ANALISIS DE RIESGOS EN SISTEMAS

Unidad 4: Proceso de gestión de riesgos I

Objetivo específico 4: El alumno aprenderá como evaluar e interpretar los valores de impacto y riesgo residual, como debe de aceptar el riesgo su tratamiento y el estudio cuantitativo y cualitativo de los costes y las diferentes opciones de tratamiento del riesgo.

Conceptos a desarrollar en la unidad: Conceptos, Evaluación: interpretación de los valores de impacto y riesgo residuales, Aceptación del riesgo, Tratamiento, Estudio cuantitativo de costes / beneficios, Estudio cualitativo de costes / beneficios, Estudio mixto de costes / beneficios, Opciones de tratamiento del riesgo: eliminación, Opciones de tratamiento del riesgo: mitigación, Opciones de tratamiento del riesgo: compartición y Opciones de tratamiento del riesgo: financiación

Introducción

A la vista de los impactos y riesgos a que está expuesto el sistema, hay que tomar una serie de decisiones condicionadas por diversos factores:

- la gravedad del impacto y/o del riesgo
- las obligaciones a las que por ley esté sometida la Organización
- las obligaciones a las que por reglamentos sectoriales esté sometida la Organización
- las obligaciones a las que por contrato esté sometida la Organización

Dentro del margen de maniobra que permita este marco, pueden aparecer consideraciones adicionales sobre la capacidad de la Organización para aceptar ciertos impactos de naturaleza intangible tales como:

- imagen pública de cara a la Sociedad (aspectos reputacionales)
- política interna: relaciones con los propios empleados, tales como capacidad de contratar al personal idóneo, capacidad de retener a los mejores, capacidad de soportar rotaciones de personas, capacidad de ofrecer una carrera profesional atractiva, etc.
- relaciones con los proveedores, tales como capacidad de llegar a acuerdos ventajosos a corto, medio o largo plazo, capacidad de obtener trato prioritario, etc.
- relaciones con los clientes o usuarios, tales como capacidad de retención, capacidad de incrementar la oferta, capacidad de diferenciarse frente a la competencia, ...
- relaciones con otras organizaciones, tales como capacidad de alcanzar acuerdos estratégicos, alianzas, etc.
- nuevas oportunidades de negocio, tales como formas de recuperar la inversión en seguridad
- acceso a sellos o calificaciones reconocidas de seguridad

Todas las consideraciones anteriores desembocan en una calificación de cada riesgo significativo, determinándose si ...

1. es **crítico** en el sentido de que requiere atención urgente
2. es **grave** en el sentido de que requiere atención
3. es **apreciable** en el sentido de que pueda ser objeto de estudio para su tratamiento
4. es **asumible** en el sentido de que no se van a tomar acciones para atajarlo

La opción 4, aceptación del riesgo, siempre es arriesgada y hay que tomarla con prudencia y justificación. Las razones que pueden llevar a esta aceptación son:

- cuando el impacto residual es asumible
- cuando el riesgo residual es asumible

- cuando el coste de las salvaguardas oportunas es desproporcionado en comparación al impacto y riesgo residuales

La calificación de los riesgos tendrá consecuencias en las tareas subsiguientes, siendo un factor básico para establecer la prioridad relativa de las diferentes actuaciones.

