ROSI

El ROI de la Seguridad de la Información

Una Introducción

© Carlos Ormella Meyer

Ing. Carlos Ormella Meyer & Asoc

ciprio@ingcomyasoc.com.ar

Introducción al ROSI

- **ROSI** es un indicador financiero derivado del **ROI**, que se usa para justificar la inversión en seguridad de la información en términos monetarios. Es un valor porcentual que relaciona el **retorno** o beneficio neto con la **inversión** que produce dicho retorno.
- En un plan de seguridad la ***inversión*** es el *costo* de la implementación de medidas de seguridad.
- El ***retorno***, a su vez, es la *diferencia entre las pérdidas actuales por incidentes de seguridad* y *las pérdidas esperadas* luego de aplicar dichas medidas de seguridad.

Introducción al ROSI

- Las pérdidas se reducen implementando **salvaguardas** o **contramedidas**, que de esta manera asumen como *retorno* el **valor** resultante por la reducción en las pérdidas y el **costo** correspondiente a la implementación de dichas salvaguardas, equivalente a la *inversión*.
- De esta manera, el retorno será la diferencia entre el *valor* y el *costo* de las salvaguardas.
- En base al ROI, entonces, en un plan de seguridad se tiene que:
  ROSI = Retorno / Costo, y por lo tanto:
  ROSI = (Valor – Costo) / Costo

Cálculo de ROSI

- Por otra parte, de forma similar al ROI, cuando el ciclo de vida del plan de seguridad es de varios años, hay que "traer" al *presente* valores y costos *futuros* de cada año, con cierta tasa de descuento equivalente al interés del dinero.
- De esta manera a valores presentes será: **Valor – Costo = VAN,** donde **VAN/VPN *(Valor Actual/Presente Neto)***, es el monto que complementa al ROSI, que es un porcentaje.
- Para calcular ROSI primero hay que determinar los valores de las pérdidas actuales y las que resultarían aplicando las medidas de seguridad.

Cálculo de ROSI

SUMARIO DE VALORES DEL ANALISIS ROSI	
Pérdidas Anuales por Incidentes - Sin tratar	$ 1,440,000
Pérdidas Anuales por Incidentes - Residual luego de mitigados	$ 671,000
Ahorro Bruto Anual por Contramedidas	$ 769,000
Costo Inicial Contramedidas	$ 278,000
Costos Anuales Recurrentes Contramedidas	$ 82,000

CALCULO DE ROSI (valores en miles)					
Años		**0**	**1**	**2**	**3**
Ahorro Bruto Anual			$ 769	$ 769	$ 769
Ahorro Bruto Anual a valor actual dto. 15%			$ 669	$ 581	$ 506
Valor Contramedidas	**$ 1,756**				
Costos Contramedidas		$ 278	$ 82	$ 82	$ 82
Costos Contramedidas a valor actual dto. 15%		$ 278	$ 71	$ 62	$ 54
Costo Contramedidas	**$ 465**				
Retorno (Valor - Costo)	**$ 1,291**				
ROSI (Retorno/Costo)	277 %	Igual a un:	56 %	anual	

