Administración
Electrónica

Gestión de Riesgos

Magerit

tiThink
Strategic Technological Consulting

Gestión de Riesgos
Magerit

Editado por tiThink
Por José María Rodríguez e Ignacio Peralta

Esta publicación incluye información obtenida de los documentos y guías técnicas publicadas por el Consejo Superior de Administración Electrónica, relativas a la adecuación de las Administraciones Públicas a las metodologías de análisis y gestión de riesgos TIC.. Esta publicación tiene el propósito general de divulgar dicha metodología y sus implicaciones prácticas a la hora de abordar su implementación. Antes de tomar cualquier decisión práctica en el momento de implementar cualquier iniciativa de las descritas en este documento se debe consultar los documentos y guías oficiales y/o asesores profesionales especializados en Magerit v3.

Contenido

Presentación

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, que permite:

Estudiar los riesgos que soporta un sistema de información y el entorno asociado a él. MAGERIT propone la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la organización; señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados.

Los resultados del análisis de riesgos permiten a la Gestión de Riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

MAGERIT interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

El análisis y gestión de los riesgos es un aspecto clave del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica que tiene la finalidad de poder dar satisfacción al principio de proporcionalidad en el cumplimiento de los principios básicos y requisitos mínimos para la protección adecuada de la información.

MAGERIT es un instrumento para facilitar la implantación y aplicación del Esquema Nacional de Seguridad proporcionando los principios básicos y requisitos mínimos para la protección adecuada de la información.

En esta línea presentamos este documento, en el que resaltamos los aspectos fundamentales del método Magerit, el cual confiamos que sea de utilidad para todos los que nos vemos involucrados en hacer frente a los retos planteados en este proceso de cambio.

tiThink Consultoría

La Gestión de Riesgos TIC

Un análisis de riesgos TIC es recomendable en cualquier Organización que dependa de los sistemas de información 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 gestión y asignar recursos con perspectiva de negocio, sean tecnológicos, humanos o financieros.

El análisis de riesgos es una herramienta de gestión que permite tomar decisiones. Las decisiones pueden tomarse antes de desplegar un servicio o con éste funcionando. Es muy deseable hacerlo antes, de forma que las medidas que haya que tomar se incorporen en el diseño del servicio, en la elección de componentes, en el desarrollo del sistema y en los manuales de usuario. Todo lo que sea corregir riesgos imprevistos es costoso en tiempo propio y ajeno, lo que puede ir en detrimento de la imagen prestada por la Organización y puede suponer, en último extremo, la pérdida de confianza en su capacidad. Siempre se ha dicho que es mejor prevenir que curar y aquí se aplica: no espere a que un servicio haga agua; hay que prever y estar prevenido.

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 hasta los 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 los riesgos, más importante aún es relativizarlos. Y esto es así porque típicamente en un análisis de riesgos aparecen multitud de datos. 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 riesgos no están bien ordenados en términos relativos, su interpretación es imposible.

En resumen, un análisis de riesgos no es una tarea menor que realiza cualquiera en sus ratos libres. Es una tarea mayor que requiere esfuerzo y coordinación. Por tanto debe ser planificada y justificada.

Si el sistema aspira a una certificación, el análisis de riesgos es un requisito previo que exigirá el evaluador. Es la fuente de información para determinar la relación de controles pertinentes para el sistema y que por tanto deben ser inspeccionados.

La Gestión de Riesgos es así mismo un requisito exigido en los procesos de acreditación de sistemas. Estos procesos son necesarios cuando se va a manipular en el sistema información clasificada nacional, UE, OTAN o de otros acuerdos internacionales.

Procede analizar y gestionar los riesgos cuando directa o indirectamente lo establezca un precepto legal y siempre que lo requiera la protección responsable de los activos de una Organización.

Contexto y Componentes de la Gestión de Riesgos TIC

La Gestión de Riesgos implica dos grandes tareas a realizar:

- Análisis de riesgos, que permite determinar qué tiene la Organización y estimar lo que podría pasar.
- Tratamiento de los riesgos, que permite organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones; como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la Dirección asume.

Ambas actividades, análisis y tratamiento se combinan en el proceso denominado Gestión de Riesgos.