4.1 Conceptos

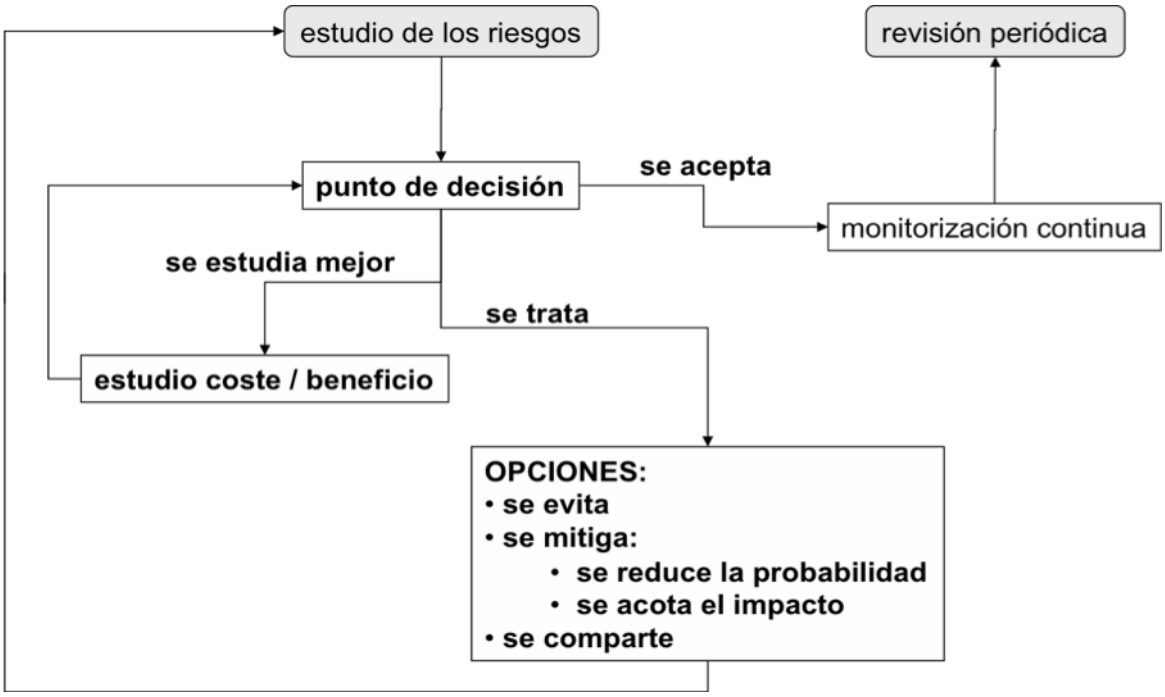
El análisis de riesgos determina impactos y riesgos. Los impactos recogen daños absolutos, independientemente de que sea más o menos probable que se dé la circunstancia. En cambio, el riesgo pondera la probabilidad de que ocurra. El impacto refleja el daño posible (lo peor que puede ocurrir), mientras que el riesgo refleja el daño probable (lo que probablemente ocurra).

El resultado del análisis es sólo un análisis. A partir de el disponemos de información para tomar decisiones conociendo lo que queremos proteger (activos valorados=, de qué lo queremos proteger (amenazas valoradas) y qué hemos hecho por protegerlo (salvaguardas valoradas). Todo ello sintetizado en los valores de impacto y riesgo.

A partir de aquí, las decisiones son de los órganos de gobierno de la Organización que actuarán en 2 pasos:

- paso 1: evaluación
- paso 2: tratamiento

La siguiente figura resume las posibles decisiones que se pueden tomar tras haber estudiado los riesgos. La caja 'estudio de los riesgos' pretende combinar el análisis con la evaluación.



Decisiones de tratamiento de los riesgos

Todos estos aspectos se desarrollan en las secciones siguientes.

4.1.1 Evaluación: interpretación de los valores de impacto y riesgo residuales

Impacto y riesgo residual son una medida del estado presente, entre la inseguridad potencial (sin salvaguarda alguna) y las medidas adecuadas que reducen impacto y riesgo a valores aceptables.

Los párrafos siguientes se refieren conjuntamente a impacto y riesgo.

Si el valor residual es igual al valor potencial, las salvaguardas existentes no valen para nada, típicamente no porque no haya nada hecho, sino porque hay elementos fundamentales sin hacer.

Es importante entender que un valor residual es sólo un número. Para su correcta interpretación debe venir acompañado de la relación de lo que se debería hacer y no se ha hecho; es decir, de las vulnerabilidades que presenta el sistema. Los responsables de la toma de decisiones deberán prestar cuidadosa atención a esta relación de tareas pendientes, que se denomina **Informe de Insuficiencias o de vulnerabilidades**.

4.1.2 Aceptación del riesgo

La Dirección de la Organización sometida al análisis de riesgos debe determinar el nivel de impacto y riesgo aceptable. Más propiamente dicho, debe aceptar la responsabilidad de las insuficiencias. Esta decisión no es técnica. Puede ser una decisión política o gerencial o puede venir determinada por ley o por compromisos contractuales con proveedores o usuarios. Estos niveles de aceptación se pueden establecer por activo o por agregación de activos (en un determinado departamento, en un determinado servicio, en una determinada dimensión, ...)

