
- ☐ 7.2 Controles físicos de entrada
- ☐ 7.3 Seguridad de oficinas, despachos y recursos
- ☐ 7.4 Monitorización de la seguridad física
- ☐ 7.5 Protección contra las amenazas físicas y ambientales
- ☐ 7.6 El trabajo en áreas seguras
- ☐ 7.7 Puesto de trabajo despejado y pantalla limpia
- ☐ 7.8 Emplazamiento y protección de equipos
- ☐ 7.9 Seguridad de los equipos fuera de las instalaciones
- ☐ 7.10 Soportes de almacenamiento
- ☐ 7.11 Instalaciones de suministro
- ☐ 7.12 Seguridad del cableado
- ☐ 7.13 Mantenimiento de los equipos
- ☐ 7.14 Eliminación o reutilización segura de equipos

☐ 8 CONTROLES TECNOLÓGICOS

- ☐ 8.10 Eliminación de la información
- ☐ 8.11 Enmascaramiento de datos
- ☐ 8.12 Prevención de fuga de datos
- ☐ 8.13 Copias de Seguridad de la información
- ☐ 8.14 Redundancia de recursos de tratamiento de la información
- ☐ 8.15 Registros de eventos
- ☐ 8.16 Seguimiento de actividades
- ☐ 8.17 Sincronización del reloj
- ☐ 8.18 Uso de programas de utilidad con privilegios
- ☐ 8.19 Instalación del software en sistemas en producción
- ☐ 8.20 Seguridad de redes
- ☐ 8.21 Seguridad de los servicios de red
- ☐ 8.22 Segregación en redes
- ☐ 8.23 Filtrado de webs
- ☐ 8.24 Uso de la criptografía
- ☐ 8.25 Seguridad en el ciclo de vida de los desarrollos
- ☐ 8.26 Requisitos de seguridad de las aplicaciones
- ☐ 8.27 Arquitectura segura de sistemas y principios de ingeniería
- ☐ 8.28 Codificación segura
- ☐ 8.29 Pruebas de seguridad en el desarrollo y la aceptación
- ☐ 8.30 Externalización del desarrollo de software
- ☐ 8.31 Separación de los recursos de desarrollo, prueba y operación
- ☐ 8.32 Gestión de cambios
- ☐ 8.33 Datos de prueba
- ☐ 8.34 Protección de los sistemas de información durante la auditoría y las pruebas