El análisis de riesgos considera los siguientes elementos:

1. **Activos**, que son los elementos del sistema de información (o estrechamente relacionados con este) que soportan la misión de la Organización
2. **Amenazas**, que son cosas que les pueden pasar a los activos causando un perjuicio a la Organización
3. **Salvaguardas** (o contra medidas), que son medidas de protección desplegadas para que aquellas amenazas no causen [tanto] daño.

Con estos elementos se puede estimar:

1. El **impacto**: lo que podría pasar
2. El **riesgo**: lo que probablemente pase

El análisis de riesgos permite analizar estos elementos de forma metódica para llegar a conclusiones con fundamento y proceder a la fase de tratamiento. Informalmente, se puede decir que la gestión de la seguridad de un sistema de información es la gestión de sus riesgos y que el análisis permite racionalizar dicha gestión.

El Análisis del Riesgo

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

1. Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación
2. Determinar a qué amenazas están expuestos aquellos activos
3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo
4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza

Estas valoraciones son teóricas en el caso de que no hubiera salvaguarda alguna desplegada. Una vez obtenido este escenario teórico, se incorporan las salvaguardas del paso 3, derivando estimaciones realistas de impacto y riesgo.

¿Qué son los Activos?

Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

En un sistema de información hay 2 cosas esenciales: la información que maneja y los servicios que presta. Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema.

Subordinados a dichos elementos se pueden identificar otros activos relevantes:

- Servicios auxiliares que se necesitan para poder organizar el sistema.
- Las aplicaciones informáticas (software) que permiten manejar los datos.
- Los equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios.
- Los soportes de información que son dispositivos de almacenamiento de datos.
- El equipamiento auxiliar que complementa el material informático.
- Las redes de comunicaciones que permiten intercambiar datos.
- Las instalaciones que acogen equipos informáticos y de comunicaciones.
- Las personas que explotan u operan todos los elementos anteriormente citados.

No todos los activos son de la misma especie. Dependiendo del tipo de activo, las amenazas y las salvaguardas son diferentes.

¿ Cual es el valor de los activos?

La valoración se debe realizar desde la perspectiva de la necesidad de proteger. Cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes.

El valor puede ser propio, o puede ser acumulado. Se dice que los activos inferiores en un esquema de dependencias, acumulan el valor de los activos que se apoyan en ellos.

El valor nuclear suele estar en la información que el sistema maneja y los servicios que se prestan (activos denominados esenciales), quedando los demás activos subordinados a las necesidades de explotación y protección de lo esencial. La valoración es la determinación del coste que supondría recuperarse de una incidencia que destrozara el activo. Hay muchos factores a considerar:

- coste de reposición: adquisición e instalación
- coste de mano de obra (especializada) invertida en recuperar (el valor) del activo

- lucro cesante: pérdida de ingresos
- capacidad de operar: confianza de los usuarios y proveedores que se traduce en una pérdida de actividad o en peores condiciones económicas
- sanciones por incumplimiento de la ley u obligaciones contractuales
- daño a otros activos, propios o ajenos
- daño a personas
- daños medioambientales

La valoración puede ser cuantitativa (con una cantidad numérica) o cualitativa (en alguna escala de niveles). Los criterios más importantes a respetar son:

- la homogeneidad: es importante poder comparar valores aunque sean de diferentes dimensiones a fin de poder combinar valores propios y valores acumulados, así como poder determinar si es más grave el daño en una dimensión o en otra
- la relatividad: es importante poder relativizar el valor de un activo en comparación con otros activos

Ambos criterios se satisfacen con valoraciones económicas (coste dinerario requerido para curar el activo) y es frecuente la tentación de ponerle precio a todo. Si se consigue, excelente.

Incluso es fácil ponerle precio a los aspectos más tangibles (equipamiento, horas de trabajo, etc.). Pero al entrar en valoraciones más abstractas (intangibles como la credibilidad de la Organización) la valoración económica exacta puede ser escurridiza y motivo de agrias disputas entre los analistas.

¿ Qué aporta una Valoración Cualitativa ?

Las escalas cualitativas permiten avanzar con rapidez, posicionando el valor de cada activo en un orden relativo respecto de los demás. Es frecuente plantear estas escalas como órdenes de magnitud y, en consecuencia, derivar estimaciones del orden de magnitud del riesgo.

