

CURSO - TALLER

“Gestionando Seguridad de la Información, construyendo una ventaja competitiva”

Episodio I – El despertar de la fuerza

Instructores: Lic. Carlos Freyre, MBA, CBCI – Lic. Valentín Almirón, Lead Auditor ISO-27001

Duración: 16 hs.

La utilización de las **Tecnologías de la Información y las Comunicaciones** ha llevado a las empresas a tener que actualizarse dando un giro radical en la forma de llevar a cabo los negocios, y para ello han incorporado a sus operaciones diarias herramientas informáticas y sistemas de información que les permitan operar más eficientemente, como factor de ventaja competitiva. De allí que en la actualidad, la mayor parte de la información de una empresa reside en equipos informáticos, redes de comunicación de datos, dispositivos móviles y soportes de almacenamiento.

Existen **riesgos físicos y naturales** que pueden afectar el adecuado funcionamiento de la tecnología utilizada y, por ende, la continuidad de las operaciones de negocio. También existen **riesgos lógicos**, intrínsecos a la propia tecnología empleada, que pueden afectar a la información y sus características. Espionaje cibernético, virus informáticos, robos de identidad y accesos no autorizados, son algunas de las amenazas que pueden acabar con la confianza de clientes y la imagen de las empresas.

En la medida en que este crecimiento y evolución hacia las TICs aumenta, también se incrementa la necesidad de tomar conciencia y capacitarse en temas relacionados con **Seguridad de la Información**. Para ello, la adopción de prácticas internacionales, como la **serie ISO-27000**, permitirá establecer y mejorar el desempeño de la gestión a través de un enfoque sistemático y de mejora continua.



▶ OBJETIVO GENERAL DEL TALLER

Desarrollar y comprender un modelo de **Sistema de Gestión de Seguridad de la Información**, a través del conocimiento de mejores prácticas internacionales que proporcionen una adecuada orientación para su implantación y gerenciamiento.

▶ OBJETIVOS ESPECIFICOS

Utilizando ejemplos y casos de estudio basados en escenarios de la vida real, el taller recorre las etapas necesarias para:

- Comprender la importancia que tiene para la organización gestionar la seguridad de la información como actividad de prevención y control.
- Conocer las metodologías y mejores prácticas que existen en la industria para una adecuadamente gestión de la seguridad.
- Aprender a realizar un análisis de situación de la organización, proponer y/o implementar acciones de mejoras.
- Entender las bases fundamentales para proteger la información de la organización.

▶ DESTINATARIOS

Profesionales de las áreas de Tecnología, Sistemas y Seguridad de la Información, Auditores, Consultores y Profesionales involucrados en la necesidad de implementar un Sistema de Gestión de Seguridad de la Información.

▶ TEMARIO

1. Introducción

- Objetivos del curso
- Agenda
- Generalidades
- La información como principal recurso
- Los sistemas de información como herramientas gerenciales
- Costos y manejo de la información empresarial

2. Problemática planteada

- Fraudes, amenazas y vulnerabilidades asociadas a las tecnologías de la información y las comunicaciones
- ¿Seguridad Informática es un centro de costos de sólo egresos?
- Creación de valor para el negocio, ¿con seguridad?
- ¿Se puede gestionar la seguridad sin un sponsor?
- ¿Seguridad intrínseca o por cumplimiento?
- ¿Tercerizar la seguridad es válido?

3. Herramientas utilizadas

- Características de seguridad de la información
- Estándares internacionales, leyes y reglamentaciones relacionadas (ISO-27000, COBIT, OSWAP, BCRA A-4609, y otros)
- Planificando la seguridad de la información en la organización
- Estableciendo los pilares de la seguridad en la organización
- Generando políticas organizacionales
- Asignando responsabilidades
- Identificando activos de información
- Acompañando las actividades del negocio
- Gestionando configuraciones de seguridad y controles en procesos
- Estableciendo acuerdos con todas las partes interesadas
- Creando un área soporte a disposición de los usuarios internos

4. Conclusiones y recomendaciones

- Oportunidades y amenazas
- Diferenciando organizaciones grandes, medianas, pequeñas, familiares y unipersonales
- Construyendo pilares con conceptos de seguridad de la información
- Consideraciones para una adecuada planificación
- Certificando ISO-27001

► PERFIL DE LOS INSTRUCTORES:

- Lic. Carlos A. Freyre, MBA, CBCI

Carlos es Licenciado en Sistemas y posee una Maestría en Administración de Empresas; está certificado por el Business Continuity Institute y aplica como miembro profesional del Project Management Institute. Tiene experiencia de más de 30 años obtenida en empresas de primera línea, gestionando operaciones en áreas de Sistemas, Seguridad de la Información, Continuidad del Negocio, Auditoría y Consultoría, en diferentes tipos de industrias: entidades financieras, redes de cajeros automáticos, tarjetas de crédito, cámaras compensadoras, empresas comerciales y de manufactura, salud, organismos públicos y no gubernamentales. También es docente universitario, participa de comités en diferentes organizaciones sin fines de lucro, ha disertado en diferentes exposiciones y dado charlas relacionadas con seguridad de la información. Su especialidad se encuentra en el análisis de procesos y controles, su integración con sistemas de información, selección e implementación de plataformas tecnológicas, brindando así herramientas para la toma de decisiones gerenciales y de negocios.

- Lic. Valentin N. Almirón, Lead Auditor ISO-27001

Valentín es Licenciado en Tecnología Informática; está certificado por TÜV Rheinland Akademie como Lead Auditor ISO-27001. Tiene experiencia de más de 10 años obtenida en empresas de primera línea, en la operación de infraestructura y redes, implementando soluciones Open Source, en la administración de servidores de correo electrónico, bases de datos y servidores web, gestionando seguridad en proyectos y en el desarrollo de software, análisis de vulnerabilidades y penetration tester, implementando la norma ISO-

27001 y mantenimiento del SGSI, en diferentes industrias: empresas de transporte de pasajeros, software factory para entidades financieras y organismos sin fines de lucro. Es un especialista en la implementación de seguridad en procesos y sistemas informatizados con amplios conocimientos técnicos y normativos. También fue redactor en la edición de Técnico en Redes y Seguridad de la revista RedUsers.

▶ **MODALIDAD DE DICTADO**

- **Presencial:** en instalaciones de primer nivel del Microcentro de la Ciudad de Buenos Aires – Argentina.
- **Bibliografía utilizada:**
 - ISO 27000 - Information Security Management Systems,
 - ITIL - Information Technology Infrastructure Library,
 - COBIT - Control Objectives for Information Technology,
 - OSWAP - Open Web Application Security Project,
 - Leyes Nacionales de Delitos Informáticos, Firma Digital, Propiedad Intelectual y Protección de Datos Personales, y
 - Comunicaciones del Banco Central de la República Argentina A-4609 / A-4793 / A-5374.
- **Descuentos por inscripción temprana. Consultas y reservas:** info@sinergialc.com