ciprio@ingcomyasoc.com.ar

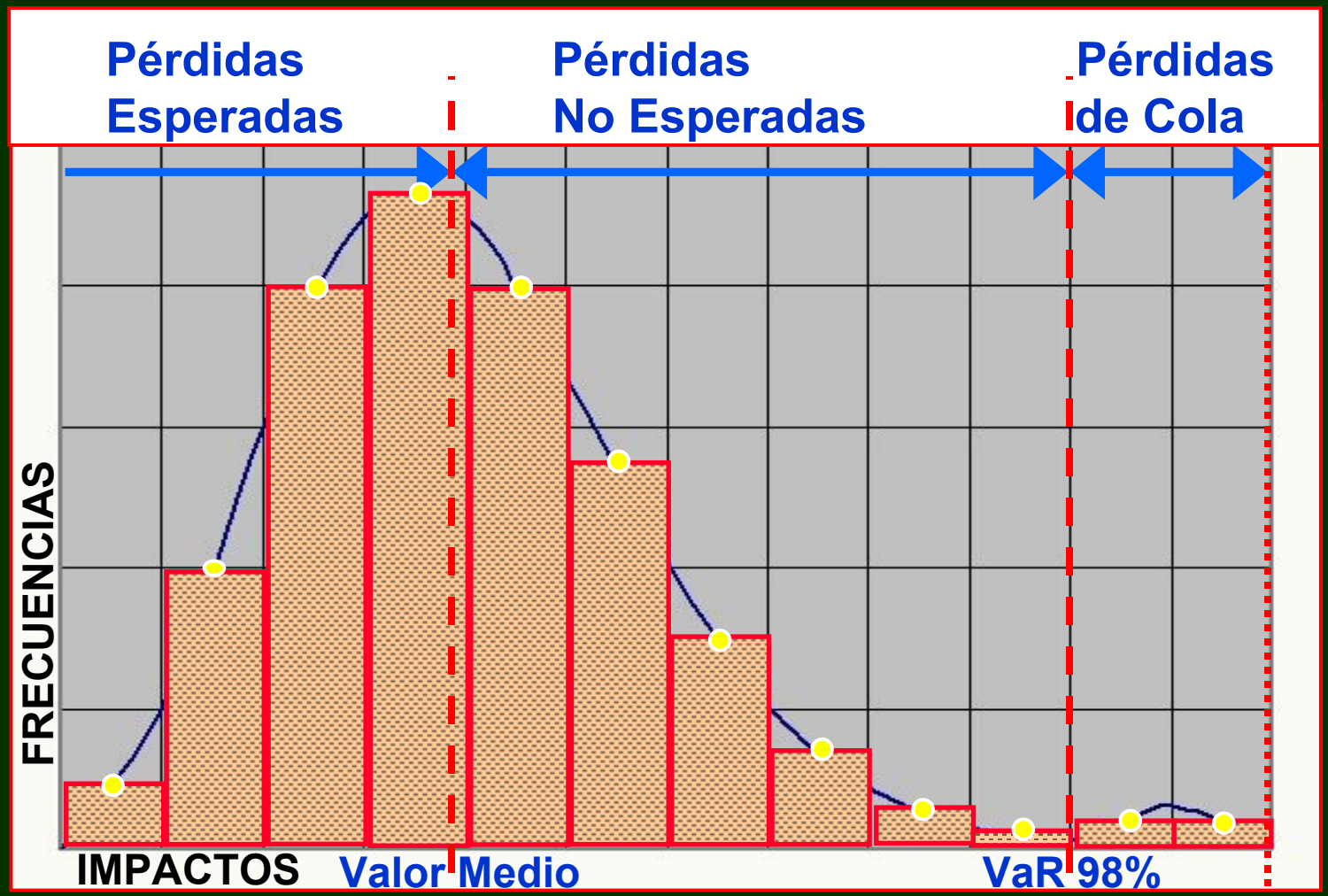
Cálculo de ROSI

- Para determinar las pérdidas que puede producir un incidente se emplea la métrica **ALE**, *Expectativa de Pérdidas Anuales*.
- ALE es igual a la **frecuencia o probabilidad anual** de ocurrencia de un incidente por el **impacto** correspondiente.
- Para un cálculo adecuado hay que tener datos históricos discretos de ambos parámetros.
- Las frecuencias iguales con diferentes impactos se pueden graficar como *diagrama de barras* y producir la curva de distribución estadística **LDA** o *Aproximación de Distribución de Pérdidas*.

Cálculo de ROSI

- En el ámbito de seguridad así como en otros como los propios de los **riesgos operacionales** que considera Basilea II, las distribuciones usuales resultan en *curvas asimétricas sesgadas a la derecha*.
- Por eso se usa el **VaR** o *Valor en Riesgo* para niveles de confianza del 95% o más.
- Además suele ocurrir que en la cola superior aparezcan valores superiores (*fat-tail*) a la tendencia de la curva en esa zona. En seguridad esto se debe a los *incidentes de baja y muy baja probabilidad de ocurrencia pero alto impacto*.

