tecnimap Murcia 2004

22

PILAR. HERRAMIENTAS PARA EL ANÁLISIS Y LA GESTIÓN DE RIESGOS

José A. Mañas
Catedrático de Universidad
Dept. Ingeniería de Sistemas Telemáticos. E.T.S.I. de Telecomunicación. Universidad Politécnica de Madrid

RESUMEN

El autor está desarrollando bajo contrato del Centro Criptológico Nacional (CCN) un conjunto de herramientas para el análisis y la gestión de riesgos en sistemas de información y comunicaciones. Esta comunicación describe las actividades de análisis y gestión, su oportunidad y el soporte que prestan las herramientas. El sistema se basa en la metodología Magerit v.1.

1. INTRODUCCIÓN

Comencemos con una definición:

- **Seguridad de las redes y de la información:** la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

Puesto el acento en los servicios que constituyen la misión de la organización y los datos que maneja para la prestación de aquellos servicios, es importante salvaguardar ambos en las siguientes dimensiones:

- **Disponibilidad:** o disposición a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.
- **Integridad:** o mantenimiento de las características de completitud y corrección de servicios o datos. Contra la integridad podemos encontrarnos información manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una organización.
- **Confidencialidad:** o que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto nos encontraremos con fugas y filtraciones de información y accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de normas y regulaciones respecto del cuidado de los datos.
- **Autenticidad (del origen de los datos):** o que no haya duda de quién se hace responsable de una información o prestación de un servicio, tanto a fin de confiar en él como de poder perseguir posteriormente los incumplimientos o errores. Contra la autenticidad nos encontramos con suplantaciones y engaños que buscan realizar un fraude. La autenticidad es la posibilidad de luchar contra el repudio y, como tal, se convierte en una dimensión básica para fundamentar el llamado comercio electrónico o la administración electrónica, permitiendo confiar sin papeles ni presencia física.

Todas estas características pueden ser requeridas o no dependiendo de cada caso. Cuando se requieren, no es evidente que se disfruten sin más, sino más bien es lo habitual que haya que poner medios y esfuerzo para conseguirlas. A racionalizar este esfuerzo se dedican las metodologías de análisis y gestión de riesgos que comienzan con una definición:

- **Riesgo:** una función de la probabilidad de que una vulnerabilidad del sistema afecte a la autenticación o a la disponibilidad, autenticidad, integridad o confidencialidad de los datos procesados o transferidos y la gravedad de esa incidencia, resultante de la utilización intencionada o no intencionada de esa vulnerabilidad;

El riesgo indica lo que le podría pasar a los elementos del sistema de información sino hacemos nada positivo por ellos. Es importante saber que características son de interés en cada elemento, así como saber en qué medida estas características están en peligro.

Sabiendo lo que nos podría pasar, tenemos que tomar decisiones:

- **Gestión del riesgo:** el proceso, distinto de la evaluación del riesgo, consistente en sopesar las alternativas políticas existentes mediante consultas con las partes interesadas, analizar la evaluación del riesgo y otros factores legítimos y, si fuera necesario, seleccionar las opciones de prevención y control

Nótese que una opción legítima es aceptar el riesgo. Es frecuente oír que la seguridad absoluta no existe; en efecto, siempre hay que aceptar un riesgo que, eso sí, debe estar por debajo del umbral de la calidad del servicio que se requiere.

Como todo esto es muy delicado, no es meramente técnico, y puede requerir asumir la decisión política de aceptar el riesgo, más nos vale a todos que sepamos en qué condiciones estamos trabajando y así podamos ajustar nuestra confianza. Para ello qué mejor que una aproximación metódica que permita tomar decisiones con fundamento y explicar racionalmente las decisiones tomadas.

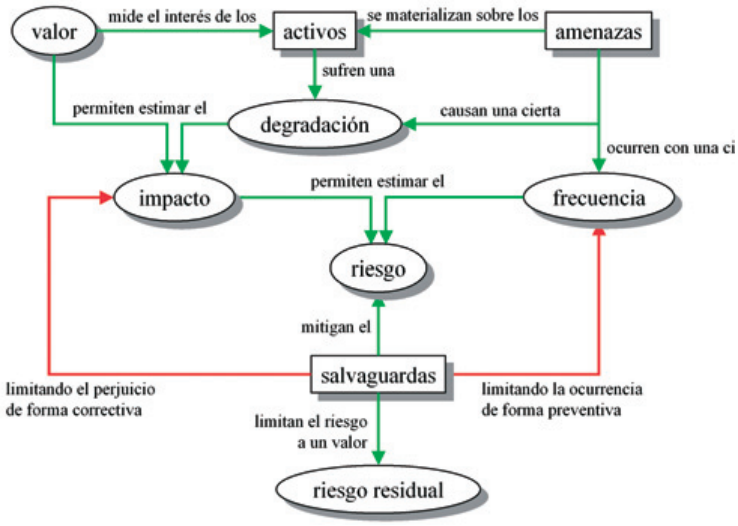
A este buen fin se orientó MAGERIT [6], que será la metodología que emplearemos en lo que sigue.

