Riesgos Residuales

Jaime Enrique Reyes Castro, Luis Orlando Porras garzón
jreyesc83@gmail.com, loporras.82@gmail.com
Diplomado en Gestión de Seguridad y Riesgo, Universidad Piloto de Colombia
Bogotá, Colombia

Resumen – El análisis de riesgos nos proporciona datos importantes sobre el diseño de las actividades de nuestra empresa, sus impactos según las amenazas y consecuentemente mitigar o evitar dichos niveles de riesgos. En la determinación del riesgo o su probabilidad de ocurrencia, los riesgos residuales nos ayudan para decidir ya sea controles adicionales o ajustes sobre controles ya establecidos.

Palabras Claves—Activos, Amenazas, Impacto, Riesgos, Riesgos Residual, SGSI.

Abstract – Risk analysis provides important information about the design of the activities of our company, its impacts as a result of threats and mitigate or avoid such risk levels. In determining the risk or probability of occurrence, the residual risks help us to decide whether additional controls or adjustments established controls.

I. INTRODUCCIÓN

Como ingenieros especialistas en seguridad de la información, es nuestro deber mantener y garantizar disponibilidad, confidencialidad e integridad la información. Actualmente las empresas no aplican soluciones relacionadas que cobijen estos tres conceptos fundamentales; si las aplican, no son las adecuadas según la filosofía u objetivo del core del negocio o bien se excluyen muchas de éstas soluciones enmarcándolas como un gasto y no como una inversión que puede reflejarse a corto, mediano o largo plazo. Con los métodos actuales es posible realizar un análisis de riesgos bien definido y estructurado en nuestras empresas teniendo en cuenta lo siguiente [1]:

- **Activos**: Lo que se debe proteger.
- **Amenazas**: El peligro sobre lo que se va a proteger.
- **Riesgo**: Corresponde a la probabilidad de materialización de las amenazas.
- **Riesgo residual**: Corresponde al grado de incertidumbre que la organización está dispuesta a asumir.
- **Impacto:** Costo para la organización si los peligros son materializados y afectan lo que se va a proteger.

II. EL RIESGO RESIDUAL

El Riesgo Residual es el nivel de riesgo existente después de la implantación de medidas de seguridad [2], es decir, que a pesar de tener información del riesgo, conocer sus peligros y tomar medidas de seguridad para ello, aún existe la exposición a dicho riesgo o peligro el cual se deberá asumir y obviamente vigilar. Otra definición que se puede encontrar según la NTC 5254 es el "nivel resultante de riesgo después de que se han tomado medidas de tratamiento del riesgo" [3]. Según la ISO 2001 Cláusula 4.2.1.h / I: "Obtener la aprobación de la dirección de la organización para el riesgo residual propuesto y para implementar y mantener el SGSI" Según ello, la dirección de una organización deberá aceptar el riesgo residual y deberá ser tenido en cuenta si llegase a existir un incidente de seguridad. Por lo tanto uno o más controles pueden ser escogidos para mitigar este riesgo [5].

Muchas veces las contramedidas no siempre tienen el mismo impacto como se puede esperar. Aun cuando son implementadas correctamente, las amenazas nunca serán eliminadas totalmente. No

existe un ambiente de seguridad perfecta por lo tanto no existe el riesgo cero; no hay forma de saber si las amenazas se han evadido a su totalidad. Se puede estimar que tan cerca se está de dicho riesgo cero. Por lo tanto, aún cuando estos problemas son evidentes (amenazas) y se tiene sus contramedidas y que pueden ser entendidas, la mejor que se puede hacer en un proceso de gestión del riesgo es su medición.

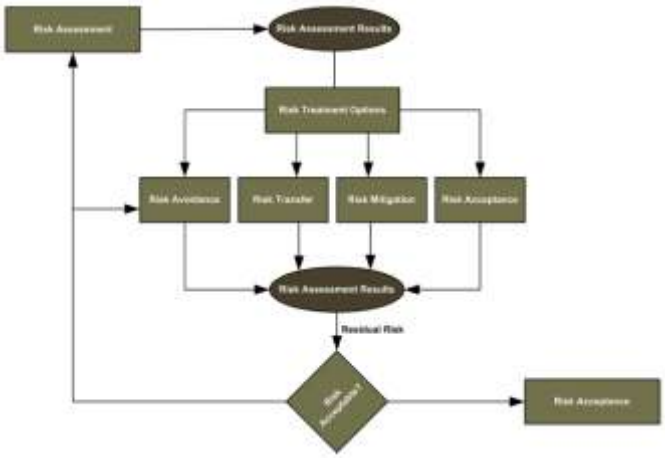


Figura 1. Riesgo Residual que permanece después de la evaluación del riesgo

Inicialmente se tiene que modelar la situación actual como también una situación en donde las contramedidas a las vulnerabilidades y amenazas se tomen para minimizar el riesgo residual de una organización.

