Anexo III

Análisis y Gestión de Riesgos en un Sistema Informático

Álvaro Gómez Vieites

CONTENIDO

ANEXO III

ANÁLISIS Y GESTIÓN DE RIESGOS EN UN SISTEMA INFORMÁTICO

Un proceso de gestión de riesgos comprende una etapa de evaluación previa de los riesgos del sistema informático, que se debe realizar con rigor y objetividad para que cumpla su función con garantías. Para ello, el equipo responsable de la evaluación debe contar con un nivel adecuado de formación y experiencia previa, así como disponer de una serie de recursos y medios para poder realizar su trabajo, contando en la medida de lo posible con el apoyo y compromiso de la Alta Dirección.

En el proceso propiamente dicho de gestión de riesgos se trata de definir un plan para la implantación de ciertas salvaguardas o contramedidas en el sistema informático, que permitan disminuir la probabilidad de que se materialice una amenaza, o bien reducir la vulnerabilidad del sistema o el posible impacto en la organización, así como permitir la recuperación del sistema o la transferencia del problema a un tercero (mediante la contratación de un seguro, por ejemplo).

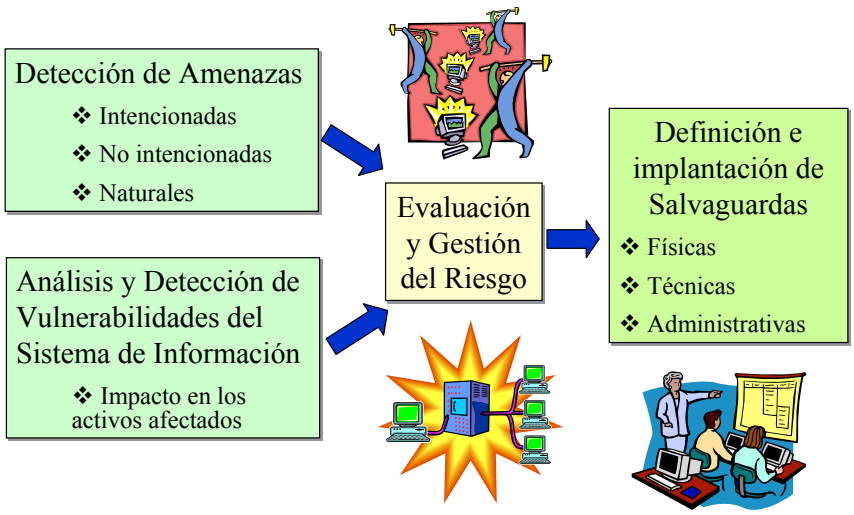

Figura 1: Análisis y Gestión de Riesgos en una organización

Seguidamente se presentan los principales conceptos y definiciones que es necesario manejar a la hora de estudiar el análisis y la gestión de riesgos en una organización:

RECURSOS DEL SISTEMA

Los **recursos** son los activos a proteger del sistema informático de la organización.

Seguidamente se presenta una relación de los principales recursos que se deberían tener en consideración a la hora de analizar y gestionar los riesgos:

- Recursos hardware: servidores y estaciones de trabajo, ordenadores portátiles, impresoras, escáneres y otros periféricos.
- Recursos software: sistemas operativos, herramientas ofimáticas, software de gestión, herramientas de programación, aplicaciones desarrolladas a medida, etc.
- Elementos de comunicaciones: dispositivos de conectividad (*hubs*, *switches*, *routers*), armarios con paneles de conexión, cableado, puntos de acceso a la red, líneas de comunicación con el exterior, etc.
- Información que se almacena, procesa y distribuye a través del sistema (activo de naturaleza intangible).
- Locales y oficinas donde se ubican los recursos físicos y desde los que acceden al sistema los usuarios finales.

- Personas que utilizan y se benefician directa o indirectamente del funcionamiento del sistema.

- Imagen y reputación de la organización.

Cada recurso o activo de la organización se podría caracterizar por un código, su descripción, su coste o precio de adquisición, su coste de reposición, su nivel de criticidad o importancia para el mantenimiento de las actividades de la organización, el nivel requerido de integridad y de confidencialidad, etc.