# EJECUCIÓN DE LA AUDITORIA

## Ciclo de las Auditorías Internas



Programa  
general de  
auditorías



Planeación  
de la auditoría



Ejecución  
de la auditoría



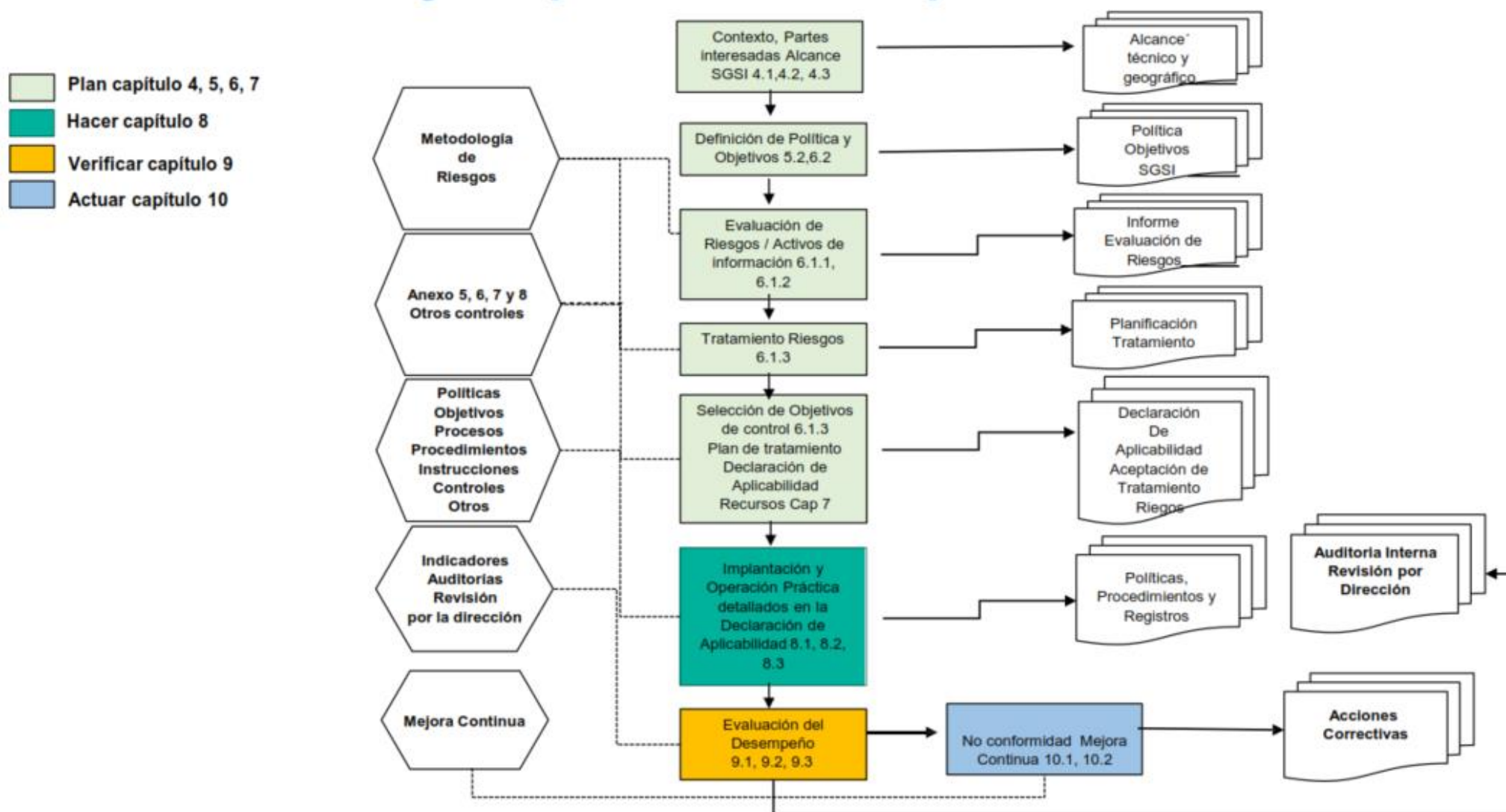
Comunicación  
de resultados de  
la auditoría



Seguimiento a  
cumplimiento  
de planes de  
mejoramiento



# EJECUCION DE LA AUDITORIA





# EJECUCION DE LA AUDITORIA

## PUNTOS A CONSIDERAR

- 1.- Reunión de Apertura
- 2.- Ejecución de la auditoria.
- 3.- Revisión de los hallazgos.
- 4.- Reunión de Cierre

## OBJETIVO

- 1.- Establecer una buena comunicación
- 2.- Cooperación con el auditado
- 3.- Cuidado con la trazabilidad de la información.





# EJECUCION DE LA AUDITORIA

## RECEPCION Y SALUDOS

## PRESENTACIÓN DE AUDITORIES Y AUDITADOS

## EXPLICAR EL PROCESO DE AUDITORIA:

- ✓ Confirmar: Objetivo, alcance y criterios
- ✓ Revisión del Plan de Auditoria: Modificaciones
- ✓ Explicar la metodología de la auditoria: practicas y muestreo, categorización de los hallazgos.
- ✓ Confirmar recursos necesarios para el equipo auditor
- ✓ Fases posteriores a la Auditoria





# EJECUCION DE LA AUDITORIA

## IMPORTANTE

- ✓ Solo una pregunta cada vez
- ✓ Esperar hasta lograr la respuesta
- ✓ No tener miedo de hacer preguntas sencillas
- ✓ Hablar claro y de forma llana
- ✓ Mirar al interlocutor
- ✓ Lenguaje adaptado al nivel del interlocutor
- ✓ Reformular la pregunta sino se ha entendido
- ✓ Preguntas al trabajador, no al guía.