Cualquier nivel de impacto y/o riesgo es aceptable si lo conoce y acepta formalmente la Dirección —

4.1.3 Tratamiento

La Dirección puede decidir aplicar algún tratamiento al sistema de seguridad desplegado para proteger el sistema de información. Hay dos grandes opciones:

- reducir el riesgo residual (aceptar un menor riesgo)
- ampliar el riesgo residual (aceptar un mayor riesgo)

Para tomar una u otra decisión hay que enmarcar los riesgos soportados por el sistema de información dentro de un contexto más amplio que cubre un amplio espectro de consideraciones de las que podemos apuntar algunas sin pretender ser exhaustivos:

- cumplimiento de obligaciones; sean legales, regulación pública o sectorial, compromisos internos, misión de la Organización, responsabilidad corporativa, etc.
- posibles beneficios derivados de una actividad que en sí entraña riesgos
- condicionantes técnicos, económicos, culturales, políticos, etc.
- equilibrio con otros tipos de riesgos: comerciales, financieros, regulatorios, medioambientales, laborales, …

En condiciones de **riesgo residual extremo**, casi la única opción es reducir el riesgo.

En condiciones de **riesgo residual aceptable** , podemos optar entre aceptar el nivel actual o ampliar el riesgo asumido. En cualquier caso hay que mantener una monitorización continua de las circunstancias para que el riesgo formal cuadre con la experiencia real y reaccionemos ante cualquier desviación significativa.

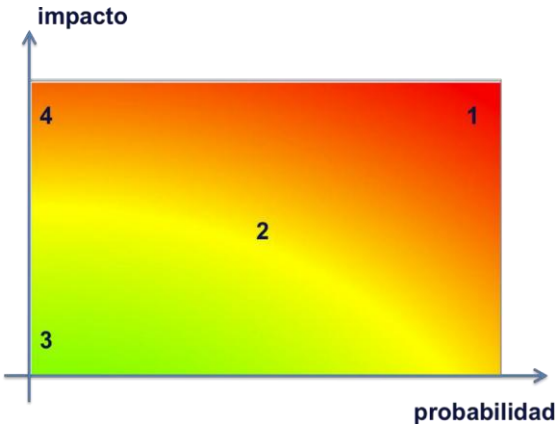


Ilustración 12. Zonas de riesgo

En condiciones de **riesgo residual medio**, podemos observar otras características como las pérdidas y ganancias que pueden verse afectadas por el escenario presente, o incluso analizar el estado del sector en el que operamos para compararnos con la "norma".

En términos de las zonas de riesgo que se expusieron anteriormente,

- zona 1 – riesgos muy probables y de muy alto impacto; posiblemente nos planteemos sacarlos de esta zona
- zona 2 – riesgos de probabilidad relativa e impacto medio; se pueden tomar varias opciones
- zona 3 – riesgos improbables y de bajo impacto; o los dejamos como están, o permitimos que suban a mayores si ello nos ofreciera alguna ventaja o beneficio en otro terreno
- zona 4 – riesgos improbables pero de muy alto impacto; suponen un reto de decisión pues su improbabilidad no justifica que se tomen medidas preventivas, pero su elevado impacto exige que tengamos algo previsto para reaccionar; es decir, hay que poner el énfasis en medidas de reacción para limitar el daño y de recuperación del desastre si ocurriera.

También conviene considerar la incertidumbre del análisis. Hay veces que sospechamos las consecuencias, pero hay un amplio rango de opiniones sobre su magnitud (incertidumbre en el impacto). En otras ocasiones la incertidumbre afecta a la probabilidad. Estos escenarios suelen afectar a las zonas 4 y 3, pues cuando la probabilidad es alta, normalmente adquirimos experiencia, propia o ajena, con rapidez y salimos de la incertidumbre. En cualquier caso, toda incertidumbre debe considerarse como mala y debemos hacer algo:

- buscar formas de mejorar la previsión, típicamente indagando en foros, centros de respuesta a incidentes o expertos en la materia;
- evitar el riesgo cambiando algún aspecto, componente o arquitectura del sistema; o
- tener preparados sistemas de alerta temprana y procedimientos flexibles de contención, limitación y recuperación del posible incidente.