AMENAZAS

Se considera una **amenaza** a cualquier evento accidental o intencionado que pueda ocasionar algún daño en el sistema informático, provocando pérdidas materiales, financieras o de otro tipo a la organización.

Se puede establecer la siguiente clasificación a la hora de estudiar las amenazas a la seguridad:

- Amenazas naturales: inundación, incendio, tormenta, fallo eléctrico, explosión, etc.

- Amenazas de agentes externos: virus informáticos, ataques de una organización criminal, sabotajes terroristas, disturbios y conflictos sociales, intrusos en la red, robos, estafas, etc.

- Amenazas de agentes internos: empleados descuidados con una formación inadecuada o descontentos, errores en la utilización de las herramientas y recursos del sistema, etc.

También podríamos definir una clasificación alternativa, teniendo en cuenta el grado de intencionalidad de la amenaza:

- Accidentes: averías del hardware y fallos del software, incendio, inundación, etc.

- Errores: errores de utilización, de explotación, de ejecución de determinados procedimientos, etc.

- Actuaciones malintencionadas: robos, fraudes, sabotajes, intentos de intrusión, etc.

La organización puede emplear una escala cuantitativa o cualitativa para definir distintos niveles para la ocurrencia de una amenaza (es decir, en función de su frecuencia): Muy baja, Baja, Media, Alta y Muy Alta.

VULNERABILIDADES

Una **vulnerabilidad** es cualquier debilidad en el sistema informático que pueda permitir a las amenazas causarle daños y producir pérdidas en la organización.

Las vulnerabilidades se corresponden con fallos en los sistemas físicos y/o lógicos, aunque también pueden tener su origen en los defectos de ubicación, instalación, configuración y mantenimiento de los equipos.

Pueden estar ligadas a aspectos organizativos (procedimientos mal definidos o sin actualizar, ausencia de políticas de seguridad...), al factor humano (falta de formación y/o de sensibilización del personal con acceso a los recursos del sistema), a los propios equipos, a los programas y herramientas lógicas del sistema, a los locales y las condiciones ambientales del sistema (deficientes medidas de seguridad físicas, escasa protección contra incendios, mala ubicación de los locales con recursos críticos para el sistema, etc.).

Se suele emplear una escala cuantitativa o cualitativa para definir el nivel de vulnerabilidad de un determinado equipo o recurso: Baja, Media y Alta.

INCIDENTES DE SEGURIDAD

Un **incidente de seguridad** es cualquier evento que tenga o pueda tener como resultado la interrupción de los servicios suministrados por un sistema informático y/o posibles pérdidas físicas, de activos o financieras. Es decir, se considera que un incidente es la materialización de una amenaza.

IMPACTOS

El **impacto** es la medición y valoración del daño que podría producir a la organización un incidente de seguridad.

Para valorar el impacto es necesario tener en cuenta tanto los daños tangibles como la estimación de los daños intangibles (incluida la información). En este sentido, podría resultar de gran ayuda la realización de entrevistas en profundidad con los responsables de cada departamento, función o proceso de negocio, tratando de determinar cuál es el impacto real de la revelación, alteración o pérdida de la información para la organización, y no sólo del elemento TIC que la soporta.

También en este caso se puede emplear una escala cuantitativa o cualitativa para medir el impacto del daño en la organización: Bajo, Moderado y Alto.

Alto	➢ Pérdida o inhabilitación de recursos críticos ➢ Interrupción de los procesos de negocio ➢ Daños en la imagen y reputación de la organización ➢ Robo o revelación de información estratégica o especialmente protegida
Moderado	➢ Pérdida o inhabilitación de recursos críticos pero que cuentan con elementos de respaldo ➢ Caída notable en el rendimiento de los procesos de negocio o en la actividad normal de la organización ➢ Robo o revelación de información confidencial, pero no considerada estratégica
Bajo	➢ Pérdida o inhabilitación de recursos secundarios ➢ Disminución del rendimiento de los procesos de negocio ➢ Robo o revelación de información interna no publicada

Tabla 1: Escala propuesta para medir el impacto del daño en la organización

RIESGOS

El **riesgo** es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un determinado impacto en la organización.

