Ing. Carlos Ormella Meyer y Asoc.
Gestión y Auditoría de Riesgos y Seguridad de la Información
Tel: +54-11-3979-7220 – Cel: +54-911-6513-2751
E-mail: ingcomyasoc@gmail.com

# GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACION

## Exposición y Taller de práctica

**Desde la emisión de las normas de seguridad de la información ISO 27001 y 27002, se ha venido poniendo en claro su importancia a nivel corporativo en los negocios de una empresa, más allá del recurrente concepto básico de la seguridad informática limitado al área TIC.**
**Los diferentes métodos de cálculo de riesgos dan lugar a una serie de posibilidades y cuestiones.**
**Por su parte, la norma ISO 27005 proporciona un importante aporte que fortalece la estrategia auto-consistente de la serie ISO 27k, al establecer cómo se analizan y gestionan los riesgos.**
**Y además, la nueva norma ISO 31000 de Riesgos Corporativos (y su complemento la ISO 31010 de Técnicas de Valuación de Riesgos) establece conceptos y criterios comunes, como los de Oportunidades y Riesgos Positivos, con otras normas de riesgos.**

**DURACION:** 12 horas, incluyendo la realización de tres Trabajos Prácticos.

**¿QUIÉNES DEBEN PARTICIPAR?:**
- Administradores de seguridad de la información que deben administrar la gestión de riesgos e informar a la gerencia media y superior en cuanto a los negocios de la empresa.
- Gerentes de Proyectos cuadros medios de Sistemas, Computación y Tecnología.
- Gerentes y Directores de Riesgos que busquen integrar los riesgos de Seguridad de la Información en los riesgos corporativos de una organización.
- Auditores de seguridad y de sistemas, auditores internos y externos.

**OBJETIVOS**
*Reconocer, revisar, analizar y articular:*
- Los riesgos organizacionales, operacionales, físicos y de sistemas TIC, y metodologías para su determinación.
- El análisis y gestión de riesgos.
- Los factores que producen la resistencia al cambio frente a la implementación de medidas de seguridad y las bases para un buen manejo de las situaciones, y obtener así resultados consistentes y sustentables.
- La participación activa en un taller realizando tres trabajos prácticos, con material disponible para proyectos particulares.

**METAS A ALCANZAR:**
Finalizado el curso, los participantes podrán:
- Diferenciar los riesgos organizacionales y operacionales de los técnicos de sistemas TIC.
- Tener un sólido entendimiento de las distintas formas de valuar los riesgos de seguridad..

**TEMARIO DE LA PRESENTACIÓN**
**MÓDULO DE ESTUDIO 1 - Aseguramiento y normas de seguridad**
- El aseguramiento de la información y el Corporate Governance
- Seguridad de la Información y Seguridad Informática
- Norma ISO 27002
- Norma ISO 27001
- Gobierno de Seguridad de la Información

**MÓDULO DE ESTUDIO 2 - Métodos de cálculo de riesgos**
- Formas de análisis de riesgos
- Cálculo de riesgos por las entidades. Metodología Delphi.

• Cálculo de riesgos por las pérdidas. Modelos cualitativos
• Análisis cuantitativos por pérdidas ALE.
• Histograma, Polígono de frecuencias.
• Distribuciones estadísticas. Curva normal, parámetros.
• Distribución LDA, Valor en Riesgo y Colas anchas
• Metodología Bow-tie
• Incertidumbre y riesgos
• El Factor Gente
• Regla de Bayes
• Redes bayesianas
• Simulación Monte Carlo
• Variantes del cálculo de riesgos. NIST 800-30
• Mejoras en el cálculo de riesgos por entidades y por pérdidas
• Estados de riesgo y Riesgo Residual
• Riesgo Residual y Salvaguardas por entidades y por pérdidas.
• Riesgos Positivos. Oportunidades. Comparación entre riesgos positivos y negativos

**MÓDULO DE ESTUDIO 3 - Normas de riesgos de Seguridad**
• Norma ISO 27005 de gestión de riesgos de seguridad
• Norma ISO 31000 de gestión de riesgos corporativos. ISO 31010 de técnicas de valuación de riesgos
• Mejoras en el cálculo de riesgos

## TALLER DE TRABAJO

• El Taller consiste en realizar tres Trabajos Prácticos basados en experiencias reales y que pueden usarse posteriormente para sus proyectos particulares.