2. ANÁLISIS DE RIESGOS

El análisis de riesgos[1] es pues una aproximación metódica que nos permite determinar el riesgo siguiendo unos pasos

1. determinar los activos relevantes para la organización,
2. valorar dichos activos en función del coste que supondría para la organización recuperarse de un fallo de disponibilidad, integridad, confidencialidad o autenticidad
3. determinar a qué amenazas están expuestos aquellos activos
4. valorar la vulnerabilidad de los activos a las amenazas potenciales
5. estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
6. estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectación de materialización) de la amenaza

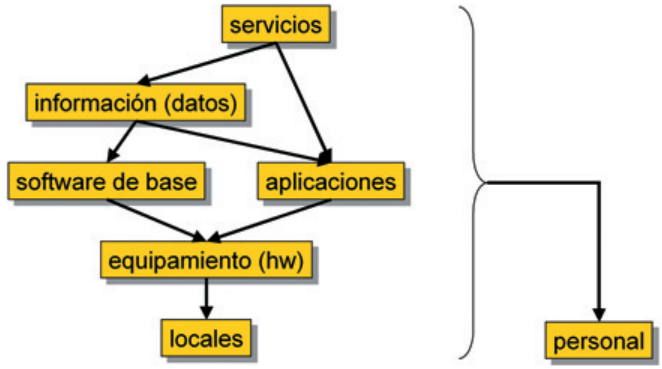
Gráficamente:



GMITS [3] define activo como "todo aquello que tiene valor para la organización". Es interesante este matiz finalista, pues no estamos valorando lo que cuesta crear o mantener la organización, sino lo que costaría repararla en caso de sufrir un percance de seguridad.

Es habitual valorar los activos de tipo servicio final o datos; pero en un sistema de información estos activos dependen de otros activos más prosaicos como pueden ser los equipos, las comunicaciones o las frecuentemente olvidadas personas que trabajan con aquellos. Por ello aparece como importante el concepto de "dependencias entre activos" o la medida en que un activo *superior* se vería afectado por un incidente de seguridad en un activo *inferior*[2].

Es típico ver cómo los servicios dependen de los datos y de los aplicativos, propios o adquiridos. Todos a su vez dependen del equipamiento, *hardware* y comunicaciones que, a su vez, dependen de los locales que los acogen y de las personas que los operan.



El siguiente paso consiste en determinar las amenazas que pueden afectar a cada activo. Las amenazas son "cosas que ocurren". Y, de todo lo que puede ocurrir, nos interesa lo que puede pasarle a nuestros activos y causar un daño. Hay accidentes naturales (terremotos, inundaciones, ...) y desastres industriales (contaminación, fallos eléctricos, ...) ante los cuales somos víctimas pasivas; pero no por ser pasivos debemos esperar indefensos. Hay amenazas causadas por las personas, bien errores, bien ataques intencionados.

Una vez determinado que una amenaza puede perjudicar a un activo, hay que estimar cuán vulnerable es el activo, en dos sentidos:

frecuencia: cada cuánto podemos estimar que va a materializarse la amenaza

degradación: cómo de perjudicado sale el activo (entre 0 y 100%)

El resto es muy sencillo:

impacto = valor * degradación

riesgo = impacto * frecuencia

Y ya tenemos estimado el riesgo de nuestro sistema, activo por activo.

2.1. Riesgo repercutido

Es habitual acumular el valor de los activos superiores sobre los activos inferiores, según el árbol de dependencias entre activos. Esta aproximación indica rápidamente qué activos son críticos, poniendo el énfasis en los componentes técnicos del sistema.

Nada que objetar; pero a veces una visión muy técnica no es la preferida por la gerencia que preferiría entender el riesgo en sus términos habituales: servicios. Es decir, responder a la pregunta ¿qué servicios están en situación de riesgo?