III. VALORACION Y OBTENCION DEL RIESGO RESIDUAL

El riesgo residual proviene de la relación entre el grado de los riesgos inherentes y la gestión de la mitigación de riesgos. [4]. Para obtener este cálculo, primero se debe tener claro que es un riesgo inherente. Un riesgo inherente se puede definir como factor de riesgo, es decir, que una vez se establecen todas las actividades se identifican los factores que intervienen en su manifestación y severidad.

Luego de tener estas medidas se procede en determinar la probabilidad de que el riesgo ocurra y su respectivo cálculo de sus efectos. Estas dos variables se pueden calcular cuantitativamente o cualitativamente y pueden también complementarse una con la otra al momento de calcular la probabilidad del riesgo. La valorización del riesgo se puede calcular realizándola en función de la probabilidad e impacto. El rango y la escala numérica son definidas a criterio propio.

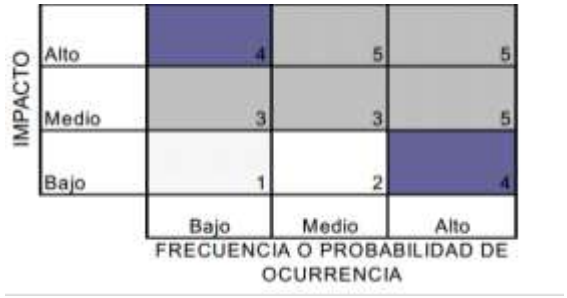


Figura 2. Ejemplo de Valoración de Impacto vs Riesgo

Una vez se realice la anterior valorización se realiza una valoración de los controles tomados en la empresa para mitigar los riesgos identificados. Entre más sea eficiente un control y la gestión de mitigación del riesgo, el riesgo inherente tiende a disminuir.

Por último se obtiene el riesgo residual que es el cálculo entre el grado de nivel del riesgo inherentes sobre la gestión de mitigación del riesgo. De acuerdo al análisis y determinación del riesgo residual se pueden tomar decisiones sobre seguir o dejar dicha actividad dependiendo su nivel de riesgo o implementar o fortalecer los controles ya existentes.

Actividad I	Nivel de riesgo	Calidad de gestión			Riesgo residual (**)
		Tipo de medidas de control	Efectividad	Promedio (*)	
Riesgo inherente 1	5	Control 1	3	3.6	1.38
		Control 2	4		
		Control 3	4		
Riesgo inherente 2	4	Control 1	5	4.25	0.94
		Control 2	5		
		Control 3	4		
Riesgo inherente 3	4	Control 1	3	3.6	1.11
		Control 2	4		
		Control 3	4		
Riesgo inherente 4	3	Control 1	5	3.5	0.85
		Control 2	2		
Perfil de riesgo (Riesgo residual total) (***)					1.07

Figura 3. Ejemplo de medición de Riesgo Residual en una empresa

Por lo tanto cuanto más alto sea el número, mayor será el riesgo. Estos datos serán de gran utilidad al momento de decidir prioridades en las acciones a tomar. Generalmente estos riesgos altos necesitan de recursos adicionales considerables y pueden indicarnos también la adecuación de métodos de control más efectivos de los inicialmente planteados. Según el resultado y la escala tomada se pueden considerar los riesgos residuales como [2]:

- Poco Probable: En este caso no requerirá mayores mejoras y los controles actuales se mantendrían.
- Riesgo controlado adecuadamente: Es tolerable cuando se implementan las respectivas medidas de control identificadas.
- Riesgo controlado moderadamente: Se deben tomar medidas o controles mayores para reducir el riesgo.
- Riesgo inaceptable: Son los riesgos no controlados adecuadamente y se deben implementar mayores controles.

Una vez identificados los riesgos residuales se pueden tomar acciones como [6]:

- Controlar el riesgo: Fortalecer o implementar nuevos controles
- Eliminar el riesgo: Se elimina el activo y por consiguiente se elimina el riesgo
- Compartir el riesgo: Mediante acuerdos se traspasa una parte o totalidad del riesgo a un tercero.
- Aceptar el riesgo: Indicar que el nivel de exposición es el adecuado

Figura 4. Ciclo donde se encuentra el Riesgo Residual

Finalmente estos riesgos residuales deben ser valorados aplicando los criterios definidos en el plan de riesgos y deben documentarse en la gestión de los riesgos.