## ASPECTOS CLAVE

- ✓ El auditor debe:
  - Permanecer seguro
  - Administrar el tiempo adecuadamente
  - No dejarse conducir o engañar
  - Ser detallista y eficiente
  - Evitar adaptarse del tema
  - Evitar saturarse





# EJECUCION DE LA AUDITORIA

## TACTICAS DEL AUDITADO

### Perdida de Tiempo

- Persona que hablan mucho
- Almuerzos largos
- Llegadas tarde

### Manejar al auditor

- Plan de auditoria del auditado
- Evidencia preparada
- Personal escogido

### Situaciones inesperadas

- Áreas no disponibles
- Personas no disponibles
- “Emergencias”

### Probar la fortaleza de carácter

- “Compadézcame”
- Adulación
- Falsedades
- Soborno



# EJECUCION DE LA AUDITORIA

## ACTITUDES QUE DEBE EVITAR EL AUDITOR

- ✓ Ser controvertido
- ✓ Ser negativo, indisciplinado
- ✓ Ser crítico
- ✓ Caer en disputas
- ✓ Discutir personalidades
- ✓ Comprar al auditado
- ✓ Ser sarcástico



No Conformidad

Incumplimiento de un requisito

Requisito

Necesidad que está establecida  
y es generalmente implícita u  
obligatoria

## REVISIÓN DE LA LISTA DE VERIFICACIÓN

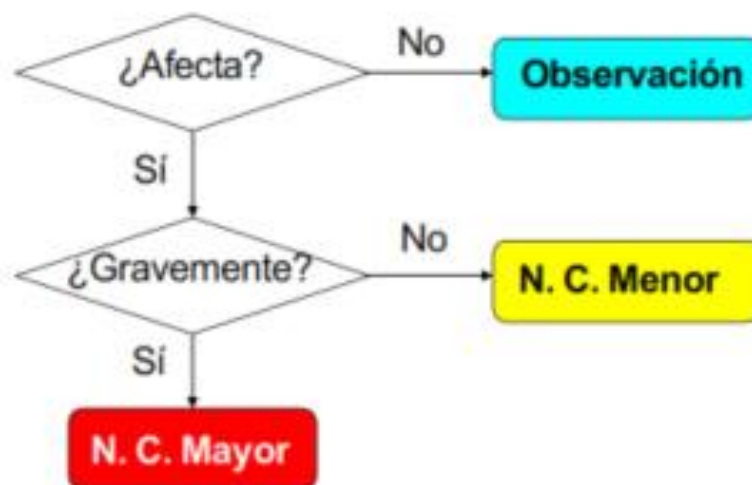
- ✓ Analizar la información y datos obtenidos
- ✓ Reunión de los auditores
  - Analizar listas de verificación
  - Hacer una lista de no conformidades



# EJECUCIÓN DE LA AUDITORIA

## CRITERIO DE LA CLASIFICACION DE LOS HALLAZGOS

✓ ¿El hallazgo afecta la funcionalidad del sistema?



### Tomar en cuenta

La clasificación de No Conformidades en tres categorías:

- ✓ No Conformidad Mayor
- ✓ No conformidad Menor
- ✓ Observación

Este tipo de calificación de hallazgos responden a las necesidades de las empresas certificadoras y no es necesario implementarlas en una organización.



# EJECUCION DE LA AUDITORIA

## CRITERIO DE CLASIFICACION DE LOS HALLAZGOS

### Definiciones de No Conformidad “MAYOR”



- Cuando existe la ausencia o falla total de un procedimiento requerido como parte del SG auditado.
- En el caso que el cliente haya fallado al manejar adecuadamente una NC menor dentro del tiempo especificado. El número de la NC menor deberá estar indicado en la emisión de la NC mayor.
- Cuando la NC tiene posibilidades de resultar en un peligro inmediato.
- En el caso que el cliente esta utilizando inadecuadamente la marca de certificación o marca de acreditación para presentar erróneamente su certificación.
- Cuando hay ocurrencia significativa de NC menores en contra de un elemento particular del modelo de SG o dentro de un departamento o actividad.