A veces que estos escenarios de incertidumbre ocurren en un terreno en el que hay obligaciones de cumplimiento y la propia normativa elimina o reduce notablemente las opciones disponibles; es decir, el sistema se protege por obligación más que por certidumbre del riesgo.

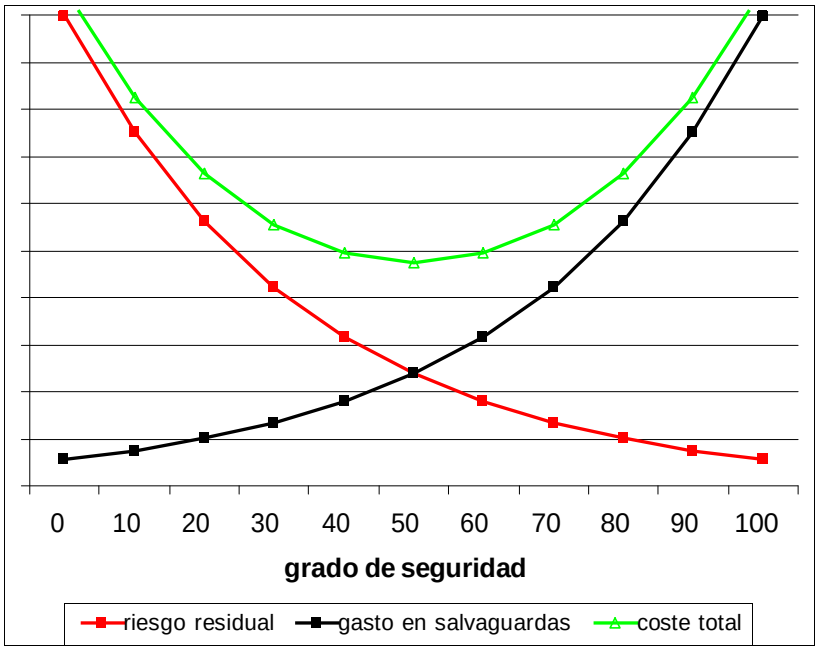
A la vista de estas consideraciones se tomarán las decisiones de tratamiento.

4.1.4 Estudio cuantitativo de costes / beneficios

Es de sentido común que no se puede invertir en salvaguardas más allá del valor que queremos proteger.

Aparecen en la práctica gráficos como el siguiente que ponen uno frente al otro el coste de la inseguridad (lo que costaría no estar protegidos) y el coste de las salvaguardas.

Este tipo de gráficas intentan reflejar cómo al avanzar de un grado de seguridad 0 hacia un grado de seguridad del 100%, el coste de la inseguridad (el riesgo) disminuye, mientras que el coste de la inversión en salvaguardas aumenta. Es intencionado el hecho de que el riesgo caiga fuertemente con pequeñas inversiones[18] y que el coste de las inversiones se dispare para alcanzar niveles de seguridad cercanos al 100%[19]. La curva central suma el coste para la Organización, bien derivado del riesgo (baja seguridad), bien derivado de la inversión en protección. De alguna forma existe un punto de equilibrio entre lo que se arriesga y lo que se invierte en defensa, punto al que hay que tender si la única consideración es económica.



Relación entre el gasto en seguridad y el riesgo residual

Pero llevar el sentido común a la práctica no es evidente, ni por la parte del cálculo del riesgo, ni por la parte del cálculo del coste de las salvaguardas. En otras palabras, la curva anterior es conceptual y no se puede dibujar en un caso real.

En la práctica, cuando hay que protegerse de un riesgo que se considera significativo, aparecen varios escenarios hipotéticos:

E0: si no se hace nada

E1: si se aplica un cierto conjunto de salvaguardas

E2: si se aplica otro conjunto de salvaguardas

Y así N escenarios con diferentes combinaciones de salvaguardas.

El análisis económico tendrá como misión decidir entre estas opciones, siendo E0 (seguir como estamos) una opción posible, que pudiera estar justificada económicamente.

