



- Protección de datos y Seguridad de la Información
- Abogados TIC
- Formación
- ISO 27001

Retorno de inversión (ROI) en proyectos ISO 27001:2005. Alineamiento con el estándar.

Versión 1.0. 15 de octubre de 2008

PARA

www.iso27000.es

INTRODUCCIÓN AL RETORNO DE LA INVERSIÓN EN PROYECTOS ISO 27001

ÍNDICE

1. INTRODUCCIÓN A ROSI	3
2. ROSI E ISO 27001. INTEGRACIÓN	4
3. BENEFICIOS DE IMPLANTAR ISO 27001	6
4. CASO PRÁCTICO	7
5. OBSERVACIONES	10

1. Introducción a ROSI

El cálculo de retorno de inversión (**ROI**) siempre ha sido una herramienta muy adecuada para justificar inversiones de cara a la gerencia de una organización. Ver beneficios no siempre es fácil, por eso este tipo de cálculos han ido ganando protagonismo en los últimos tiempos.

En el caso particular de inversiones en seguridad, el término a utilizar se denomina **ROSI** (*Return Of Security Investment*) y al igual que ROI mide la relación entre el retorno que produce una inversión y la inversión propiamente dicha.

Centrándonos en ROSI, la esencia del cálculo se basa en calcular los **costes ahorrados como consecuencia de evitar incidentes de seguridad** o de mitigar los efectos de los mismos en caso de ocurrencia. Es por esto que en ROSI el beneficio es en realidad el ahorro conseguido (además de otro tipo de beneficios como pueden ser mejorar la imagen de la empresa consiguiendo así nuevos clientes).

ISO 27001 nos aporta confianza en este sentido, ya que habiendo implantado un sistema de gestión en seguridad de la información (**SGSI**) como se define en dicho estándar nos estamos asegurando una importante reducción y eliminación de incidentes de seguridad. Además, al estar dentro de un ciclo de mejora continua, conseguimos que el sistema de gestión responda a las nuevas necesidades de seguridad de la organización que vayan apareciendo.

A través de los diferentes **controles de seguridad** que plantea ISO 27001 en su ANEXO A podemos reducir de forma considerable la gran mayoría de incidentes que en caso de no implantar ningún sistema de seguridad podrían amenazar nuestra organización.

Otro factor clave a la hora de calcular el retorno de inversión en proyectos de implantación ISO 27001 es el hecho de tener que contar con un **Plan de Continuidad de Negocio (BCP, Business Continuity Plan)**. Gracias a un BCP tendremos asegurada –en un alto porcentaje– la continuidad de nuestro negocio en caso de desastre, como por ejemplo un incendio o un terremoto. Si bien en estos casos vamos a sufrir un importante daño en cuanto a costos, el hecho de poder seguir prestando servicios a nuestros clientes nos reporta unos beneficios que están muy por encima de los costos en implantar el plan (y nos evita las pérdidas de no poder prestar servicio, además de evitar daño hacia la imagen de nuestra marca y la percepción negativa que se llevaría el cliente).

LOPD - CONSULTORÍA – AUDITORÍA- FORMACIÓN – ISO 27001- ABOGADOS TIC

AUDISEC SEGURIDAD DE LA INFORMACIÓN S.L.

Hilarión Eslava 21 9º A Esc. Izq. 28015 MADRID

CENTRO CÍVICO EMPRESARIAL Vía Principal, S/N, 13200 - Manzanares (CIUDAD REAL)

Tlf: **902 056 203 -926 61 23 10** Fax 926 614 836 www.audisec.es -e-mail: comercial@audisec.es

2. ROSI e ISO 27001. Integración

La norma ISO 27001 contempla en todas sus fases elementos que son perfectamente integrables dentro de un estudio de retorno de inversión en seguridad.

- **Inventario y valoración de activos:** en esta etapa evaluamos el valor que para nuestra organización tiene cada uno de los activos que vamos a incluir dentro del alcance del SGSI a implantar.

La pérdida de confidencialidad, integridad o disponibilidad de alguno de nuestros activos puede ocasionarnos pérdidas tanto tangibles (reemplazo de activos o restauración de los daños causados) como intangibles (pérdida de imagen, reducción de la confianza de nuestros clientes, problemas para conseguir nuevos clientes).

