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

ROSI

El ROI de la Seguridad de la Información

Exposición y Taller de Práctica

Nunca ha sido simple estimar el retorno de una inversión de seguridad por lo que se volvió usual recurrir al FUD: Temor, incertidumbre y duda. Y, de hecho, promoviéndose los llamados Penetration Tests.

Pero todo eso hoy no basta para "vender" un proyecto de seguridad de la información.

ROSI es la herramienta adecuada para mostrar valores posibles que justifiquen tal inversión, sobre todo cuando se recurre a simulaciones como Monte Carlo que permite transformar criterios cualitativos de probabilidades en estimados cuantitativos razonables de beneficio-costo de seguridad.

DURACIÓN: 10 horas incluyendo la realización de dos Trabajos Prácticos

¿QUIÉNES DEBEN PARTICIPAR?:
- Jefes y líderes de proyecto de las áreas de Tecnología y Sistemas.
- Administradores y auditores de seguridad y sistemas.
- Gerentes y personal especializado del área de Administración, Finanzas y Organización y Métodos.
- Auditores internos.
- Profesores universitarios y personal docente de carreras de negocios y tecnológicas.
- Consultores

OBJETIVOS:
Reconocer, revisar, analizar y articular:
- Los conceptos económicos básicos de inversión, costos y gastos que permitan evaluar y justificar sus proyectos de seguridad.
- Forma sustentable de evaluar proyectos de seguridad de la información.
- Diferentes maneras de calcular el ROSI, como Retorno Sobre la Seguridad de la Información.
- Soluciones estadísticas a estimaciones de riesgos de seguridad en especial la simulación Monte Carlo.
- Participación activa en un taller realizando dos trabajos prácticos con material disponible para proyectos personales.

METAS A ALCANZAR
Finalizado el curso, los participantes podrán:
- Tener claro los conceptos de inversión, costos y gastos.
- Identificar y reconocer los diferentes factores que dan soporte al cálculo de ROSI: indicadores financieros, riesgos, toma de decisiones, estadística y simulación Monte Carlo.
- Identificar y aplicar los costos indirectos y las pérdidas de oportunidad.

TEMARIO

INTRODUCCION
- Las carencias del factor FUD: Temor, incertidumbre y duda.
- Problemática y estrategias.

CONCEPTOS BASICOS DE ROSI
- Objetivos. Reducción de las pérdidas por incidentes de seguridad.
- Valor y Costo de las salvaguardas o contramedidas.
- Cálculo básico de ROSI.
- Soporte para el análisis ROSI.

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

MODULOS DE SOPORTE

1 - Economía y Finanzas

- Concepto de indicadores financieros. Valor del dinero a lo largo del tiempo, valor actual y valor futuro. Flujo de fondos o flujo de caja. Flujo de Caja descontado. Costo de Oportunidad.
- Principales Indicadores financieros. Liquidez y rentabilidad. Período de recuperación de la inversión, PRI; el PRI descontado. Valor Actual/Presente Neto, VAN/VPN o NPV. Tasa interna de retorno, TIR o IIR. Retorno sobre la inversión, ROI. Valor económico agregado, EVA.

2 - Estadística

- Sistemas estocásticos. Variables aleatorias. Probabilidades.
- Distribución de probabilidades. Funciones de densidad de probabilidad y funciones de probabilidad acumulada. Distribuciones de variables discretas y continuas. Distribución normal o gaussiana, normalización. Parámetros de tendencia central: valor medio, desviación estándar, mediana, moda. Sesgo, curtosis. Normalización. Percentiles. Otros tipos de distribuciones, Poisson.

3 - Riesgos

- Riesgos, formas de análisis: por las pérdidas y por las entidades; análisis cuantitativo y cualitativo.
- Entidades de riesgos de seguridad. Activos, parámetros CIA de seguridad. Vulnerabilidades. Amenazas. Matriz de riesgos.
- Riesgos por pérdidas. Análisis cualitativo, niveles y matriz de riesgos.
- ALE, impacto y frecuencia anual de ocurrencia. Diagrama de barras., polígono de frecuencias.
- Aproximación a la Distribución de Pérdidas, LDA, pérdidas esperadas., Valor en Riesgo, VaR, y Pérdidas no esperadas.
- El problema de las colas anchas, incidentes de muy baja probabilidad y gran impacto.

4 - Toma de Decisiones

- Pérdidas de oportunidad.
- Condiciones de incertidumbre y riesgo.

5 - Bayes y Simulación Monte Carlo

- Limitaciones del LDA.
- Aproximación de Bayes. Probabilidades combinadas de datos históricos y distribución a priori en base a apreciaciones de expertos; probabilidades a posteriori.
- Incertidumbre y simulación de las condiciones aleatorias.
- Características de la simulación Monte Carlo. Generación de números aleatorios. Muestras.
- Aplicación de la simulación Monte Carlo. Riesgos cualitativos. Distribución de las variables de entrada. La Ley de los Grandes Números.