### Definiciones de no conformidad “menor”



- Cuando un fallo (error) aislado ha sido identificado respecto al estándar o un procedimiento requerido por parte del SG.
- En el caso que el cliente esta utilizando inadecuadamente la marca de certificación o la marca de acreditación, pero no esta presentando inadecuadamente su certificación.





# REVISION DE LOS HALLAZGOS

## PAUTAS PARA LA DECLARACION DE HALLAZGOS

- ✓ Centrarse en los hechos

Los resultados de las auditorias internas realizadas en los meses de enero y febrero no han sido considerados en las revisiones por la dirección del mes de julio, tal como se requiere en la clausula 9.3 de ISO/IEC 27001

## POSIBLES TIPOS DE INCUMPLIMIENTOS

- ✓ Requisitos fuera del ámbito de la norma, impuestos por el cliente.
- ✓ Soluciones especificas a los requisitos de la norma, implementados por la empresa.
- ✓ Disposiciones dentro del ámbito del sistema, aunque no específicamente prescritas por la norma.





# REVISION DE LOS HALLAZGOS

## DECLARACIONES DE OBSERVACIONES

- ✓ Deben redactarse de igual forma que las N/C
- ✓ Deben redactarse si existe un incumplimiento focalizado (no sistemático) y su impacto no pone en duda el cumplimiento de un requisito del sistema de gestión.
- ✓ La observación no requiere acción correctiva (típicamente se atiende con la corrección)
- ✓ Debilita o puede debilitar la eficacia del sistema.





# EJECUCION DE LA AUDITORIA

## REUNION DE CIERRE

- ✓ Asegurar la comprensión de la totalidad de los resultados de la auditoria
- ✓ Informal para las auditorias internas pero fundamental.
- ✓ Explicar las solicitudes de Acciones Correctiva
- ✓ Destacar la importancia de las No conformidades y de las necesidades de una acción correctiva.
- ✓ Estar preparado para sustentar
- ✓ Permitir explicaciones del auditado
- ✓ En caso de error, retirar la No conformidad y disculparse
- ✓ Obtener de los auditados las acciones correctivas
- ✓ Definir el plazo de entrega del informe final.
- ✓ Agradecer.