**Documentos sobre los que se realizan los Trabajos Prácticos**
1 - Análisis Gap de riesgos según ISO 27002
2 - Cálculo de Riesgos con LDA
3 - Selección de técnicas de valuación de riesgos según ISO 31010

## MATERIAL DE LECTURA Y SOPORTE

1) Módulos de estudio
2) Material del taller (3 documentos para Trabajos Prácticos)
3) Otros archivos
   • Normas ISO de Seguridad de la Información – Abstract
   • ISO 27000:2014
   • ISO 27001:2013
   • ISO 27002:2013
   • Las nuevas versiones de las normas ISO 27001 e ISO 27002
   • ISO 27005
   • ISO 31000
   • ISO 31010
   • Objetivos de Control y Controles de la ISO 27002:2013
   • NIST 800-53
   • NIST 800-55v1
   • Controles NIST (De la publicación 800-53r1)
   • Listado y enlaces de publicaciones de la serie 800 del NIST
   • Gobierno de Seguridad de la Información y Gobierno Corporativo
   • Hacia un Marco de Medición – GQM (en inglés)
   • Nuevas Perspectivas de la Seguridad de la Información
   • Seguridad Informática vs. Seguridad de la Información
   • Análisis de Impactos y Valuación de Riesgos
   • El Factor Gente y la Seguridad de la Información
   • El ROI de la Seguridad y las Primas de seguro

- Preguntas y Respuestas Normas de Seguridad de la Información
- Preguntas y Respuestas Riesgos de Seguridad de la Información
- Preguntas y Respuestas Métricas de Seguridad
- Preguntas y Respuestas Privacidad y Protección de Datos Personales
- Preguntas y Respuestas ROSI, el ROI de la Seguridad
- Preguntas y Respuestas Firma Digital y Factura Electrónica

**Instructor:** Ing. Carlos Ormella Meyer

Ha sido Profesor Universitario de Grado en la UTN y de Maestría en la UMSA.Consultor, analista y auditor interno en seguridad de la información, estrategias y políticas de seguridad y protección de datos personales, especializado en:

- Transformación Digital. Proceso completo: Digitalización: Cultura y Estrategias Digitales, Modelo de Negocio, Cadena y Propuesta de Valor, y Experiencia de los clientes.
- Machine/Deep Learning, analítica predictiva y ciencia de datos. Big Data e IoT.
- Analítica Avanzada e Inteligencia Artificial
- Edge Computing y aplicaciones de IoT e Internet Industrial
- Aplicaciones empresariales de Blockchain
- Análisis y tratamiento de Oportunidades como Riesgos Positivos
- Métricas de controles ISO 27001. Uso en la Nube con CSF de NIST y CCM de CSA
- Aplicación de Bayes en incidentes. Redes bayesianas: análisis y toma de decisiones.
- Métricas para medir la Efectividad de Planes de Concientización.
- Medición de la efectividad de medidas de seguridad y tratamiento de observables en auditoría por medio del Tablero de Control del Balanced Scorecard.
- Justificación de inversiones en seguridad, ROSI y Business Case.
- Análisis y gestión de riesgos, cumplimiento de normas ISO 27001/27002, evaluación y administración de proyectos de seguridad.

Participó y dirigió en Venezuela y Argentina la implementación y dirección de sistemas de telecomunicaciones por microondas, y sistemas de seguridad de la información.

Desde 1985 dicta cursos en Argentina y otros países, últimamente sobre tecnologías digitales, Machine Learning, Inteligencia Artificial, Transformación Digital, y tecnologías y metodologías de soporte de la Cadena de Valor.

Fue editor de la revista LAN & WAN donde publicó más de un centenar de artículos.

Desde hace años ha venido vertiendo sus experiencias en notas y artículos la página Web (www.angelfire.com/la2/revistalanandwan) y comunidades como Criptored (www.criptored.upm.es/paginas/docencia.htm).

Es miembro de Linkedin y participa activamente en grupos profesionales de la especialidad.