

## AUDITORIA INTERNA ISO 27001:2005

### INTRODUCCIÓN

Al implantar un Sistema de Gestión de Seguridad de Información (ISO 27001:2005, las empresas se enfrentan ante la necesidad de efectuar auditorias internas a su sistema de gestión de seguridad de información y poder identificar su conformidad con dicho modelo. La idea básica de la auditoria interna es que la empresa demuestre a terceros que esta en un proceso constante de mejora continua, buscando oportunidades para superar el actual desempeño.

El estándar es muy puntual, la cláusula 6.0 exige que la empresa realice anualmente auditorias a su sistema de gestión de seguridad de información. Ante esta exigencia de la norma, es recomendable que la empresa forme sus propios auditores internos provenientes de distintas áreas funcionales.

El presente curso esta orientado a formar "auditores internos" para que la empresa tenga la capacidad interna instalada y poder de manera independiente y objetiva realizar sus auditorias.

### OBJETIVO GENERAL

- Desarrollar un profundo entendimiento de las exigencias del estándar ISO 27001:2005 en cuanto la realización de auditorias internas se refiere.
- Desarrollar las habilidades y destrezas para planificar, ejecutar y evaluar una auditoria interna según el ISO 19011:2002.
- Desarrollar las habilidades para elaborar in informe final de auditoria.
- Poder entender como se elabora un reporte de no conformidad y la documentación de las evidencias objetivas de un incidente de seguridad.
- Entender la relación entre la auditoria interna, la mejora continua y la acción correctiva.

## BENEFICIOS

El participante al terminar el curso, habrá desarrollado las siguientes competencias:

- Entender los requerimientos de la norma en relación a realizar auditorias internas.
- Saber programar y planificar una auditoria para el ISO 27001:2005.
- Entender como se planifica y ejecuta una auditoria interna de ISO 27001:2005
- Saber hacer listas de chequeo para auditar.
- Saber elaborar un informe de auditoria.

## EXPOSITOR



**Alberto G. Alexander Ph.D.** The University of Kansas, 1977, M.A. Northern Michigan University, 1974, Licenciatura en Administración, Universidad de Lima, 1972. El Dr. Alexander posee una amplia experiencia académica en Instituciones de Post-Grado. Ha sido profesor a dedicación exclusiva en la Dirección de Post-Grado de la Universidad de Carabobo, Valencia - Venezuela (1977-1978). Fue profesor de Post-Grado de la Universidad Católica Andrés Bello, Caracas - Venezuela (1978-1979). Se desempeñó como profesor residente del Instituto de Estudios Superiores de Administración (IESA), Caracas - Venezuela (1978-1983). Ha sido profesor afiliado de la Escuela de Administración de Negocios para Graduados (ESAN), Lima - Perú. El Dr. Alexander posee una amplia experiencia en el diseño y dictado de Programas de Desarrollo Gerencial para Ejecutivos. Sus áreas de interés, así como de experiencia en la Docencia y en Consultoría, son: Productividad, Calidad Total, Modelos de Aseguramiento de la Calidad, Sistema de Recursos Humanos y Planificación Estratégica. Ha publicado artículos y ensayos en revistas internacionales. Es ganador del Concurso Nacional Venezolano de Productividad "**Don Eugenio Mendoza**", patrocinado por **FEDECAMARAS**, en el año 1980. En el año 1990, la Federación Venezolana de Prensa le otorgó "**EL SOL DORADO**", en reconocimiento a sus aportes para el

