Centro de Especializaciones Noeder

Florida Global University

Diplomado de Especialización

IMPLEMENTADOR Y AUDITOR INTERNO EN SEGURIDAD DE LA INFORMACIÓN ISO 27001

CICLO REGULAR

MÓDULO VI

CLASE 02

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 02

1. Planeación de la Auditoria
2. Lista de Verificación ISO 27001
3. Ejecución de auditoria

PLANEACION DE LA AUDITORIA

PLANEACION DE LA AUDITORIA

1.- Definición del Equipo Auditor / Auditor Líder

2.- Análisis preliminar de los documentos

- Adecuación a la norma
- Comprensión del producto/servicio
- Ultima versión del procedimiento

3.- Análisis de registros de Auditorias Anteriores

4.- Preparación del Plan de auditoria

5.- Preparación de la lista de verificación

- Herramienta útil
- Documento de trabajo y registro de la auditoria

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

Qreamoz

Plan de Auditoria

Proceso a Auditar	Planeación Estratégica	**Área**	Oficina de Planeación	**Líder del proceso**	Jefe Oficina de Planeación	**Código** **Versión** **Emisión**	
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**	**Equipo Auditor**	Juan David Pedro Pablo
						Norma ISO 9001, Manual de Calidad, Normas	

N	Actividades	Fecha	Hora Inicia	Hora Final	Lugar	Equipo auditor	Recursos
1	Reunió 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

LISTA DE COMPROBACIÓN ISO/IEC 27002:2022

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 autentificación
  - ☐ 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
  - ☐ 5.22 Seguimiento, revisión y gestión del cambio de los servicios de proveedores
  - ☐ 5.23 Seguridad de la información para el uso de servicios en la nube
  - ☐ 5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información
  - ☐ 5.25 Evaluación y decisión sobre los eventos de seguridad de información
  - ☐ 5.26 Respuesta a incidentes de seguridad de información
  - ☐ 5.27 Aprender de los incidentes de seguridad de la información
  - ☐ 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
  - ☐ 8.1 Dispositivos de punto final de usuario
  - ☐ 8.2 Gestión de privilegios de acceso
  - ☐ 8.3 Restricción del acceso a la información
  - ☐ 8.4 Acceso al código fuente
  - ☐ 8.5 Autenticación segura
  - ☐ 8.6 Gestión de capacidades
  - ☐ 8.7 Controles contra el código malicioso
  - ☐ 8.8 Gestión de vulnerabilidades técnicas
  - ☐ 8.9 Gestión de la configuración
  - ☐ 8.10 Eliminación de la información
  - ☐ 8.11 Enmascaramiento de datos
  - ☐ 8.12 Prevencion 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

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

LAS PREGUNTAS

- ✓ Preguntas efectivas: preguntas abiertas
- ✓ Estimular al auditado a conversar
  Muéstreme los tipos de informes que tiene, ¿Cómo lo hace?, ¿Dónde archiva sus registros?
- ✓ Estimular preguntas “las no preguntas”
  “*Veo que hace un entrenamiento para todos los operadores de las maquinas de prensa, ¿no es verdad?*

Primera pregunta típica:

**“Por favor, ¿puede explicarme lo que está haciendo?
¿Quién, cuándo, cómo , dónde, por qué?**

Otro posible seguimiento:

**"Creo que está haciendo.. para... ,
¿Me equivoco?
Por favor, enséñeme..."
Perdón, no lo entiendo ¿puede repetírmelo?**

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	Manejar al auditor	Situaciones inesperadas	Probar la fortaleza de carácter
• Persona que hablan mucho • Almuerzos largos • Llegadas tarde	• Plan de auditoria del auditado • Evidencia preparada • Personal escogido	• Áreas no disponibles • Personas no disponibles • “Emergencias”	• “Compadézcame” • Adulación • Falsedades • Soborno

EJECUCION DE LA AUDITORIA

ACTITUDES QUE DEBE EVITAR EL AUDITOR

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

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

No Conformidad

Incumplimiento de un requisito

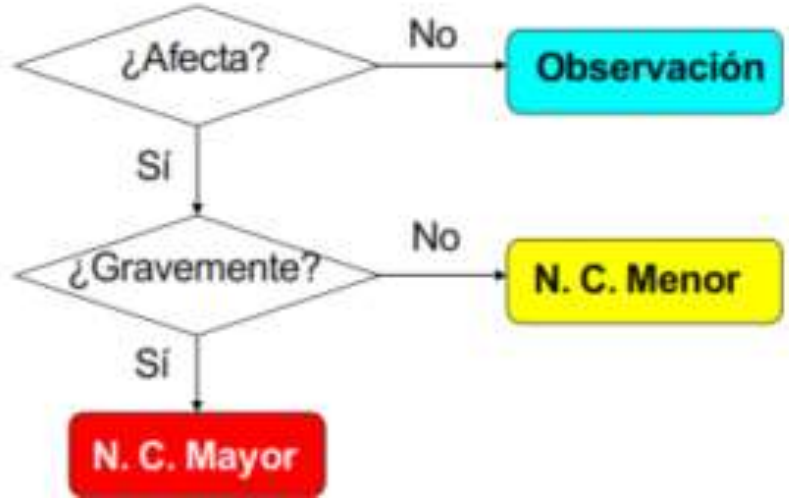
Requisito

Necesidad que está establecida y es generalmente implícita u obligatoria

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.

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.

¡Gracias!

Centro de
Especializaciones
Noeder

Conéctate con nuestra comunidad