- **Análisis de riesgos sobre los activos:** estudiamos las amenazas que podrían materializarse sobre nuestros activos y nuestros procesos de negocio. Calculamos también la frecuencia de ocurrencia de esas amenazas y el impacto que tendría sobre nuestro negocio.

Estas amenazas, a través de sus impactos, causan un daño al negocio que puede cuantificarse desde dos puntos de vista: desde el ahorro que supone no sufrir esos incidentes o desde el daño que supondría sufrirlas.

La propia ausencia de controles es una amenaza que se materializa en sufrir incidentes de seguridad.

- **Tratamiento de esos riesgos (reducción de incidentes):** en esta fase es donde implantamos los controles de seguridad que harán reducir o eliminar los incidentes de seguridad. Posteriormente se medirá la eficacia de esos controles para comprobar que realmente están siendo útiles para proteger nuestra organización.

El gasto de implantar estos controles es uno de los costos a tener en cuenta a la hora de calcular el ROSI.

- **Plan de continuidad (BCP):** un plan de continuidad de negocio, como su propio nombre indica, nos asegura poder seguir dando servicio a nuestros clientes en caso de catástrofes de origen natural (terremotos, inundaciones, etc.), industrial (incendios, explosiones, averías, etc.) o humano (errores no intencionados, ataques deliberados). Si bien implantar un BCP es costoso en tiempo y dinero, los beneficios obtenidos en caso de ocurrir un incidente grave pueden ser incalculables.

LOPD - CONSULTORÍA – AUDITORÍA- FORMACIÓN – ISO 27001- ABOGADOS TIC

AUDISEC SEGURIDAD DE LA INFORMACIÓN S.L.

Hilarión Eslava 21 9º A Esc. Izq. 28015 MADRID

CENTRO CÍVICO EMPRESARIAL Vía Principal, S/N, 13200 - Manzanares (CIUDAD REAL)

Tlf: **902 056 203 -926 61 23 10** Fax 926 614 836 www.audisec.es -e-mail: comercial@audisec.es

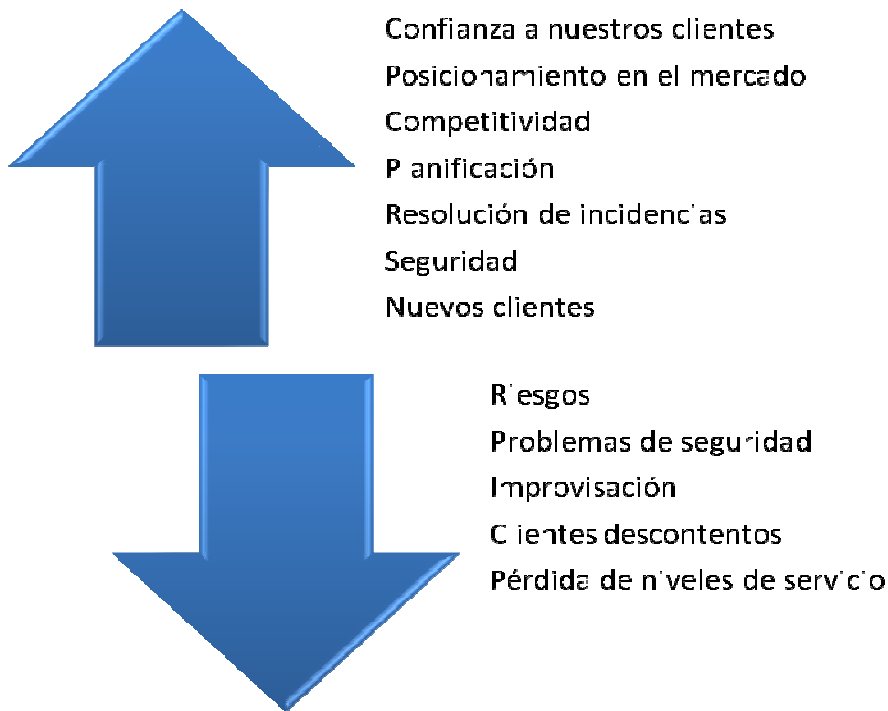
Por dar algunos ejemplos, podemos pensar en la pérdida de productividad ocasionada al no poder prestar servicio (pérdidas diarias), la pérdida de imagen, las pérdidas por no cumplir con acuerdos de nivel de servicio, sanciones económicas al infringir regulaciones legales, etc. Es por esto que un BCP por si solo aporta suficiente retorno de inversión; más aún si lo enmarcamos dentro de un plan de implantación de un SGSI.