desarrollo y bienestar de Venezuela. El Dr. Alexander posee una amplia experiencia internacional en el asesoramiento a empresas en áreas tales como: Modelos de Aseguramiento de la Calidad: ISO 9000, Reingeniería de Procesos, Mejoramiento de la Calidad, Reducción de Costos de la Mala Calidad y Sistemas de Recursos Humanos. Es miembro activo de American Society for Quality. Es **auditor líder de Sistemas de Gestión de la Calidad ISO 9000**, certificado por el: International Register of Certificated Auditors (IRCA), Inglaterra. **Auditor de "Sistemas de Gestión de Seguridad de Información"** certificado por el International Register of Certificated Auditors" (IRCA) Inglaterra. Entrenado como auditor líder en **ISO 14000** certificado ante el EARA (Inglaterra) y el RAB (USA). Auditor de Sistemas **TL 9000**, certificado ante el **QuEST (USA)**. **Autor de los libros:** La Mala Calidad y sus Costos, 1994. Aplicación del ISO 9000 y Cómo Implementarlo, 1995. Ambos ejemplares publicados por la Editorial Addison Wesley, U.S.A., Manual para Documentar Sistemas de Calidad. Prentice Hall Hispanoamerica, 1999, México, Metodología Para el Mejoramiento Continuo. Prentice Hall Hispanoamericana 2001, México, e Implantación Estratégica del ISO 9000 versión 2000. Fondo Editorial Pontificia Universidad Católica del Perú. 2003, Perú. Metodología para Documentar el ISO 9000 versión 2000, Prentice Hall, 2005, México. Su mas reciente publicación es Diseño y Gestión de un Sistema de seguridad de Información: Óptica 27001:2005, Editorial Alfaomega, Colombia, 2007. Se ha desempeñado como Director Gerente de la firma **EFICIENCIA GERENCIAL Y PRODUCTIVIDAD S.A.**, con sede en Caracas - Venezuela. Actualmente actua en las mismas funciones para las operaciones de latinoamerica, desde Lima, Perú. [www.eficienciagerencial.com](http://www.eficienciagerencial.com)

## ESTRUCTURA DEL PROGRAMA

### Herramientas Metodológicas a Utilizar

- **Clases Lectivas:** Presentación explícita del contenido y de los aspectos conceptuales y técnicos asociados a cada tema en formato Powerpoint.

- **Análisis de Casos y Distribución de Lecturas:** Las explicaciones conceptuales se combinarán con el análisis de casos prácticos que permitirán profundizar en los diferentes aspectos tratados. Cada participante recibirá el estándar ISO 27001:2005 .
- **Juegos de Simulación:** Se utilizarán juegos de simulación que replicarán situaciones reales en las empresas al tratar de auditar el modelo.

## DESCRIPCIÓN DE LA ESTRUCTURA DEL PROGRAMA

### **1.-Exigencias de la norma en Relación a Efectuar Auditorias Internas a un Sistema de Gestión de Seguridad de Información**

#### **Temario**

- Análisis de los requerimientos de la norma ISO 27001:2005
- Las exigencias de la cláusula 6.0 del ISO 27001:2005
- Requerimientos de programación de auditorias internas.
- El plan de auditoria.
- La auditoria y la acción correctiva. Tipos de auditoria.

### **2.-Metodología para la Elaboración de un Plan de Auditoria**

#### **Temario**

- Diseño de un programa de auditoria.
- Componentes de un plan de auditoria.
- Elaboración del cronograma de la auditoria
- Identificación de auditores.
- Rol del auditor líder.

### **3.-Ejecución de la Auditoria**

## Temario

- Reunión de apertura y de cierre en la auditoría.
- Elaboración de listas de chequeo y su manejo en la auditoría.
- Pautas para ejecutar la auditoría de adecuación y de cierre.
- Identificación de no conformidades
- Redacción de evidencias objetivas.

## 4.-Elaboración de un Informe Final de Auditoría

### Temario

- Redacción de las no conformidades
- Bosquejo de un informe final de auditoría
- Entrega del informe y el cierre de la auditoría.
- Rol de la gerencia ante las no conformidades.
- Tiempo permisible para cerrar las no conformidades.

### MATERIAL DIDÁCTICO

Cada participante recibirá una copia de las diapositivas del instructor así como un ejemplar de: Estándar ISO 27001:2005 (traducido al castellano), ISO 19011:2002 (traducido al castellano).