Para responder a esta pregunta se introduce un nuevo concepto de "repercusión de las amenazas" de forma que ante una amenaza que se materializa sobre un activo inferior, transferimos el cálculo del impacto a los activos que dependen del perjudicado (cuantificando la degradación causada en la proporción en que dependan). Así

impacto_repercutido = valor_propio * degradación_repercutida

riesgo_repercutido = impacto_repercutido * frecuencia

Impacto y riesgo repercutidos no son otro análisis de riesgos, sino simplemente una forma alternativa de presentar el mismo análisis de riesgos.

3. GESTIÓN DE RIESGOS

Si el riesgo que estima la fase anterior es perfectamente asumible por la organización, hemos terminado. Cualquier nivel de riesgo es aceptable si lo conoce y acepta la dirección[3].

Si no es aceptable, hay que decidir por dónde se ataja:

eliminando la fuente del riesgo, lo que puede suponer prescindir de algún servicio en extremo riesgoso, o de algún activo que aporta poco valor añadido, o ...

mitigando el riesgo, de forma que caiga a unos niveles aceptable

transfiriendo el riesgo, de forma que, sin eliminarlo, no seamos sus víctimas

La mitigación del riesgo requiere entrar en más detalle, pues podemos

actuar preventivamente para que no ocurra; muy atractivo, pero a veces imposible o extremadamente costoso

actuar reactivamente para que cuando la amenaza se materialice las consecuencias no sean graves; esto supone disponer de un plan de emergencia y de un plan de recuperación

Es habitual que una buena política de gestión de riesgos incluya medidas preventiva en combinación con medidas reactiva para lograr una protección cabal con un digno margen de seguridad.

Por último hay que destacar que un plan de protección debe trabajar en varios frentes:

salvaguardas técnicas: en equipos y comunicaciones

salvaguardas físicas: protegiendo el entorno de trabajo de las personas y los equipos

medidas organizativas: de prevención y gestión de las incidencias

política de personal: que es el final el eslabón imprescindible y más delicado

3.1. Riesgo residual

Con toda esta batería de salvaguardas se puede repetir el cálculo del impacto y del riesgo, sabiendo que el valor de los activos no ha cambiado; pero sí habremos disminuido su vulnerabilidad, bien reduciendo la frecuencia a un valor residual, bien reduciendo la degradación a un valor residual. Se denominan

impacto_residual = valor * frecuencia_residual

riesgo_residual = impacto_residual * frecuencia_residual

Que, como anteriormente, puede estimarse acumulando valor sobre los activos inferiores o repercutiendo la degradación sobre los activos superiores.

4. ¿CUÁNDO PROCEDE ANALIZAR Y GESTIONAR LOS RIESGOS?

Realizar un análisis de riesgos es laborioso y costoso. Levantar un mapa de activos y valorarlos requiere la colaboración de muchos perfiles dentro de la organización, desde los niveles de gerencia de negocio hasta los detalles técnicos. Y no solo es que haya que involucrar a muchas personas, sino que hay que lograr una uniformidad de criterio entre todos pues, si importante es cuantificar el riesgo, más importante aún es relativizarlo. Y esto es así porque típicamente en un análisis de riesgos aparecen miles de datos de imposible observación directa. La única forma de afrontar la complejidad es centrarse en lo más importante (máximo impacto, máximo riesgo) y obviar lo que es secundario o incluso despreciable. Pero si los datos no están bien ordenados en términos relativos, su interpretación es imposible.

Un análisis de riesgos es recomendable en cualquier organización que dependa de los sistemas de información y comunicaciones para el cumplimiento de su misión. En particular en cualquier entorno donde se practique la tramitación electrónica de bienes y servicios, sea en contexto público o privado. El análisis de riesgos permite tomar decisiones de inversión en tecnología, desde la adquisición de equipos de producción hasta el despliegue de un centro alternativo para asegurar la continuidad del negocio, pasando por las decisiones de adquisición de salvaguardas técnicas y de selección y capacitación del personal.

El análisis de riesgos es además requisito previo exigido por los protocolos de certificación en seguridad de los sistemas de información (sea BS 7799-2 [1] o UNE 71502 [10]). Antes de proceder a la certificación, debe haber realizado un análisis de riesgos que, además, será un punto de control de la gestión del sistema.