- **Mejora continua:** ISO 27001 contempla en su cláusula 8 la mejora continua del sistema, basada en mejorar la eficacia del SGSI implantado y responder a las nuevas necesidades en seguridad de la información que tiene la empresa.

Para enlazar este punto con el cálculo del ROSI podemos pensar que un sistema de seguridad que no se mantenga “vivo” en el tiempo no podrá responder con las garantías oportunas ante las nuevas incidencias de seguridad que podrían afectar a nuestro negocio.

3. Beneficios de implantar ISO 27001

Entre los principales beneficios de implantar ISO 27001 podríamos destacar los siguientes de forma esquemática:



AUMENTO DE INGRESOS GRACIAS A ISO 27001

Para calcular el ROSI de implantar ISO 27001 en nuestra organización es importante tener en cuenta tres factores:

- Coste de la implantación de la norma.
- Ahorro al reducir o eliminar incidentes.
- Beneficios directos al mejorar nuestra imagen de marca y conseguir así nuevos clientes.

Estos tres factores son los que deben hacernos decantarnos de forma positiva para implantar un SGSI en nuestra organización.

LOPD - CONSULTORÍA – AUDITORÍA- FORMACIÓN – ISO 27001- ABOGADOS TIC

4. Caso práctico

Una fórmula sencilla para el cálculo del ROSI podría ser la siguiente:

$$ROSI = [(BENEFICIO - COSTOS) / COSTOS] * 100\%$$

Sin embargo, para un correcto cálculo del retorno de inversión deberían conocerse todos los posibles incidentes que afectan a la organización en cuestión y llevar a cabo el proceso indicado a lo largo de este documento.

CASO PRÁCTICO OBTENIDO EN "ROSI, EL ROI DE LA SEGURIDAD DE LA INFORMACIÓN" por Carlos Ormella Meyer. Abril de 2006. Resumen de resultados:

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	

LOPD - CONSULTORÍA - AUDITORÍA- FORMACIÓN - ISO 27001- ABOGADOS TIC

AUDISEC SEGURIDAD DE LA INFORMACIÓN S.L.

Hilarión Eslava 21 9º A Esc. Izq. 28015 MADRID

CENTRO CÍVICO EMPRESARIAL Vía Principal, S/N, 13200 - Manzanares (CIUDAD REAL)

Tlf: **902 056 203 -926 61 23 10** Fax 926 614 836 www.audisec.es -e-mail: comercial@audisec.es

CASO PRÁCTICO OBTENIDO EN "Calculating Security Return on Investment". Don O'Neill, Software Engineering Institute. Carnegie Mellon University. 2007-02-06.

Savings: = (Resistance Savings + Recognition Savings + Reconstitution Savings)

Cost: = (Total Preparation + Total Cleanup + Total Lost Opportunity + Total Critical Infrastructure Impact)

Where:

Incidents: = 100 [Expected number of incidents]

IR1: Number of expected incidents successfully resisted = 60

IR2: Number of expected incidents successfully recognized = 30

IR3: Number of expected incidents successfully survived = 5

IR4: Number of expected incidents undetected (duds) except for a forensic trace = 5

Resistance Savings

SR1: = IR1 * (Cleanup1 + Lost Opportunity1 + Critical Infrastructure Impact1)

SR1: = 60 * (2,500 + 10,000 + 0) = 750,000

Recognition Savings

SR2: = IR2 * (Cleanup2 + Lost Opportunity2 + Critical Infrastructure Impact2)

SR2: = 30 * (25,000 + 20,000 + 0) = 1,350,000

Reconstitution Savings

SR3: = IR3 * (Cleanup3 + Lost Opportunity3 + Critical Infrastructure Impact3)