El nivel de riesgo depende, por lo tanto, del análisis previo de vulnerabilidades del sistema, de las amenazas y del posible impacto que éstas puedan tener en el funcionamiento de la organización.

Se han propuesto distintas metodologías como CRAMM (*CCTA Risk Analysis and Management Method*, http://www.cramm.com) para la evaluación de riesgos en sistemas informáticos. Esta metodología fue desarrollada por la agencia CCTA (*Central Computer and Telecommunications Agency*) del gobierno del Reino Unido en 1985. Se han publicado distintas revisiones desde entonces, la última de ellas (versión 5) en 2003, incluyendo varias escalas para la valoración del impacto en una organización.

Figura 2: Esquema propuesto por la metodología CRAMM

En España cabría destacar la metodología MAGERIT, publicada en 1996 por el Ministerio de Administraciones Públicas, que ha sido revisada recientemente, durante el pasado verano de 2005. Otros países europeos han elaborado sus propias metodologías de análisis y evaluación de riesgos, como las francesas MARION (propuesta en 1985 por la Asociación de Empresas Aseguradoras Francesas) y MELISA (definida en 1984 dentro del entorno militar francés).

En definitiva, la organización debería evaluar el nivel de riesgo atendiendo a la frecuencia de materialización de las amenazas y al nivel de impacto causado en el negocio.

Veamos a continuación un ejemplo práctico de evaluación del nivel de riesgo:

- Activo: servidor de ficheros de la organización.
- Amenaza: fallo hardware en un servidor, con una probabilidad de ocurrencia baja (una vez cada 5 años).
- Vulnerabilidad del sistema: alta, ya que no se dispone de un servidor alternativo ni de medidas redundantes (como los discos RAID, etc.).
- Impacto: indisponibilidad durante 24 horas del activo afectado (hasta que sea reparado por el servicio técnico), por lo que se puede considerar como un impacto de nivel alto.
- Nivel de riesgo: se obtiene a partir de las tablas de valoración que se hayan adoptado, teniendo en cuenta que la amenaza es baja, la vulnerabilidad es alta y el impacto es alto.

Seguidamente se presenta una propuesta de formato de tabla con los elementos necesarios para poder realizar una evaluación del nivel de riesgo asociado a cada uno de los recursos del sistema informático de la organización:

Recurso	Importancia para la organización (Factor de ponderación)	Identificación de una Amenaza	Probabilidad de materialización de una Amenaza	Vulnerabilidad del Sistema ante esta Amenaza	Evaluación del Impacto (Económico, etc.)	Evaluación del Riesgo
Rec. 1	8	Amenaza X	20%	50%	100,00	80,00
Rec. 2	6	Amenaza Z	30%	40%	200,00	180,00

Tabla 2: Ejemplo de tabla para la Evaluación de Riesgos

Por otra parte, también se han propuesto otras herramientas y metodologías que permiten evaluar el riesgo, entre las que podríamos destacar las que se mencionan a continuación:

- OCTAVE (*Operationally Critical Threat, Analysis and Vulnerability Evaluations*), metodología de análisis y evaluación de riesgos (www.cert.org/octave).

- "*RiskWatch*", software de evaluación del riesgo que contempla los controles previstos por la norma ISO 17799 (www.riskwatch.com).

- COBRA (*Consultative, Objective and Bi-functional Risk Analysis*), software de evaluación del riesgo que también contempla los controles previstos por la norma ISO 17799 (www.security-risk-analysis.com).

DEFENSAS, SALVAGUARDAS O MEDIDAS DE SEGURIDAD

> Una **defensa, salvaguarda o medida de seguridad** es cualquier medio empleado para eliminar o reducir un riesgo. Su objetivo es reducir las vulnerabilidades de los activos, la probabilidad de ocurrencia de las amenazas y/o el nivel de impacto en la organización.