A. Tratamiento para minimizar el riesgo residual

La administración en el manejo del riesgo no sólo es cuestión de tener buenas prácticas. Es posible que más riesgos estén presentes que los riesgos aceptables y deberán ser escogidas contramedidas adicionales para llevar el riesgo a un nivel aceptable. Entonces es necesario de un método que proporciona un control adicional y tenga una noción más detallada en el riesgo residual de una empresa u

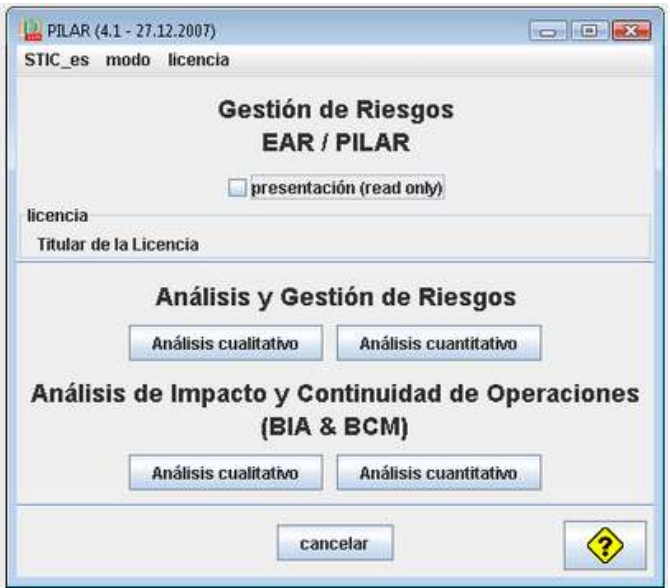
organización. Por lo tanto cabe preguntarse como que procedimientos o métodos son útiles y prácticos para una medición cuantitativa o cualitativa de los riesgos iniciales para que los riesgos residuales sean mínimos.

Sea cual sea el método a seleccionar, la selección más apropiada debe incluir un equilibrio del costo de la implementación de cada opción versus los beneficios derivados de ella. Existen los siguientes métodos para la identificación de riesgos [3]:

- Métodos cualitativos: No tienen cálculos numéricos.
- Métodos semicualitativos: Tienen valores cuantitativos respecto a la frecuencia de ocurrencia de un suceso.
- Métodos comparativos: Utilizan técnicas a partir de experiencias existentes o análisis de sucesos que ocurrieron.

El tratamiento del riesgo identifica las diversas opciones para tratar el riesgo, evaluar dichas opciones, preparación de planes para el tratamiento del riesgo y su respectiva implementación. Pero si después del tratamiento existe este tipo de riesgo residual, se debe tomar una decisión de retenerlo o repetir su proceso de tratamiento. [3]

IV. HERRAMIENTAS PARA EL RIESGO RESIDUAL



Ri

Actualmente existe una herramienta llamada PILAR que realiza una estimación del riesgo residual teniendo en cuenta la madurez de las medidas relevantes para un sistema [7]. Esta herramienta se puede utilizar en entorno Windows o Unix según los requisitos de sistema indicados en la página web al momento de descargarlo.

Figura 5. Menú Inicio de la herramienta PILAR

V. CONCLUSIONES

- Se debe escoger el respectivo método que ayude a la evaluación de la organización (método cualitativo, métodos semicualitativo o método comparativo) y que este método permita un conocimiento a nivel interno de la organización para así tener una mitigación del riesgo de forma proactiva. Todos los métodos posibles deben ser validados o verificados con el fin de proteger el recurso más importante como lo es la información
- Como se mencionó el resigo cero nunca existirá. Por lo tanto se debe revisar los métodos o las ponderaciones que se toman al momento de realizar un cálculo de los riesgos inherentes y los controles para posteriormente minimizar los cálculos en los riesgos residuales.
- La generación de los modelos de riesgos deben estar de acuerdo con el core del negocio y entendiendo bien a que se dedica el negocio.
- Entre mejor sea el control y el riesgo inherente sea menor, el cálculo del riesgo residual será mucho menor. Esto nos quiere decir que son directamente proporcionales.

REFERENCIAS

[1] Dante, (2008) *Análisis de Riesgos*. [En línea]. Disponible en: http://danteslab.blogspot.com/2008/08/anlisis-de-riesgos.html

[2] Lic. Javier A. Da Cunha , (2011) *Seguridad I* [En línea]. Disponible en: http://es.scribd.com/javier_cunha_1/d/68555252/27-Riesgo-Residual

[3] Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC) *Norma NTC 5254*, Tratamiento del Riesgo, pp. 3,17,19, Mayo 2004.

[4] SIGWEB, (2010) *Matriz de Riesgo, Evaluación y Gestión de Riesgos*, [En línea]. Disponible en: http://www.sigweb.cl/biblioteca/MatrizdeRiesgo.pdf

[5] Nextel S.A. , (2011) *Gestión de Riesgos en ISO 27001Experiencia práctica en la implantación y gestión en Nextel S.A.* [En línea]. Disponible en: http://www.nexusasesores.com/docs/ISO%2027001-gestion-de-riesgos.pdf

[6] S. Leonardo, (2004) *Introducción a Riesgo Informático*, [En línea]. Disponible en: http://www.ccee.edu.uy/ensenian/catcomp/material/riesgo.pdf

[7] EAR / PILAR (2011) *Entorno de Análisis de Riesgos* [En línea]. Disponible en: https://www.ccn-cert.cni.es/publico/herramientas/pilar43/tools/index.html