SR3: = 5 * (250,000 + 500,000 + 5,000,000) = 28,750,000

Dud Costs

SR4: = IR4 * (Cleanup4)

SR4: = 5 * (250) = 1,250

Preparation

Step 1: = 75,000 [3 days * 50 participants * \$500/day]

Step 2: = 75,000 [5 days * 25 participants * \$600/day]

Step 3: = 250,000 [Resistance and Recognition implementation costs]

Step 4: = 500,000 [Reconstitution implementation costs]

Step 5: = 50,000 [Information disclosure control costs]

Total Preparation: = (Step1 + Step2 + Step3 + Step4 + Step5)

Total Preparation: = (75,000 + 75,000 + 250,000 + 500,000 + 50,000)

Total Preparation: = 950,000

Cleanup Per Incident

Cleanup1: = [2,500/incident]

Cleanup2: = [25,000/incident]

Cleanup3: = [250,000/incident]

Cleanup4: = [250/incident]

Total Cleanup: = (IR1 * Cleanup1) + (IR2 * Cleanup2) + (IR3 * Cleanup3) + (IR4 * Cleanup4)

LOPD - CONSULTORÍA - AUDITORÍA- FORMACIÓN - ISO 27001- ABOGADOS TIC

AUDISEC SEGURIDAD DE LA INFORMACIÓN S.L.

Hilarión Eslava 21 9º A Esc. Izq. 28015 MADRID

CENTRO CÍVICO EMPRESARIAL Vía Principal, S/N, 13200 - Manzanares (CIUDAD REAL)

Tlf: **902 056 203 -926 61 23 10** Fax 926 614 836 www.audisec.es -e-mail: comercial@audisec.es

Total Cleanup: = (60 * 2,500) + (30 * 25,000) + (5* 250,000) + (5 * 250) = 150,000 + 750,000 + 1,250,000 + 1,250

Total Cleanup: = 2,151,250

Lost Opportunity Per Incident

Lost Opportunity1:= 0.1 day * 10,000/day: = 10,000

Lost Opportunity2:= 0.2 days * 10,000/day: = 20,000

Lost Opportunity3:= 5 days * 100,000/day:= 500,000

Total Lost Opportunity: = (IR1 * Lost Opportunity1) + (IR2 * Lost Opportunity2) + (IR3 * Lost Opportunity3)

Total Lost Opportunity: = (60 * 10,000) + (30 * 20,000) + (5 * 500,000)

Total Opportunity: = 600,000 + 600,000 + 2,500,000

Total Lost Opportunity: = 3,700,000

Critical Infrastructure Impact Per Incident

Critical Infrastructure Impact1:= 0 * 1,000,000:= 0

Critical Infrastructure Impact2:= 0 * 1,000,000:= 0

Critical Infrastructure Impact3:= 5 * 1,000,000:= 5,000,000

Total Critical Infrastructure Impact: = (60 * 0) + (30 * 0) + (5* 5,000,000): = 25,000,000

Savings: = (Resistance Savings + Recognition Savings + Reconstitution Savings)

Cost: = (Total Preparation + Total Cleanup + Total Lost Opportunity + Total Critical Infrastructure Impact)

Savings: = 750,000 + 1,350,000 + 28,750,000) = 30,850,000

Cost: = (950,000 + 2,151,250 + 3,700,000 + 25,000,000) = 31,801,250

ROI: = Savings/Cost

ROI: = 30,850,000/31,801,250

ROI: = 0.97008765379

5. Observaciones

Como se ha dicho antes, este tipo de estudios no es posible realizarlo sin conocer de forma exhaustiva las amenazas que afectan a una organización.

Para realizarlo de la forma más precisa posible (siempre son estimaciones probabilísticas) debemos remontarnos a la historia reciente de la organización y ver qué incidentes se han sufrido, para así poder prever los posibles incidentes futuros.

Una vez estimadas las posibles incidencias debemos calcular el coste asociado a ellas y ver en qué grado ISO 27001 nos permite reducir el impacto económico de las mismas.

Respecto a la posibilidad de sufrir una catástrofe de gran tamaño (incendios, terremotos, etc.) ISO 27001 cubre la incidencia con la elaboración y puesta en marcha de un plan de continuidad.