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

METRICAS 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.
La norma ISO 27004 proporciona un importante aporte que fortalece la estrategia auto-consistente de la serie ISO 27k, al establecer cómo se mide la eficiencia del sistema de gestión y la efectividad de las medidas de seguridad que se implementen, para reducir no sólo los riesgos técnicos de IT, sino también especialmente los riesgos operacionales, incluyendo los propios de los nuevos escenarios de ciberseguridad, estableciendo todo un marco que comparte la visión corporativa de negocios, especialmente mediante el uso del Balanced Scorecard, BSC.

DURACIÓN: 12 horas. Incluyendo la realización de tres Trabajos Prácticos.

¿QUIÉNES DEBEN PARTICIPAR?:
- Personal superior y funcionarios que necesitan conocer el alcance corporativo de la problemática y soluciones en cuanto a seguridad de la información y su trascendencia en los riesgos de negocios.
- Gerentes y cuadros medios de Sistemas, Computación y Tecnología. Administradores de seguridad de la información que deben administrar la gestión de riesgos, mensurar las medidas de seguridad y justificar las inversiones correspondientes.
- Auditores informáticos y de sistemas, auditores internos y externos.

OBJETIVOS:
Reconocer, revisar, analizar y articular:
- La ISO 27004 para las métricas del SGSI de la ISO 27001 y de la efectividad de los controles implementados.
- Las diferentes formas de verificar el cumplimiento de los objetivos de control y controles implementados de la ISO 27001.
- El mapeado de Objetivos de Control y Controles de seguridad con los Objetivos Operacionales e Iniciativas del Balanced Scorecard.
- 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:
- Tener un sólido entendimiento de los diferentes métodos para la determinación y uso de métricas de controles.
- Poder clasificar las verificaciones de eficiencia y efectividad de las medidas de seguridad en el contexto del necesario alineamiento de los objetivos operacionales de seguridad con los objetivos estratégicos a nivel corporativo.
- Comprender la importancia de las oportunidades como riesgos positivos y cómo pueden mensurarse.

TEMARIO DE LA PRESENTACIÓN
Conceptos Básicos para la Aplicación de Métricas
- El aseguramiento de la información y el Corporate Governance
- Seguridad de la Información y Seguridad Informática. Riesgos y Vulnerabilidades.
- Norma ISO 27002

• Norma ISO 27001
• Gobierno de Seguridad de la Información
• Métodos de análisis de riesgos.
• Salvaguardas. Riesgos residuales.
• Norma ISO 27005 de Gestión de Riesgos de Seguridad.
• El aporte de la norma británica BS 7799-3
• Norma ISO 31000 de Gestión de Riesgos Corporativos
• Riesgos Positivos: Oportunidades:
• El Factor Gente.
• Evaluación de la Concientización.
• Introducción a la Ciberseguridad. Infraestructuras Críticas.
• Marco de Ciberseguridad CSF de NIST. Mapeado a controles ISO 27001

Métricas de Seguridad de la Información y Aplicaciones
• Conceptualización de las métricas
• Norma de Métricas ISO 27004
• Características que deben satisfacer las métricas
• Métricas de controles, metodologías NIST y GQM
• Controles Críticos de Seguridad CIS.
• Madurez de las Métricas, modelo NIST.
• Las nuevas versiones de las normas ISO 27001 e ISO 27002
• Valuación de prioridades
• Métricas de Objetivos de Control
• Métricas de Oportunidades.

Desempeño de las Medidas de Seguridad - El Balanced Scorecard, BSC
• Gestión del desempeño de las medidas de seguridad
• Breve Introducción a CSF y KPI
• Presentación del Balanced ScoreCard (BSC)
• Perspectivas del BSC
• Objetivos estratégicos del BSC
• Temas Estratégicos del BSC
• Mapa Estratégico del BSC

Tablero de Control del BSC y Seguridad de la Información
• Tablero de Control o Comando
• Características de los Indicadores del BSC. Validación.
• Metas e Iniciativas del Tablero de Control
• Gestión y Reportes del BSC
• Objetivos Operacionales de Seguridad, Gestión y BSC
• KRI, Indicadores Claves de Riesgos

TALLER DE PRÁCTICA
• 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 - Métricas de Controles ISO 27002
2 - Indicadores y Medidas del BSC en función de Métricas
3 - Objetivos de Control y Controles de la ISO 27002 a partir de Objetivos Operacionales de Seguridad

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

MATERIAL DE SOPORTE Y LECTURA

1) Material de la Presentación
2) Material del taller (3 documentos para los Trabajos Prácticos)
3) Otros archivos
   - Normas ISO de Seguridad de la Información – Abstract
   - ISO 27000:2014
   - ISO 27001:2013
   - Las nuevas versiones de las normas ISO 27001 e ISO 27002
   - ISO 27005
   - ISO 31000
   - ISO 31010
   - NIST 800-53
   - NIST 800-55v1
   - Controles NIST (De la publicación 800-53r1)
   - CSF, Marco de Ciberseguridad de NIST.
   - Controles Críticos de Seguridad CIS
   - Objetivos de Control y Controles de la ISO 27002:2013
   - Gobierno de Seguridad de la Información y Gobierno Corporativo
   - Hacia un Marco de Medición – GQM (en inglés)
   - AHP, Tutorial sobre el Proceso de Análisis Jerárquico (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
   - Medidas del desempeño y el Balanced Scorecard
   - 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.