El análisis de riesgos es la fuente de información para rellenar una declaración de aplicabilidad, también necesaria para proceder a una certificación.

Desde el punto de vista legal, van apareciendo leyes de carácter administrativo que imponen la necesidad de que se haya realizado un análisis de riesgo del servicio antes de su puesta en operación. Véase, por ejemplo, [7].

5. HERRAMIENTAS DE SOPORTE

Como ya se ha indicado, la realización de un análisis de riesgos es muy laboriosa y su mantenimiento también. La necesidad del mantenimiento deriva tanto de la conveniencia para la organización como de los protocolos de certificación. El mantenimiento permite incorporar nuevos activos resultado de nuevas adquisiciones, nuevos servicios o procesos de negocio y nuevas amenazas. A lo largo del tiempo puede variar la percepción del valor de un activo, o la estimación de la vulnerabilidad frente a las amenazas. Todo esto es muy conveniente tratarlo de una forma incremental que permita seguir la evolución del sistema.

También es conveniente la evolución del riesgo a lo largo de las etapas de un plan director de seguridad que, a lo largo de un periodo prolongado, va incorporando los resultados de inversiones en seguridad de la información.

Todo esto lleva a la necesidad de disponer de un entorno automatizado de análisis y mantenimiento.

5.1. PILAR – Herramientas de soporte

Para afrontar estos escenarios se ha desarrollado PILAR, que es un conjunto de herramientas que actualmente ofrece

Análisis cualitativo. Las valoraciones de los elementos (activos, amenazas y salvaguardas) se realiza por niveles, desde la irrelevancia hasta la máxima importancia o criticidad. Esto hace un análisis rápido del que lo más importante es la relativización de impactos y riesgos.

Análisis cuantitativo. Las valoraciones son numéricas, típicamente en términos dinerarios. Esto hace el análisis mucho más preciso, si se consigue validar los datos empleados. El análisis puede llegar a ofrecer resultados de recuperación de la inversión en salvaguardas, en términos de riesgo menguante.

Es importante poder pasar del análisis cualitativo al cuantitativo y viceversa, pues la presentación de los niveles de riesgo es diferente. Es importante destacar el papel de la herramienta como ayuda al analista; primero, para introducir y consolidar datos, calculando los impactos y riesgos que se derivan de los valores introducidos. Y segundo, la herramienta permite la navegación entre los diferentes puntos de vista, ayudando a la comprensión del sistema y de las razones que llevan a conclusiones. Análisis y gestión no pueden verse como "procesos ciegos" que metabolizan de forma mágica los datos que entran. Muy al contrario, muchas veces el "por qué" es más importante que el resultado final.

Las herramientas emplean el concepto de "categoría de activos" para organizar el inventario y para ayudar al analista en la identificación de amenazas y salvaguardas relevantes. Las herramientas pueden hacer sugerencias al analista, basándose en la categoría de los activos involucrados.

También se soporta la presentación del riesgo como acumulado sobre los activos de soporte o repercutido en los servicios prestados, como se explicó anteriormente.

La herramienta busca un amplio espectro de utilización. En su vertiente más ejecutiva (casi con toda seguridad, cualitativa) se busca poder levantar un primer plano de riesgos en una jornada, con resultados al menos orientados en la dirección correcta. La captura de datos y automatización permite que aquel esbozo rápido pueda ser refinado y mantenido capturando una caracterización más precisa (probablemente cuantitativa) de la organización.

5.2. Bibliotecas

PILAR es un entorno adaptable. Se puede trabajar con diferentes marcos, estando dentro de lo parametrizable

- las categorías de activos
- las dimensiones de valoración de los activos (típicamente, disponibilidad, integridad, confidencialidad y autenticidad; pero hay casos más simples y más complejos)
- la colección de amenazas
- los niveles de valoración cualitativa de activos y amenazas
- la clasificación de salvaguardas, unas técnicas, otras de tipo organizativo; pero todas ellas con un efecto sobre el riesgo

En el desarrollo actual se trabaja con tres bibliotecas

criterios de seguridad (ver [2]) que es una guía de recomendaciones y obligaciones para proteger los activos empleados por la administración pública

UNE-ISO/IEC 17799 (ver [9]) que es una guía ampliamente difundida internacionalmente, y base de los protocolos de certificación 7799-2 y 71502, antes citados

defensa, que es una biblioteca específica del Ministerio de Defensa para material clasificado

