SINERGIA Learning Center

CURSO - TALLER
"Implementando Seguridad de la Información, poniendo manos a la obra"

Episodio II – Nace una esperanza

Instructores: Lic. Carlos Freyre, MBA, CBCI – Lic. Valentín Almirón, Lead Auditor ISO-27000
Duración: 16 hs.

El apego de las empresas a las **Tecnologías de la Información y las Comunicaciones** que brindan tantas herramientas para generar ventajas competitivas tan importantes, trae aparejado consigo **riesgos intrínsecos** derivados del mismo entorno. A medida que las organizaciones fueron consolidando sus procesos en los sistemas informáticos, su supervivencia termina basándose netamente sobre la misma tecnología aplicada la cual dista enormemente de ser perfecta e inviolable. Desde desastres naturales como **incendios, inundaciones o terremotos**, pasando por situaciones no intencionales como **fallas eléctricas, tecnológicas o errores humanos**, hasta acciones deliberadas como **espionaje, falsificación, fraudes, sabotaje o venta de información**, pueden bastar para generar una grave crisis. Pero no sólo las causas externas son los únicos factores a los cuáles habrá que temer, por el contrario, la mayor cantidad de amenazas suele provenir del propio personal de la compañía, usuarios internos que cometen errores involuntarios o directamente delitos malintencionados.

En esta nueva dimensión para el intercambio de información, existe un área de la informática que se especializa en la protección de las plataformas tecnológicas y de la información que en ellas se gestiona. La Seguridad de Tecnologías de la Información, o simplemente Seguridad de la Información, dispone de estándares, protocolos, métodos, reglas, mejores prácticas y herramientas que permiten minimizar posibles riesgos informáticos y esas amenazas a las que nos vemos expuestos con el uso de las nuevas tecnologías. Una adecuada implementación de un **Sistema de Gestión de Seguridad de la Información** brindará la protección del activo más valioso de las organizaciones actuales, la información.

OBJETIVO GENERAL DEL TALLER

Desarrollar y comprender el proceso de evolución de un modelo que proporcione una adecuada orientación para aquéllos que deseen implementar, gestionar y/o mejorar un **Sistema de Gestión de Seguridad de la Información** dentro de su organización.

OBJETIVOS ESPECIFICOS

Utilizando casos de estudio basados en escenarios de la vida real, los asistentes adquirirán conocimientos prácticos sobre cómo llevar a cabo la implementación de un SGSI en el marco de la **serie ISO-27000**:

- Reconocer la extensión y alcance para lograr una adecuada planificación de la implementación.
- Analizar la integración del SGSI a implementar con los Sistemas de Gestión existentes en la organización (Planificación Estratégica, Calidad, Responsabilidad Empresarial).
- Desarrollar políticas y procedimientos basados en estándares y mejores prácticas de la industria.
- Definir controles para garantizar el cumplimiento de las políticas internas.
- Conocer las herramientas que faciliten su implementación y ejecución.

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
    - Seguridad de la información en las organizaciones

2. Problemática planteada
    - ¿Es posible contar con un adecuado entorno de seguridad y control?
    - ¿Podemos crear valor implementando seguridad?, ¿a qué costo?
    - ¿Sirven los estándares internacionales a la hora de la implementación?
    - Cumpliendo leyes y reglamentaciones, apalancamiento para la seguridad
    - Ransomware, ¿es la nueva vieja estrella del malware?

3. Herramientas utilizadas
    - Planificando la implementación seguridad de la información a largo plazo
    - Evaluando plataformas tecnológicas y canales críticos
    - Desarrollando procedimientos, instructivos, estándares y criterios
    - Seleccionando herramientas corporativas de gestión como Caballos de Troya
    - Gestionando los activos de información en la organización
    - Identificando adecuadamente los riesgos y sus mitigaciones

- Estableciendo:
  - Seguridad de los recursos humanos
  - Protección física de los recursos tecnológicos
  - Seguridad lógica de los recursos tecnológicos
  - Prevención de fuga de información
- Adquisición, desarrollo y mantenimiento seguro en el ciclo de vida del software
- Buenas prácticas en la utilización de redes sociales y comunicaciones externas
- Identificando eventos y gestionando incidentes
- Acompañando la continuidad del negocio
- Auditoria de sistemas de información, nuestros primos cercanos
- Bondades del ethical hacking
- Desarrollando actividades de concientización

4. Conclusiones y recomendaciones
   - Fortalezas y debilidades
   - Planificando la seguridad en la organización
   - Consideraciones para una adecuada planificación
   - Desarrollando una guía básica para la implementación de seguridad
   - Creando indicadores de confianza

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-27000:

  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 considerada:**
  - 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**