LDA aproximada con Poisson y Cola



ciprio@ingcomyasoc.com.ar

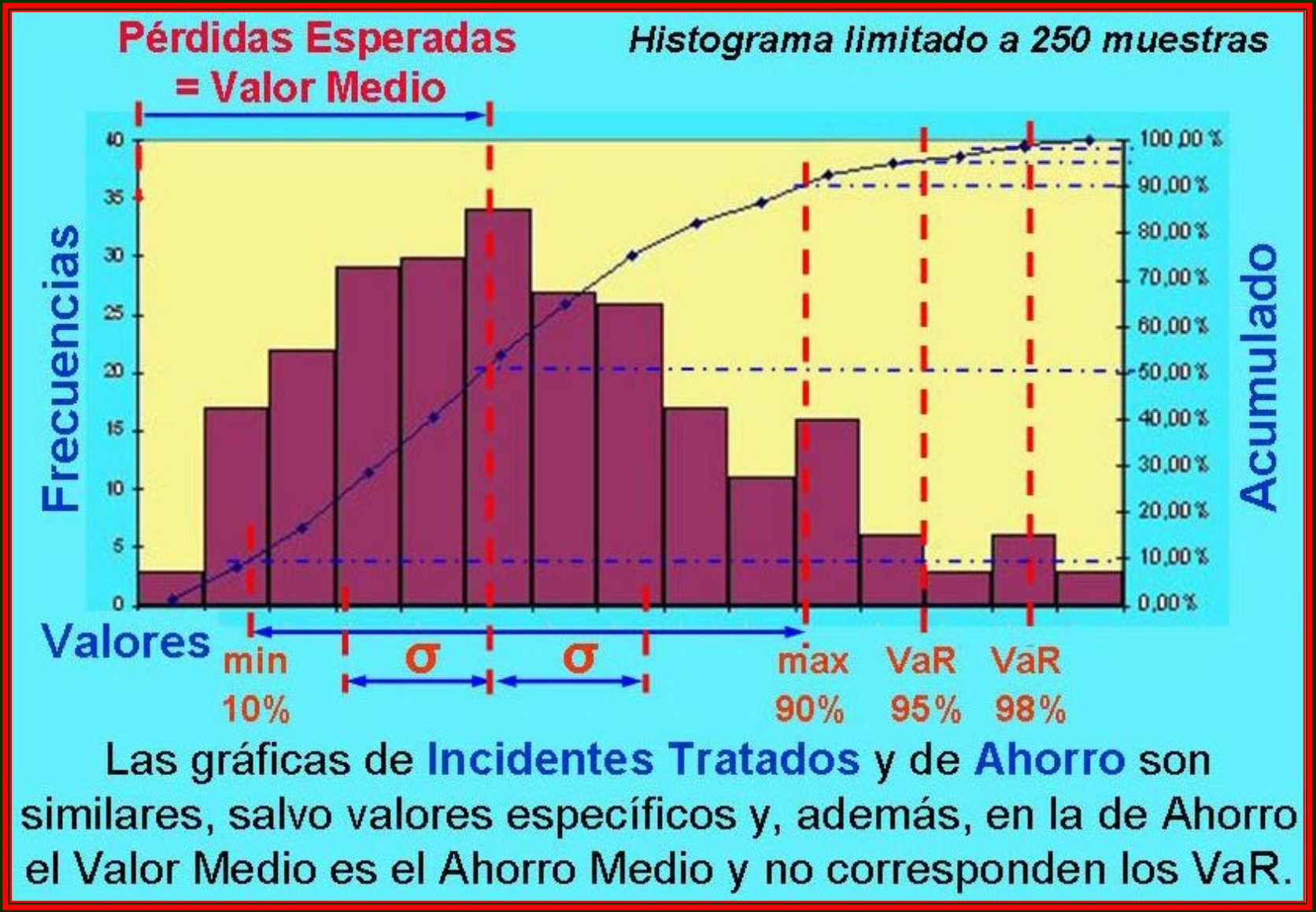
Problemática de la Incertidumbre

- Cuando no hay datos históricos concretos de impactos y/o de frecuencias de ocurrencia, el LDA pierde utilidad.
- Una solución es recurrir a métodos que combinen datos *cuantitativos* con *cualitativos*, como la aproximación de **Bayes**, donde los datos cualitativos responden al conocimiento u opinión personal, generalmente de expertos.
- Este procedimiento puede acarrear ***condiciones de riesgo*** con un margen importante de ***incertidumbre***, especialmente con datos históricos reducidos o nulos.

Simulación Monte Carlo

- La **toma de decisiones** en condiciones de *riesgo* puede analizarse con la **teoría estadística** y la *incertidumbre* de estas situaciones se puede tratar con la **simulación Monte Carlo**.
- **Simulación Monte Carlo:** Método estocástico, es decir aleatorio, que genera múltiples muestras en base a distribuciones estadísticas, de datos de impactos y frecuencias para el caso.
- Así se obtienen las *pérdidas antes* y *después* de aplicar salvaguardas, y la *diferencia resultante*.
- Los resultados serán valores y cotas indicativos de un análisis aceptable de proyectos.

Incidentes sin tratar con Monte Carlo



Las gráficas de **Incidentes Tratados** y de **Ahorro** son similares, salvo valores específicos y, además, en la de Ahorro el Valor Medio es el Ahorro Medio y no corresponden los VaR.