En cada escenario hay que estimar a lo largo del tiempo el coste que va a suponer. Para poder agregar costes, se contabilizan como valores negativos las pérdidas de dinero y como valores positivos las entradas de dinero. Considerando los siguientes componentes:

– (recurrente) riesgo residual

– (una vez) coste de las salvaguardas

– (recurrente) coste anual de mantenimiento de las salvaguardas

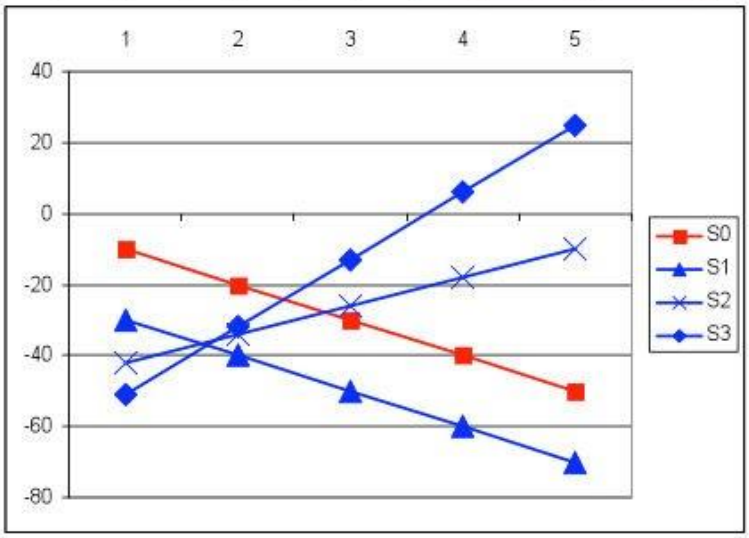
\+ (recurrente) mejora en la productividad[22]

\+ (recurrente) mejoras en la capacidad de la Organización para prestar nuevos servicios, conseguir mejores condiciones de los proveedores, entrar en asociación con otras organizaciones, etc.

El escenario E0 es muy simple: todos los años se afronta un gasto marcado por el riesgo, que se acumula año tras año.

En los demás escenarios, hay cosas que suman y cosas que restan, pudiendo darse varias situaciones como las recogidas en la gráfica siguiente. Se presentan valores acumulados a lo largo de un periodo de 5 años. La pendiente de la recta responde a los costes recurrentes. El valor el primer año corresponde a los costes de implantación.

						año				
	riesgo (anual)	coste (inicial)	coste (anual)	mejora (anual)	otros (anual)	1	2	3	4	5
E0	10	0	0	0	0	-10	-20	-30	-40	-50
E1	5	20	5	0	0	-30	-40	-50	-60	-70
E2	2	50	10	20	0	-42	-34	-26	-18	-10
E3	1	70	15	35	0	-51	-32	-13	6	25



Ejemplos de decisiones de tratamiento del riesgo

- En E0 se sabe lo que cada año (se estima que) se pierde
- El escenario E1 aparece como mala idea, pues supone un gasto añadido el primer año; pero este gasto no se recupera en años venideros.
- No así el escenario E2 que, suponiendo un mayor desembolso inicial, empieza a ser rentable a partir del cuarto año.
- Más atractivo aún es el escenario E3 en el que a costa de un mayor desembolso inicial, se empieza a ahorrar al tercer año, e incluso se llega a obtener beneficios operativos a partir del quinto año. Se puede decir que en escenario E3 se ha hecho una buena inversión.

4.1.4 Estudio cualitativo de costes / beneficios

Cuando el análisis es cualitativo, en la balanza de costes beneficios aparecen aspectos intangibles que impiden el cálculo de un punto numérico de equilibrio.

Entre los aspectos intangibles se suelen contemplar:

— aspectos reputacionales o de imagen

— aspectos de competencia: comparación con otras organizaciones de mismo ámbito de actividad

— cumplimiento normativo, que puede ser obligatorio o voluntario

— capacidad de operar

— productividad

Estas consideraciones nos llevan a contemplar diversos escenarios para determinar el balance neto. Por ejemplo, el no adoptar medidas puede exponernos a un cierto riesgo que causaría mala imagen; pero si la solución preventiva causa también mala imagen o supone un merma notable de oportunidades o de productividad, hay que buscar un punto de equilibrio, eligiendo una combinación de medidas que sea asumible.