Se está trabajando en nuevas librerías, concretamente para afrontar

protección de datos, de carácter personal, en base a [5] y [8], que permita analizar el estado de seguridad de los datos a la vista de las medidas de seguridad implantadas, más allá del mero cumplimiento de las obligaciones legales

criterios comunes (en base a [4]) que permita tanto la elaboración de perfiles de protección como una evaluación del riesgo efectivo cuando se satisfacen perfiles de certificación

Las bibliotecas establecen una diferencia entre el marco de análisis y el caso concreto, a fin de facilitar la labor del analista y la interpretación de los resultados que son acordes a un contexto estable. Se busca evitar la situación actual donde cada análisis de riesgos responde a metodologías propias o ad-hoc que hacen muy difícil, por no decir imposible, la comparación de dos análisis.

Las bibliotecas pueden ser modificadas por un responsable de seguridad, bien sectorial, bien de seguridad corporativa en entornos complejos. Conviene no inventar la rueda en cada ocasión; pero en un entorno complejo es necesario que los inventos sean consolidados y mantenidos corporativa o sectorialmente.

6. CONCLUSIONES

Realizar un análisis de riesgos y gestionar el riesgo residual es una actividad muy interesante para tomas decisiones de inversión en seguridad de las TIC; pero al tiempo es una actividad larga y costosa cuyos resultados deben mantenerse actualizados con el paso del tiempo.

En consecuencia se ha buscado un soporte de programas que permitan crear un modelo de análisis en un contexto adecuado y mantenerlo de forma incremental en el tiempo. El resultado es la herramienta PILAR.

7. MENCIONES

La herramienta PILAR se desarrolla bajo contrato con el Centro Nacional de Inteligencia. Las especificaciones iniciales partieron del Centro Criptológico Nacional, habiendo evolucionado gracias al equipo de dirección del proyecto en el que han intervenido tanto el mismo CNI como el MAP (Ministerio para las Administraciones Públicas) y la FNMT (Fábrica Nacional de Moneda y Timbre). Aunque los errores de esta comunicación sean del autor, los méritos son de este sacrificado equipo que ha sido tanto caldo de cultivo de ideas como beta-testers de las diferentes versiones de PILAR.

REFERENCIAS

[1] BS 7799-2:2002, "Information security management systems — Specification with guidance for use", British Standards Institute, 2002.

[2] "Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades", MAP, 2003, http://www.csi.map.es/csi/pg5c10.htm.

[3] GMITS, ISO/IEC TR 13335-1: 1996, "Concepts and models for IT security". Publicado como UNE 71501-1. Actualmente en proceso de revisión.

[4] ISO/IEC 15408, "Information technology — Security techniques — Evaluation criteria for IT security", 1999.

[5] LOPD, Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

[6] MAGERIT, "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información", MAP, versión 1.0, 1997, http://www.csi.map.es/csi/pg5m20.htm

[7] Orden PRE/1551/2003, de 10 de junio, por la que se desarrolla la Disposición final primera del Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.

[8] Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

[9] UNE-ISO/IEC 17799:2002, "Tecnología de la Información. Código de Buenas Prácticas de la Gestión de la Seguridad de la Información". 2002.

[10] UNE 71502:2003, "Especificaciones para los Sistemas de Gestión de la Seguridad de la Información", AENOR,

BIBLIOGRAFÍA

1- A veces denominado "elaboración del mapa de riesgos".

2- Un ejemplo puede ser mejor que mil palabras. Si se quema el local que hospeda los equipos, lo que no funciona es el servicio percibido por el usuario a kilómetros de distancia. Si roban el portátil de un ejecutivo con información estratégica de la empresa, lo que sufre es la confidencialidad de dicha información. Los locales se reconstruyen; pero puede haberse pasado la oportunidad de prestar el servicio. El robo se subsana comprando otro portátil; pero el secreto ya está perdido.

3- Hablar de dirección es pecar de simplificar la realidad. En inglés suele emplearse el término "stakeholders" (o tenedores de la estaca) para referirse a los afectados por las decisiones estratégicas de una organización: dueños, gerentes, usuarios, empleados e incluso la sociedad en general. Porque al final si se aceptan riesgos imprudentemente elevados, el perjudicado puede no ser sólo el que dirige, sino todos los que tienen su confianza puesta en la organización y cuyo lamentable desempeño oscurecería sus legítimas expectativas. En última instancia puede verse afectada la confianza en un sector o en una tecnología por la imprudente puesta en escena de algunos actores.