ROSI, Caso de Negocios y BSC

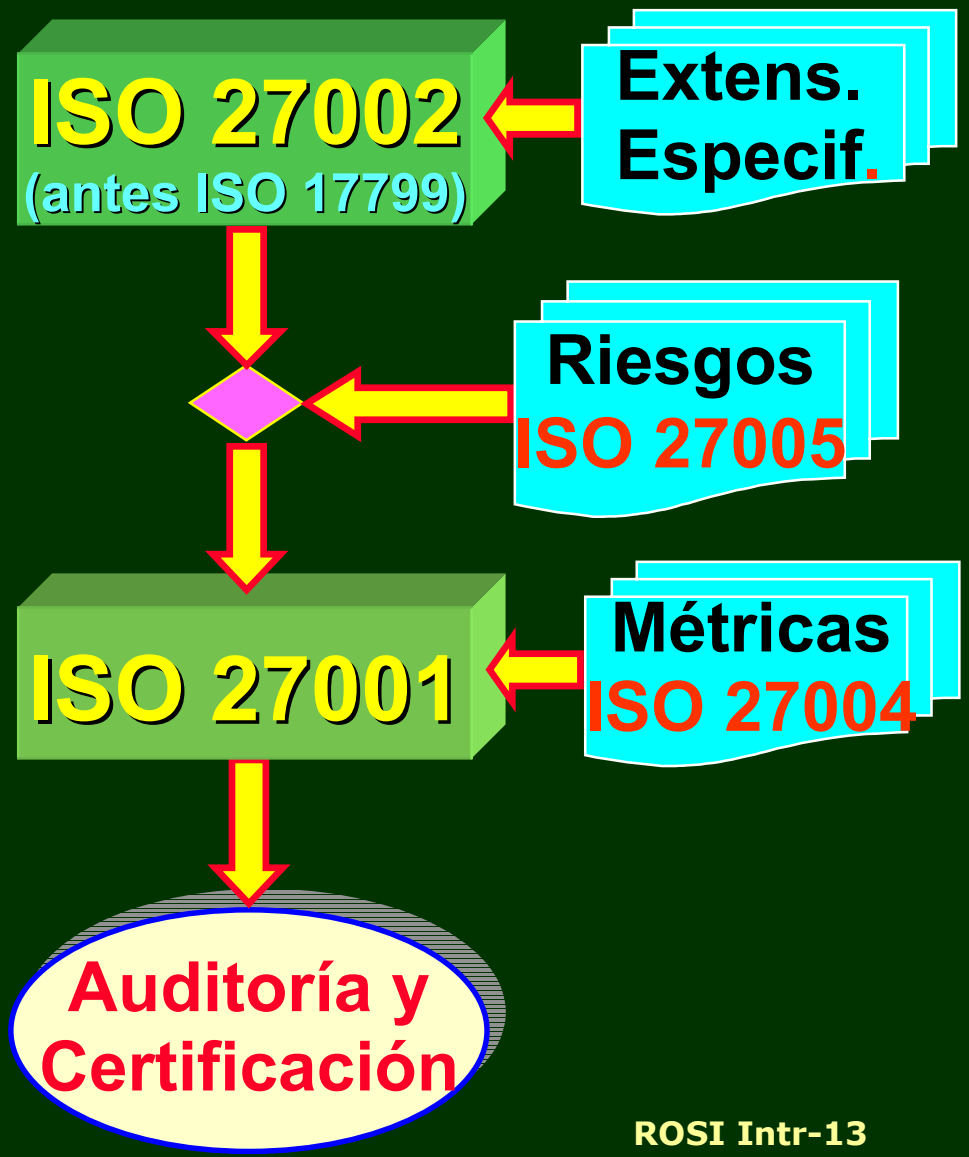
- ROSI puede ser parte del llamado **caso de negocios** o ***business case*** que permita tomar decisiones aceptables de riesgo en seguridad.
- Por su parte el **BSC**, *Balance-Scorecard (Mando Integral Balanceado, o Tablero de Comando)* es una metodología para medir el *desempeño* de las empresas y que puede usarse para presentar la información de seguridad como para que los ejecutivos pueden entenderla fácilmente.
- Al **BSC** se vincula la norma de métricas **ISO 27004**, de la serie de normas usadas justamente para determinar las medidas de seguridad.

Normas de seguridad de la información

Lista de controles *recomendados*

Selección de controles

Requisitos para implementar controles y establecer el **Sistema de Gestión de Seguridad de la Información, SGSI**



ciprio@ingcomyasoc.com.ar

ROSI

El ROI de la Seguridad de la Información

Una Introducción

Muchas gracias

Ing. Carlos Ormella Meyer

email: ciprio@ingcomyasoc.com.ar