CALCULO DE ROSI

- Valorización y costo de las salvaguardas.
- Costos indirectos y pérdidas de oportunidad. Tipos de costos indirectos.
- Forma valorizada del ROSI, VAN o NPV. Gastos recurrentes, tiempo de vida del proyecto, valores presentes. Indicadores financieros complementarios.
- Análisis de ROSI con valores fijos. Resultados de indicadores financieros.
- Distribuciones estadísticas de las variables. Cálculo con valores estadísticos y simulación Monte Carlo.
- Observaciones al modelo.
- ROSI y el Caso de Negocios (Business Case).

TALLER DE PRÁCTICA

- Consiste en realizar dos Trabajos Prácticos.

DOCUMENTOS SOBRE LOS QUE SE TRABAJA

1 - Análisis ROSI de un proyecto de seguridad simplificado.
2 - Análisis y revisión de Riesgos y ROSI de un proyecto de seguridad con variables estadísticas por medio de la simulación Monte Carlo.

Tel: +54-11-3979-7220 – Cel: +54-911-6513-2751
E-mail: ingcomyasoc@gmail.com

a) Análisis y revisión las tres salidas de la simulación, junto con los parámetros correspondientes, así como de las Pérdidas No Esperadas.
b) Determinación de valores para el 10% y 90%, valores más frecuentes, dispersión, sesgo y percentiles; determinación del VaR, y valores de la cola.
c) Cambiar la escala de los impactos; primero triangular continuo en 6 escalas de 2x2 de 2,5 K a 10M, y luego con valores de 2x2,5 de 1K a 15,6 M. Comparar los resultados con los obtenidos en a).
d) Dejar únicamente las salvaguardas que reducen sólo las probabilidades de ocurrencia, y revisar los resultados obtenidos luego de correr la Simulación Monte Carlo.

MATERIAL DE SOPORTE Y LECTURA

• xla (Quadrant)
• xl Sim
• Soporte ROSI
• Normas ISO de Seguridad de la Información – Abstract
• ROSI, Retorno Sobre la Inversión en Seguridad - Abstract
• El ROI de la Seguridad y las Primas de seguro
• El Factor Gente y la Seguridad de la Información
• Medidas del desempeño y el Balanced Scorecard
• Seguridad Informática vs. Seguridad de la Información
• Análisis de Impactos y Valuación de Riesgos
• 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

Instructor: Ing. Carlos Ormella Meyer

Ha sido Profesor Universitario de Grado en la UTN y de Maestría en la UMSA.
Es consultor, analista y auditor interno en seguridad de la información, análisis y gestión de riesgos, protección de datos personales, cumplimiento/certificación de normas ISO 27002/ISO 27001, con especial dedicación en los últimos años a la determinación y uso de:

• Aplicación de Machine Learning y Deep Learning en Big Data e IoT.
• Analítica Avanzada y técnicas de Inteligencia Artificial en Ciberseguridad
• Métricas para controles ISO 27002 en base a las métricas de controles NIST
• Valuación de los resultados de los planes de concientización/capacitación bajo los criterios del conocimiento, actitud y comportamiento.
• Objetivos y métricas del tablero del control del Balanced Scorecard para medir la efectividad de las medidas de seguridad así como también la evolución en el tratamiento de observables en una auditoría interna.
• La regla de Bayes para la combinación de datos históricos cuantitativos y estimaciones subjetivas de expertos en los cálculos del ROI de la Seguridad, ROSI.
• Redes Bayesianas para la valuación de riesgos operacionales, especialmente para las entidades financieras que deben dar cumplimiento a los acuerdos de Basilea II y III.
• Complementación en la Nube de controles ISO 27001 con controles del CSF de NIST y controles CCM de CSA.
• Seguridad en BYOD, IoT (Internet de las Cosas), Big Data y Analítica.

Especializado también en la gestión de cambios organizacionales, implementación de medidas de seguridad en sistemas de Continuidad de Negocios, para tratamiento de Riesgos Operacionales en entidades financieras según Basilea II/III, y conformidad Sarbanes-Oxley. Asimismo se desempeña en trabajos de evaluación económica-financiera y administración de proyectos de seguridad.
Por más de 35 años ha venido 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 planes de continuidad de negocios y de contingencia.
Desde 1985 viene dictando cursos y conferencias en Argentina, Venezuela, El Salvador, Ecuador, Perú y Paraguay.
Ha sido editor de la revista LAN & WAN donde ha publicado más de un centenar de artículos de tecnología.
Últimamente viene vertiendo sus experiencias en notas y artículos en páginas Web y comunidades como Criptored (www.criptored.upm.es/paginas/docencia.htm).

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

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