Una **medida de seguridad activa** es cualquier medida utilizada para anular o reducir el riesgo de una amenaza. Las medidas activas podrían, a su vez, clasificarse en *medidas de prevención* (de aplicación antes del incidente) y *medidas de detección* (de aplicación durante el incidente).

Por su parte, una **medida de seguridad pasiva** es cualquier medida empleada para reducir el impacto cuando se produzca un incidente de seguridad. Por ello, a las medidas pasivas también se las conoce como *medidas de corrección* (se aplican después del incidente).

Así, como ejemplos de medidas preventivas podríamos citar la autenticación de usuarios, el control de accesos a los recursos, la encriptación de datos sensibles, la formación de los usuarios, etc. Entre las medidas detectivas se encuentran los Sistemas de Detección de Intrusiones (IDS) o las herramientas y procedimientos para el análisis de los "*logs*" (registros de actividad de los equipos). Por último, como medidas correctivas se podrían considerar las copias de seguridad, el plan de respuesta a incidentes y de continuidad del negocio, etc.

Por otra parte, también podemos distinguir entre **defensas físicas** y **defensas lógicas**. Las primeras se refieren a medidas que implican el control de acceso físico a los recursos y de las condiciones ambientales en que tienen que ser utilizados (temperatura, humedad, suministro eléctrico, interferencias...), mientras que las segundas se encuentran relacionadas con la protección conseguida mediante distintas

herramientas y técnicas informáticas: autenticación de usuarios, control de acceso a los ficheros, encriptación de los datos sensibles, etc.

La organización debe llevar a cabo una adecuada y cuidosa selección, implantación y verificación de las medidas de seguridad. En la etapa de selección puede resultar de ayuda estándares aprobados a nivel internacional como el ISO 17799, que incluye una relación de controles y de buenas prácticas de seguridad. Además, será necesario tener en cuenta una serie de parámetros que permitan analizar la aplicabilidad de cada medida propuesta: coste económico de la medida; dificultad para su implantación tanto a nivel técnico, como en el plano humano y organizativo; disminución del riesgo que se prevé conseguir tras la implantación de la medida; etc.

Por último, tras la correcta implantación de las medidas seleccionadas, la organización deberá determinar el "**Nivel de Riesgo Residual**", obtenido tras un nuevo proceso de evaluación de riesgos teniendo en cuenta que los recursos ya se encuentran protegidos por las medidas de seguridad seleccionadas.

Si el nivel de riesgo resultante para un determinado activo todavía continuase siendo demasiado alto para los objetivos fijados por la organización, se tendrían que seleccionar medidas de seguridad adicionales y repetir nuevamente el proceso. No obstante, es necesario asumir que siempre existirá un cierto Riesgo Residual en el sistema informático. Este "Nivel de Riesgo Residual" representa el nivel de riesgo que la organización estaría dispuesta a aceptar, teniendo en cuenta que no resultaría beneficioso reducirlo aún más debido al esfuerzo técnico y económico que ello conllevaría. Se trata, por lo tanto, de mantener un equilibro entre el esfuerzo técnico y económico y el nivel de riesgo aceptable por la organización, tal y como se representa en la siguiente figura:

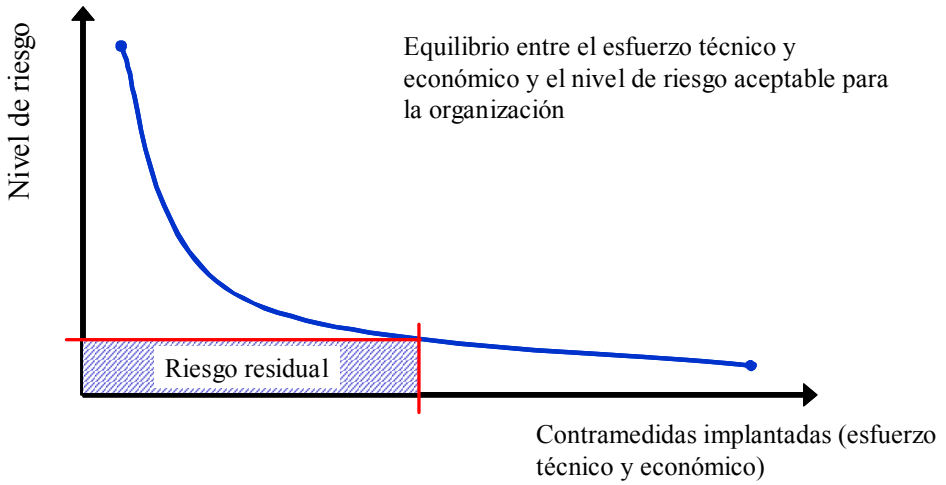

Figura 3: Nivel de riesgo residual

Conviene llevar a cabo una reevaluación del nivel de riesgo tras la implantación de las medidas de seguridad. Además, también sería recomendable realizar nuevas evaluaciones del nivel de riesgo de forma periódica en la organización, ya que será necesario contemplar los cambios experimentados por el sistema de información de la organización: adquisición y puesta en marcha de nuevos recursos, nuevas aplicaciones y servicios; incorporación de personal; puesta en marcha de nuevas instalaciones; etc.

Asimismo, esta reevaluación periódica del nivel de riesgo también estaría justificada por el descubrimiento de nuevas vulnerabilidades, como podrían ser el caso de nuevos fallos detectados en las aplicaciones informáticas, o por la aparición de nuevas amenazas en el entorno o el cambio en la probabilidad de ocurrencia de alguna de las amenazas previamente detectadas.

Por supuesto, en todo este proceso de evaluación y gestión de riesgos será necesario prestar una especial atención a la situación de los recursos o activos críticos, es decir, de aquellos que resulten esenciales para el normal funcionamiento de la organización. La priorización de las actuaciones y de la implantación de medidas de seguridad vendrá determinada por estos recursos críticos.

Todo el proceso descrito en los párrafos anteriores se presenta de forma esquemática en la siguiente figura:

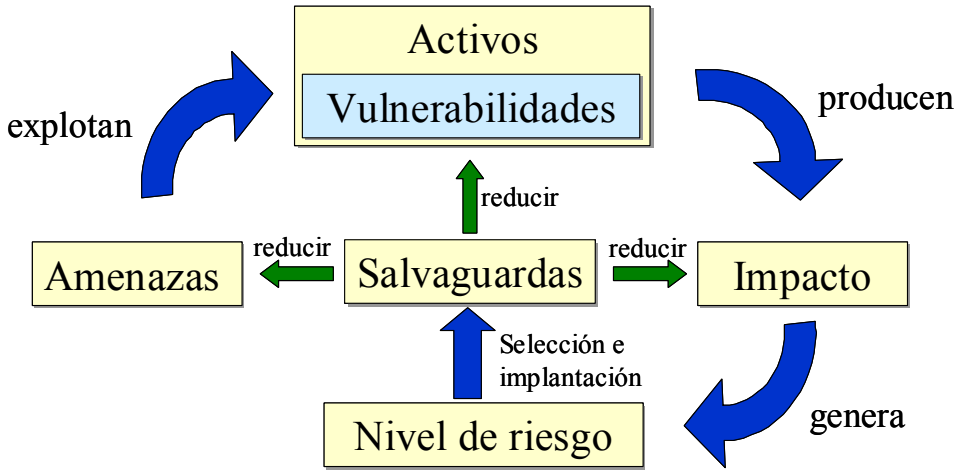

Figura 4: El proceso de Evaluación y Gestión de Riesgos

TRANSFERENCIA DEL RIESGO A TERCEROS

Como alternativa a la implantación de una serie de medidas de seguridad, una organización también podría considerar la transferencia del riesgo a un tercero, ya sea mediante la contratación de una póliza de seguros especializada o bien a través de la subcontratación de un proveedor especializado en ofrecer determinados servicios de seguridad informática.

