

# Curso Gestión y Auditoría de la Seguridad de la Información

## Detalle del Curso

Gestión y Auditoría de la Seguridad de la Información.

Taller de implementación trabajando con una experiencia real.

Las nuevas posibilidades de negocios electrónicos y las ventajas competitivas y de cumplimiento de leyes y regulaciones, más la necesidad y conveniencia del análisis de riesgos de negocios, abonan la problemática de la nueva era de las interrelaciones holísticas de un sistema de gestión de seguridad de la información: Los riesgos, las normas de seguridad ISO 27002 (anteriormente 17799) y 27001, y las relaciones con otros sistemas de gestión.

La práctica grupal extensiva e intensiva de un workshop basado en experiencias reales y la consideración de todo este material, permite desarrollar y verificar políticas, normas y controles de seguridad conforme a su implementación, así como también incursionar en los aspectos más importantes del análisis de riesgos.

## Objetivos

Reconocer, revisar, analizar y articular:

- \* La evaluación de la seguridad, el análisis y gestión de riesgos, y las herramientas para su tratamiento.
- \* Las normas ISO 17799 (hoy, ISO 27002) y 27001 que rigen la seguridad de la información. Complementación, selección e implementación de controles.
- \* El aporte de integración de la familia de normas 27000 a la problemática de riesgos y seguridad.
- \* Las normas, estándares e información especializada de seguridad y análisis y gestión de riesgos.
- \* Análisis de un caso real de implementación de alcance corporativo de la ISO 27001
- \* La participación activa en un taller de implementación de un día completo

Metas a alcanzar

Finalizado el curso, los participantes podrán :

- \* Tener un sólido entendimiento de la forma de valuar y gestionar riesgos, y su relación a nivel corporativo.
- \* Diferenciar los riesgos organizacionales y operacionales de los meramente técnicos de sistemas ICT.
- \* Conocer los principales detalles de implementaciones reales.
- \* Poder llevar adelante una implementación exitosa y guiar al personal de su empresa.
- \* Comprender la importancia y ventajas de la armonización entre el sistema de gestión de seguridad de la información respecto de otras normas de gestión como las de Calidad y Ambiental.
- \* Tener las bases de la justificación de las inversiones en seguridad

## Requisitos

¿Quiénes deben asistir?:

o Personal superior y funcionarios que necesitan conocer la problemática y soluciones en cuanto a seguridad de la información y su trascendencia en los riesgos de negocios.

o Gerentes y cuadros medios de Sistemas, Computación y Tecnología, administradores de redes y seguridad de la información que necesitan adecuar a criterios de confiabilidad internacional el nivel de seguridad en operaciones de e-commerce, accesos remotos e inalámbricos.

o Auditores informáticos y de sistemas, auditores internos y externos.

o Auditores de diferentes sistemas de gestión corporativos.

o Profesores universitarios y personal docente de carreras de negocios y tecnológicas.

o Consultores

## Modalidad

Primer día: exposición

Segundo día: taller de trabajo

## Plan de Estudio

Temario General de la Presentación

Conceptos básicos de riesgos

\* Valuación de riesgos. Análisis cualitativo y cuantitativo, ALE.

\* Factores de riesgos de Seguridad de la Información

Normas de seguridad de la información

\* Áreas, objetivos y controles de la ISO 27002. Controles claves. Procedimientos

\* Selección de controles. Declaración de aplicabilidad. SOA.

\* Implementación ISO 27001 de un Sistema de Gestión de Seguridad de la Información, SGSI. Fases del modelo PDCA de mejoramiento continuo.

\* Documentación del SGSI.

\* Acciones gerenciales

\* Certificación. Auditorías Internas.

Otras normas

\* Normas complementarias. ISO 13335, 15408, 18028 y 18044

\* La nueva serie 27000 de normas ISO. Títulos, publicaciones.

Gestión de riesgos de Seguridad de la Información

- \* Las normas ISO 27005 y AS/NZS 4360
- \* El aporte de la norma BS 7799-3. Ciclo de vida y PDCA. Procesos y funciones de negocio. Criticidad de activos. Reajuste de niveles de riesgo, coeficiente de importancia. Prorización. Monitoreo y métricas de gestión; medición del desempeño, CSF y KPI; revisión; informes. Mejoramiento.
- \* Pérdidas de productividad y de ingresos.
- \* Introducción al ROSI. El caso de negocios. El BSC o Tablero de Comando aplicado a la seguridad.

#### Sistemas de gestión

- \* Armonización con los Sistemas de Gestión de Calidad (ISO 9001) y Ambiental (ISO 14001).
- \* Corporate Governance, Principios de la OECD. Código combinado y Turenbulli; COSO/ERM.

#### Guías y ayudas de implementación

- \* Herramientas comerciales de libre acceso.

#### Experiencias y proyectos

- \* Experiencia de implementación.
- \* Gerenciamiento en Seguridad de la Información: Formación de un CISO.

#### Valores agregados

- \* Necesidades y oportunidades
- \* Aplicaciones de un SGSI: Continuidad de Negocios, Sarbanes-Oxley, Basilea II y protección de datos.

#### Taller de Práctica

Con una duración de todo un día, el esquema de trabajo para el taller se basa en grupos a modo de Foro de Gestión conforme a la recomendación de la norma.