La limitación de las valoraciones cualitativas es que no permiten comparar valores más allá de su orden relativo. No se pueden sumar valores.

¿ Podemos realizar una Valoración Cuantitativa ?

Las valoraciones numéricas absolutas cuestan mucho esfuerzo; pero permiten sumar valores numéricos de forma absolutamente natural. La interpretación de las sumas no es nunca motivo de controversia.

Si la valoración es dineraria, además se pueden hacer estudios económicos comparando lo que

se arriesga con lo que cuesta la solución respondiendo a las preguntas:

- ¿Vale la pena invertir tanto dinero en esta salvaguarda?
- ¿Qué conjunto de salvaguardas optimizan la inversión?
- ¿En qué plazo de tiempo se recupera la inversión?
- ¿Cuánto es razonable que cueste la prima de un seguro?

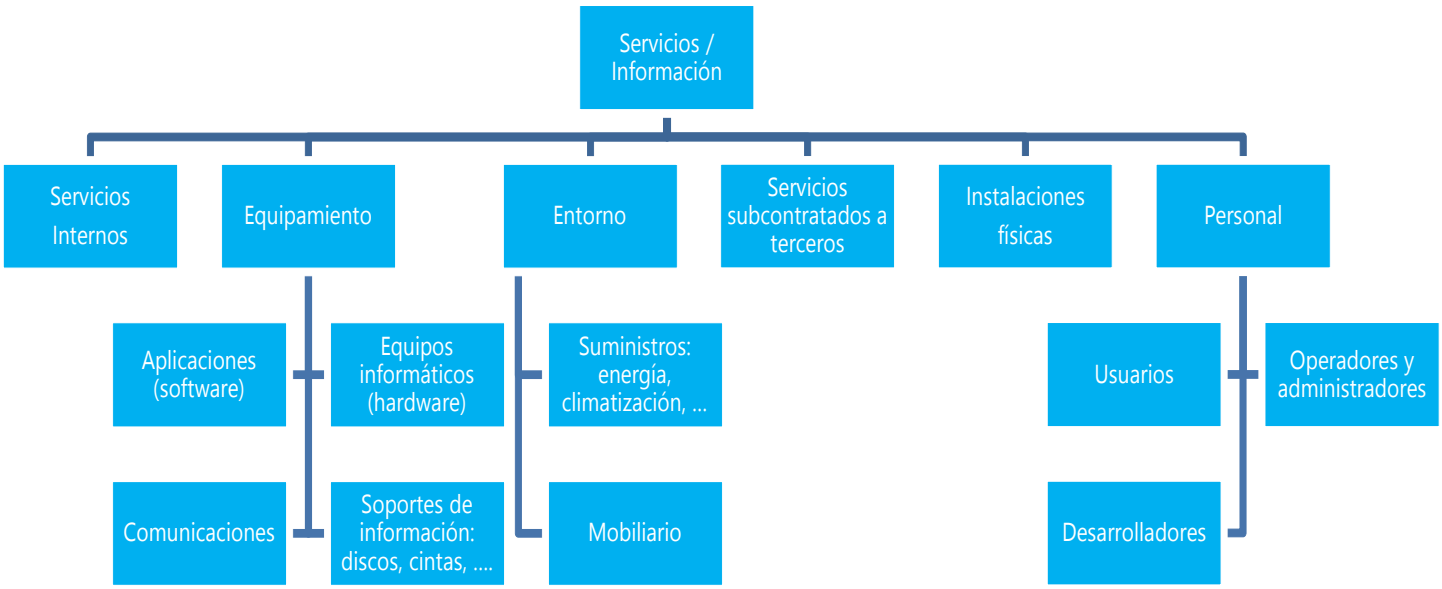
Dependencias entre Activos

Los activos vienen a formar árboles o grafos de dependencias donde la seguridad de los activos que se encuentran más arriba en la estructura o superiores depende de los activos que se encuentran más abajo o inferiores.

Estas estructuras reflejan de arriba hacia abajo las dependencias, mientas que de abajo hacia arriba la propagación del daño caso de materializarse las amenazas.