### INFORMACIÓN E INSCRIPCIÓN

**E-Mail:** [servicios@eficienciagerencial.com](mailto:servicios@eficienciagerencial.com)

**Website:** [www.eficienciagerencial.com](http://www.eficienciagerencial.com)

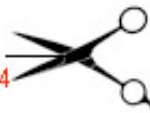
**Dirección:** Av. Del Pinar # 134, Edificio El Pinar II, Ofic. 803, Chacarilla del Estanque, Santiago de Surco, Lima – Perú

**Teléfonos:** (511) 3721441 / 3721415

**Fax:** (511) 436 6144

Este seminario puede confeccionarse y adaptarse a las necesidades específicas de la empresa y ser dictado de manera exclusiva.

Favor completar y enviar vía email a [cursos@eficienciagerencial.com](mailto: cursos@eficienciagerencial.com) o por fax al (511) 436-6144



## FORMULARIO DE INSCRIPCIÓN

### AUDITORÍA INTERNA ISO 27001:2005

#### INFORMACIÓN DE LA EMPRESA

Nombre de la Empresa \_\_\_\_\_  
RUC \_\_\_\_\_  
Actividad Especifica de la Empresa \_\_\_\_\_  
Dirección \_\_\_\_\_  
Ciudad \_\_\_\_\_ Provincia \_\_\_\_\_  
Teléfono \_\_\_\_\_ Fax \_\_\_\_\_

#### INFORMACIÓN DEL PARTICIPANTE

Nombres y Apellidos \_\_\_\_\_  
Cargo \_\_\_\_\_  
Email Empresa \_\_\_\_\_ Email Personal \_\_\_\_\_  
Teléfono (Empresa) \_\_\_\_\_ Teléfono (Móvil) \_\_\_\_\_  
Sexo 

F	M
---	---

 Fecha Nacimiento (Día/Mes) \_\_\_\_\_

¿Cómo desea que aparezcan sus datos en su certificado de participación?  
(Indique Nombres y Apellidos)

Objetivos: ¿Qué espera lograr asistiendo a este seminario?

¿Cómo se enteró del curso?

Prensa  Revista  Email  Google  Website  Un amigo

Otros, indique \_\_\_\_\_

#### DATOS DE FACTURACIÓN

Formas de Pago  (\*) Depósito en cuenta bancaria  Pago en línea vía web EGP  
<http://www.eficienciagerencial.com/tienda>  
Facturar a  Participante  Empresa

Si eligió **facturar a empresa** llene la siguiente información:

Persona responsable de la inscripción \_\_\_\_\_  
Departamento \_\_\_\_\_ Posición \_\_\_\_\_  
Teléfono \_\_\_\_\_ Fax \_\_\_\_\_

(\*) Datos para depósito en cuenta bancaria:

#### Abono en cuenta ahorro US \$:

- Banco: BBVA  
Beneficiario: EFICIENCIA GERENCIAL Y PRODUCTIVIDAD S.A.C.  
Cuenta US \$ N° 0011-0194-0200289850-86

#### Abono en cuenta corriente en nuevos soles S/:

- Banco: SCOTIABANK  
Beneficiario: EFICIENCIA GERENCIAL Y PRODUCTIVIDAD S.A.C.  
Cuenta N° 6459374

## POLÍTICAS DE CANCELACIÓN Y REEMBOLSOS

1. Nos reservamos el derecho de cancelar el curso si no se cumplen con las condiciones estipuladas, en este caso el costo de inscripción será reembolsado a los participantes.
2. No nos hacemos responsables por gastos de pasaje u hospedaje en el cual el participante haya incurrido. Toda notificación de cambio o cancelación por parte de nuestra empresa será indicada no menos de quince (15) días antes del inicio del curso.
3. Los asistentes que den por cancelada su participación en el curso quince (15) días antes del inicio del curso tendrán un cargo del 20% del valor de la inscripción del curso, correspondiente a gastos administrativos.

Cancelaciones después de este período no tendrán reembolso, sin embargo el cupo puede ser usado por otro participante de la misma empresa

4. Sólo el envío de la solicitud de inscripción debidamente llenada y el pago adelantado del importe del evento formalizará la inscripción.
5. El curso debe ser pagado en su totalidad antes de la fecha de inicio.