- \* Análisis de riesgos, niveles de trabajo. Discusión y pruebas con diferentes aproximaciones.
- \* Análisis gap. Ampliación del temario de verificación.
- \* Plan basado en Delphi para la determinación de vulnerabilidades organizacionales y operacionales.
- \* Desarrollo práctico del alcance, política general, normas de uso, controles de seguridad y procedimientos.
- \* Guía y práctica de implementación con más de 40 archivos de trabajo Word y Excel, tomadas de experiencias reales con ejemplos saneados de información sensible.

### **Material Entregado**

#### MATERIAL DEL TALLER

- 1 - Documentación del taller
- 2 - Esquema general de procesos
- 3 - Diagrama de flujo
- 4 - Cronograma de implementación
- 5 - Alcance, política general y políticas de uso
- 6 - Activos primarios clasificados
- 7 - Vulnerabilidades clasificadas
- 8 - Vulnerabilidades físicas, organizacionales y operacionales verificadas

- 9 - Vulnerabilidades verificadas Unix/Linux
- 10 - Amenazas definidas
- 11 - Matriz de Riesgos
- 12 - Amenazas vs. Activos
- 13 - Riesgo Activo de muestra
- 14 - Vulnerabilidades en Incidentes
- 15 - Prioridades riesgos totales de Activos
- 16 - Centro de Cómputos - Amenazas vs. Vulnerabilidades
- 17 - Riesgos Centro de Cómputo - Localización n
- 18 - Software y Aplicaciones - Amenazas vs. Vulnerabilidades
- 19 - Riesgos Software y Aplicaciones - Localización m
- 20 - Riesgos Servidor Windows
- 21 - Riesgos Servidor Windows - S11
- 22 - Resumen riesgos servidores
- 23 - Riesgos y Cruces
- 24 - Pérdidas productividad e ingresos
- 25 - Punteo controles 27002:2005
- 26 - Análisis Gap según ISO 27002
- 27 - Contraseñas: Controles vs. Riesgos
- 28 - Políticas de Uso
- 29 - Política de Contraseñas
- 30 - Foro de Gestión - Sugerencias
- 31 - Antecedentes de Controles y Procedimientos de seguridad
- 32 - Lista de Controles ISO 27002:2005
- 33 - Controles clasificados por Acciones
- 34 - Controles vs Parámetros seguridad
- 35 - Medición del desempeño: CSF, KPI y BSC
- 36 - Controles comparados por v2000
- 37 - Controles comparados por v2005
- 38 - Controles de seguridad a desarrollar
- 39 - Análisis sistemas contraseñas
- 40 - Checklist de auditoría
- 41 - Analista/Auditor de Seguridad - Perfil de requerimientos
- 42 - Programa de Concientización y Capacitación

#### CONTENIDO DEL CD

- o Material del taller (42 documentos)
- o Norma IRAM 17550 (Draft)
- o ISO 27002 en Español
- o Sistema Alemán BSI
- o ISO 27001 en Español
- o Nuevo Manual BSI 2007

## **Fechas de cursada :**

Miércoles 27 de mayo y jueves 28 de mayo

## **Lugar de Dictado**

Centro Argentino de Ingenieros

Instituto de Formación Continua

Cerrito 1250 - Ciudad Autónoma de Buenos Aires

## **Horario:**

Miércoles y jueves de 9 a 18 hs.

## **Duración**

16 horas, en dos jornadas de 8 horas

## **Profesor**

Ing. Carlos Ormella Meyer

## **Curriculum**

Ingeniero Electrónico, ha sido Profesor universitario y de Maestría.

Es consultor, analista y auditor en seguridad de la información, redes inalámbricas e Internet, con especial dedicación al análisis y gestión de riesgos, cumplimiento/certificación de normas ISO 27002/ISO 27001, y protección de datos personales. Especializado en implementación de medidas de seguridad en sistemas de Continuidad de Negocios, para tratamiento de Riesgos Operacionales en entidades financieras según Basilea II, y conformidad Sarbanes-Oxley. De la misma manera se desempeña en trabajos de evaluación económica-financiera y administración de proyectos.

Desde hace 30 años viene participando en Venezuela y Argentina en la implementación y dirección de sistemas de telecomunicaciones por microondas terrestres y satelitales, sistemas de control de estaciones no atendidas, teleproceso, acceso remoto, LAN, WAN, LANs Inalámbricas, sistemas de seguridad de la información, y planificación de continuidad de negocios y planes de contingencia.

Los últimos años los ha dedicado en gran parte a la implementación de las normas en diferentes empresas, entre ellas , el grupo Aluar/Fate, donde Aluar es una de las plantas de aluminio más grandes de Latinoamérica, y Fate es una de las principales fábricas de neumáticos de Argentina.

Desde 1985 viene dictando cursos y conferencias en Argentina, Venezuela, Paraguay, Perú, El Salvador y Uruguay.

Ha sido editor de la revista LAN & WAN donde ha publicado varios centenares de artículos de tecnología.

## **Inscripcion**

Por esta WEB, por e-mail a [clubdeprogramadores@fibertel.com.ar](mailto:clubdeprogramadores@fibertel.com.ar)  
o por TE al 4383-2670

### **Reserva de vacante**

LA VACANTE SE RESERVA ABONANDO EL CURSO

### **Costo**

\$800

### **Descuentos especiales a estudiantes y socios del CAI**