Se dice que un "activo superior" depende de otro "activo inferior" cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior.

Típicamente, la estructura de dependencia sigue el siguiente grafo:



¿Qué son las Amenazas?

Las amenazas son “cosas que ocurren”. Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a nuestros activos y causar un daño. Típicamente:

- De origen natural. Hay accidentes naturales (terremotos, inundaciones, ...). Ante esos avatares el sistema de información es víctima pasiva, pero debemos tener en cuenta lo que puede suceder.
- Del entorno (de origen industrial). Hay desastres industriales (contaminación, fallos eléctricos, ...) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos.
- Defectos de las aplicaciones. Hay problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidades técnicas o, simplemente, vulnerabilidades.
- Causadas por las personas de forma accidental . Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.
- Causadas por las personas de forma deliberada. Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

No todas las amenazas afectan a todos los activos, sino que hay una cierta relación entre el tipo de activo y lo que le podría ocurrir.

¿ Afectan las amenazas al valor de los activos ?

Una vez determinado que una amenaza puede perjudicar a un activo, hay que valorar su influencia en el valor del activo, en dos sentidos:

- degradación: cuán perjudicado resultaría el [valor del] activo. La degradación mide el daño causado por un incidente en el supuesto de que ocurriera. La degradación se suele caracterizar como una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto “totalmente degradado”, o “degradado en una pequeña fracción”.
- probabilidad: cuán probable o improbable es que se materialice la amenaza. La probabilidad de ocurrencia es más compleja de determinar y de expresar. A veces se modela cualitativamente por medio de alguna escala nominal. A veces se modela numéricamente como una frecuencia de ocurrencia. Es habitual usar 1 año como referencia, de forma que se recurre a la tasa anual de ocurrencia como medida de la probabilidad de que algo ocurra.

¿ Qué es el Impacto ?

Conociendo el valor de los activos y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema. Se miden dos variables de impacto:

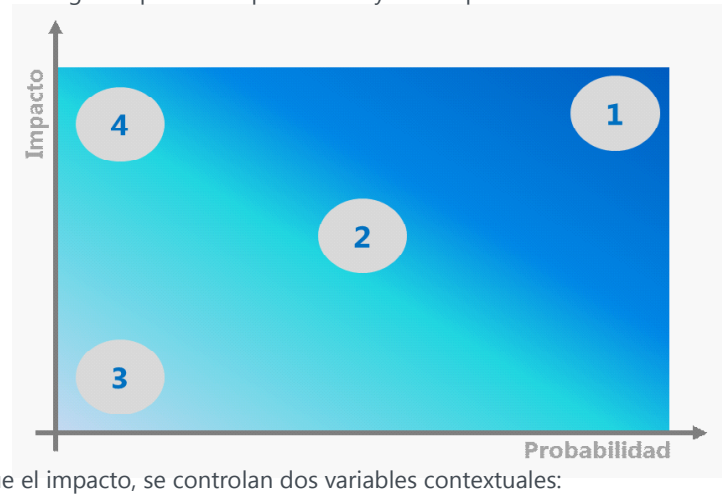
- Impacto acumulado. Es el calculado sobre un activo teniendo en cuenta su valor acumulado (el propio mas el acumulado de los activos que dependen de él) y las amenazas a que está expuesto.
- Impacto repercutido. Es el calculado sobre un activo teniendo en cuenta su valor propio y las amenazas a que están expuestos los activos de los que depende

¿Qué es el Riesgo Potencial?

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, para derivar el riesgo no hay más que tener en cuenta la probabilidad de ocurrencia.

El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo:

- zona 1 – riesgos muy probables y de muy alto impacto
- zona 2 – cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables pero de impacto bajo o muy bajo
- zona 3 – riesgos improbables y de bajo impacto
- zona 4 – riesgos improbables pero de muy alto impacto



Al igual que el impacto, se controlan dos variables contextuales:

- Riesgo acumulado. Es el calculado sobre un activo teniendo en cuenta el impacto acumulado sobre un activo debido a una amenaza y la probabilidad de la amenaza
- Riesgo repercutido. Es el calculado sobre un activo teniendo en cuenta el impacto repercutido sobre un activo debido a una amenaza y la probabilidad de la amenaza.