En lo que se refiere a la contratación de un seguro frente a daños o ataques informáticos ("***Network Risk Insurance***"), es necesario tener en cuenta que los aseguradores suelen exigir una valoración externa del sistema de seguridad de la organización. Además, la organización interesada en este tipo de seguro puede ser obligada a redefinir sus Políticas de Seguridad, a la adquisición de un software y hardware específicos y a la implantación de una serie de procedimientos y controles de seguridad rutinarios.

Las pólizas tradicionales de responsabilidad civil y cobertura de daños suelen excluir expresamente las pérdidas ocasionadas por fallos y ataques informáticos: virus, *hackers* y *crackers*, etc. Sin embargo, las pólizas especializadas en la seguridad informática contemplan la cobertura de los daños propios de la organización derivados de ataques y otros incidentes de seguridad: pérdidas económicas derivadas de las reparaciones y sustituciones de equipos y sistemas; daños ocasionados por la interrupción en el negocio; contratación de consultores informáticos y legales para mitigar los daños; etc.

Además, en estas pólizas especializadas en la seguridad informática también se puede contemplar la cobertura de las reclamaciones de terceros, motivadas por los daños que se puedan ocasionar a otros sistemas y redes informáticas que resulten como consecuencia de virus o ataques iniciados desde equipos de la propia organización; el incumplimiento de las condiciones del servicio pactadas con los clientes; la violación de derechos de propiedad intelectual; la difusión de contenidos ofensivos contra terceros; la violación de la confidencialidad o de la privacidad de los usuarios; etc.

Como ejemplo de empresa especializada en este tipo de pólizas podríamos citar a American International Group (AIG), que gestiona el 70% de las pólizas en Estados Unidos y ofrece una amplia variedad de coberturas.

Por otra parte, la segunda alternativa propuesta sería la contratación de una empresa especializada en ofrecer determinados Servicios de Seguridad Informática, alternativa también conocida como "*Managed Security Services*" (MSS –Servicios de Seguridad Gestionados–), con un planteamiento similar al de la propia seguridad física de las instalaciones de la organización, que hoy en día suele estar subcontratada a una empresa especializada que se encarga del mantenimiento de las alarmas, el control del acceso del personal a las instalaciones o la vigilancia nocturna y durante los fines de semana.

Se trata, por lo tanto, de otra modalidad de transferencia del riesgo a un tercero, mediante un contrato con unas determinadas exigencias de nivel servicio (SLA, "*Service Level Agreement*") y cláusulas de responsabilidad. La empresa contratada debe ofrecer un servicio permanente (24 horas al día durante los 7 días de la semana) por parte de profesionales cualificados: monitorización de los registros de actividad en los equipos informáticos y del tráfico en la red de la organización; detección y contención de ataques; actualización permanente de aplicaciones y de servidores; filtrado de contenidos y mensajes dañinos; eliminación de virus; etc.

Teniendo en cuenta que hoy en día es imprescindible dominar múltiples tecnologías, en un entorno complejo y cambiante, caracterizado por un mercado en el que se ofrecen gran cantidad de productos y servicios de seguridad, la alternativa de la subcontratación de determinados servicios de seguridad podría mejorar, en general, la Gestión de la Seguridad de la Información, contribuyendo a reducir y controlar los costes para la organización.

Por último, la organización también podría considerar conveniente recurrir a una empresa externa especializada para la revisión de la seguridad de los servicios públicos que ofrece a través de Internet: Website, servidor FTP, servidor DNS...

Así, por ejemplo, podríamos citar los servicios de empresas como ScanAlert (www.scanalert.com), que se encargan de comprobar y certificar la seguridad de un determinado Website, otorgando un sello de confianza si cumple con unas condiciones de seguridad previamente especificadas.

Figura 5: ScanAlert

REFERENCIAS DE INTERÉS

- ✓ COBRA: http://www.security-risk-analysis.com/
- ✓ CRAMM: http://www.cramm.com/
- ✓ RiskWatch: http://www.riskwatch.com/
- ✓ OCTAVE: http://www.cert.org/octave
- ✓ ScanAlert: http://www.scanalert.com/
- ✓ SecurityFocus: http://www.securityfocus.com/
- ✓ FoundStone: http://www.foundstone.com/