4.1.6 Estudio mixto de costes / beneficios

En análisis de riesgos meramente cualitativos, la decisión la marca el balance de costes y

beneficios intangibles, si bien siempre hay que hacer un cálculo de lo que cuesta la solución y cerciorarse de que el gasto es asumible. De lo contrario, la supuesta solución no es una opción. Es decir, primero hay que pasar el filtro económico y luego elegir la mejor de las soluciones factibles.

4.1.7 Opciones de tratamiento del riesgo: eliminación

La eliminación de la fuente de riesgo es una opción frente a un riesgo que no es aceptable.

En un sistema podemos eliminar varias cosas, siempre que no afecten a la esencia de la Organización. Es extremadamente raro que podamos prescindir de la información o los servicios esenciales por cuanto constituyen la misión de la Organización. Cambiar estos activos supone reorientar la misión de la Organización.

Más viable es prescindir de otros componentes no esenciales, que están presentes simple y llanamente para implementar la misión, pero no son parte constituyente de la misma. Esta opción puede tomar diferentes formas:

- Eliminar cierto tipo de activos, emplean otros en su lugar. Por ejemplo: cambiar de sistema operativo, de fabricante de equipos, …
- Reordenar la arquitectura del sistema (el esquema de dependencias en nuestra terminología) de forma que alteremos el valor acumulado en ciertos activos expuestos a grandes amenazas. Por ejemplo: segregar redes, desdoblar equipos para atender a necesidades concretas, alejando lo más valioso de lo más expuesto, …

Las decisiones de eliminación de las fuentes de riesgo suponen realizar un nuevo análisis de riesgos sobre el sistema modificado.

4.1.8 Opciones de tratamiento del riesgo: mitigación

La mitigación del riesgo se refiere a una de dos opciones:

- reducir la degradación causada por una amenaza (a veces se usa la expresión ‘acotar el impacto’)
- reducir la probabilidad de que una amenaza de materializa

En ambos casos lo que hay que hacer es ampliar o mejorar el conjunto de salvaguardas. En términos de madurez de las salvaguardas: subir de nivel.

Algunas salvaguardas, notablemente las de tipo técnico, se traducen en el despliegue de más equipamiento[24] que se convierte a su vez en un activo del sistema. Estos nuevos activos también acumularán valor del sistema y estarán a su vez sujetos a amenazas que pueden perjudicar a los activos esenciales.

Hay pues que repetir el análisis de riesgos, ampliándolo con el nuevo despliegue de medios y, por supuesto, cerciorarse de que el riesgo del sistema ampliado es menor que el del sistema original; es decir, que las salvaguardas efectivamente disminuyen el estado de riesgo de la Organización.

4.1.9 Opciones de tratamiento del riesgo: compartición

Tradicionalmente se ha hablado de ‘transferir el riesgo’. Como la transferencia puede ser parcial o total, es más general hablar de ‘compartir el riesgo’.

Hay dos formas básicas de compartir riesgo:

- Riesgo cualitativo: se comparte por medio de la externalización de componentes del sistema, de forma que se reparten responsabilidades: unas técnicas para el que opera el componente técnico; y otras legales según el acuerdo que se establezca de prestación del servicio.
- Riesgo cuantitativo: se comparte por medio de la contratación de seguros, de forma que a cambio de una prima, el tomador reduce el impacto de las posibles amenazas y el asegurador corre con las consecuencias. Hay multitud de tipos y cláusulas de seguros para concretar el grado de responsabilidad de cada una de las partes.

Cuando se comparten riesgos cambia, bien el conjunto de componentes del sistema, bien su

valoración, requiriéndose un nuevo análisis del sistema resultante.

4.1.10 Opciones de tratamiento del riesgo: financiación

Cuando se acepta un riesgo, la Organización hará bien en reservar fondos para el caso de que el riesgo se concrete y haya que responder de sus consecuencias. A veces de habla de ‘fondos de contingencia’ y también puede ser parte de los contratos de aseguramiento.

Normalmente esta opción no modifica nada del sistema y nos vale el análisis de riesgos disponible.