# COMUNICACION DE RESULTADOS DE LA AUDITORIA

## Ciclo de las Auditorías Internas



Programa  
general de  
auditorías



Planeación  
de la auditoría



Ejecución  
de la auditoría



Comunicación  
de resultados de  
la auditoría



Seguimiento a  
cumplimiento  
de planes de  
mejoramiento



# COMUNICACION 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.



# COMUNICACION 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



# COMUNICACION DE RESULTADOS DE LA AUDITORIA

## Ciclo de las Auditorías Internas



**Programa  
general de  
auditorías**



**Planeación  
de la auditoría**



**Ejecución  
de la auditoría**



**Comunicación  
de resultados de  
la auditoría**



**Seguimiento a  
cumplimiento  
de planes de  
mejoramiento**



# REDACCION DE INFORME DE AUDITORIA

## CARACTERISTICAS

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

## CONTENIDO

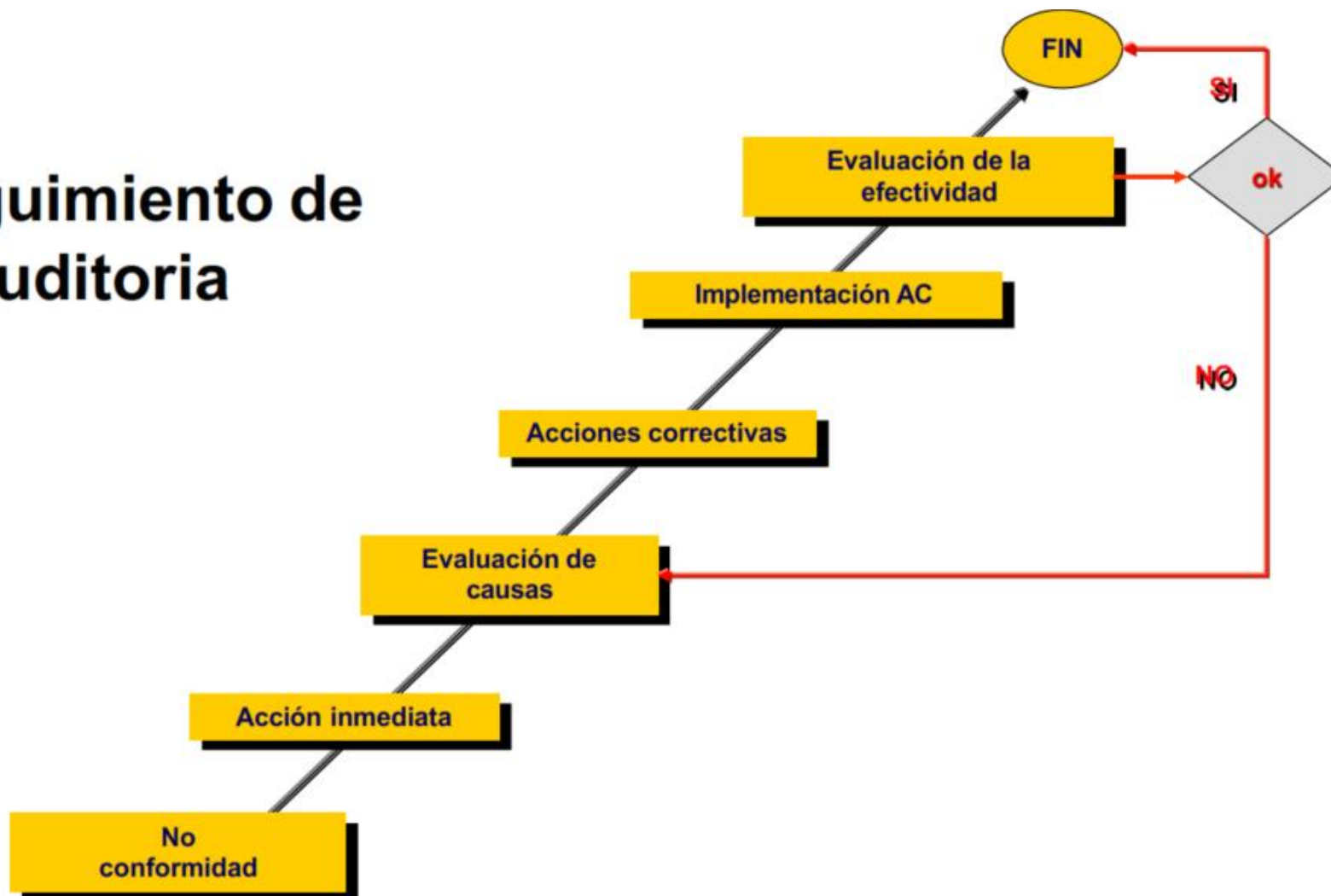
- ✓ Alcance y Objetivo
- ✓ Itinerario
- ✓ Documentación de referencia
- ✓ Referencia a las listas de verificación
- ✓ Integrantes del equipo auditor
- ✓ Personal contactado
- ✓ Resumen de hallazgos
- ✓ Descripción de No Conformidades





# SEGUIMIENTO DE LA AUDITORIA

## Seguimiento de la auditoria





# REDACCION DE INFORME DE AUDITORIA

## LO QUE NO DEBE INCLUIR

- ✓ Opiniones subjetivas
- ✓ Información confidencial
- ✓ Criticas hacia las personas
- ✓ Declaraciones ambiguas
- ✓ Detalles triviales
- ✓ Hallazgos no mencionados en la reunión de cierre

## CUIDADO 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 3era)
- ✓ No emplear frases “Me parece que...”, “En mi opinión...” que expresan ideas subjetivas





# 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





# CLASIFICACION 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;**



# CLASIFICACION 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;





# CLASIFICACION 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 específicas de la disciplina o sector que se va a auditar.**

# ¡Gracias!



Centro de  
Especializaciones  
Noeder

Conéctate con nuestra comunidad