¿Qué son las Salvaguardas?

Se definen las salvaguardas, o contra medidas, como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Ante el amplio abanico de posibles salvaguardas a considerar, es necesario hacer una criba inicial para quedarnos con aquellas que son relevantes para lo que hay que proteger. En esta criba se deben tener en cuenta los siguientes aspectos:

1. Tipo de activos a proteger, pues cada tipo se protege de una forma específica
2. Dimensión o dimensiones de seguridad que requieren protección
3. Amenazas de las que necesitamos protegernos
4. Si existen salvaguardas alternativas

Además, es prudente establecer un principio de proporcionalidad y tener en cuenta:

1. El mayor o menor valor propio o acumulado sobre un activo, centrándonos en lo más valioso y obviando lo irrelevante
2. La mayor o menor probabilidad de que una amenaza ocurra, centrándonos en los riesgos más importantes (ver zonas de riesgo)
3. La cobertura del riesgo que proporcionan salvaguardas alternativas

Esto lleva a dos tipos de declaraciones para excluir una cierta salvaguarda del conjunto de las que conviene analizar:

- no aplica – se dice cuando una salvaguarda no es de aplicación porque técnicamente no es adecuada al tipo de activos a proteger, no protege la dimensión necesaria o no protege frente a la amenaza en consideración
- no se justifica – se dice cuando la salvaguarda aplica, pero es desproporcionada al riesgo que tenemos que proteger

Como resultado de estas consideraciones dispondremos de una “declaración de aplicabilidad” o relación de salvaguardas que deben ser analizadas como componentes nuestro sistema de protección.

¿ Cómo afectan las Salvaguardas en el Ánalisis del Riesgo?

Las salvaguardas entran en el cálculo del riesgo de dos formas:

- Reduciendo la probabilidad de las amenazas. Se llaman salvaguardas preventivas. Las ideales llegan a impedir completamente que la amenaza se materialice.
- Limitando el daño causado. Hay salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance. Incluso algunas salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye. En cualquiera de las versiones, la amenaza se materializa; pero las consecuencias se limitan.

¿ Cómo se miden las Salvaguardas: Eficacia y Madurez ?

Las salvaguardas se caracterizan, además de por su existencia, por su eficacia frente al riesgo que pretenden conjurar. La salvaguarda ideal es 100% eficaz combinando 2 factores:

desde el punto de vista técnico

- es técnicamente idónea para enfrentarse al riesgo que protege
- se emplea siempre

desde el punto de vista de operación de la salvaguarda

- está perfectamente desplegada, configurada y mantenida
- existen procedimientos claros de uso normal y en caso de incidencias
- los usuarios están formados y concienciados
- existen controles que avisan de posibles fallos

Entre una eficacia del 0% para aquellas que faltan y el 100% para aquellas que son idóneas y que están perfectamente implantadas, se estimará un grado de eficacia real en cada caso concreto. Para medir los aspectos organizativos, se puede emplear una escala de madurez que recoja en forma de factor corrector la confianza que merece el proceso de gestión de la salvaguarda:

Factor	Nivel	Madurez
0%	L0	inexistente
	L1	inicial / ad hoc
	L2	reproducible, pero intuitivo
	L3	proceso definido
	L4	gestionado y medible
100%	L5	optimizado

Efecto de la Salvaguarda	Tipo de Salvaguarda
Preventivas: reducen la probabilidad	[PR] preventivas [DR] disuasorias [EL] eliminatorias
Acotan la degradación	[IM] minimizadoras [CR] correctivas [RC] recuperativas
Consolidan el efecto de las demás	[MN] de monitorización [DC] de detección [AW] de concienciación [AD] administrativas

¿Qué son las Vulnerabilidades ?

Son vulnerabilidades todas las ausencias o ineficacias de las salvaguardas pertinentes para salvaguardar el valor propio o acumulado sobre un activo. A veces se emplea el término "insuficiencia" para resaltar el hecho de que la eficacia medida de la salvaguarda es insuficiente para preservar el valor del activo expuesto a una amenaza.

¿ Qué es el Impacto Residual ?

Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de posible impacto que se denomina residual. Se dice que hemos modificado el impacto, desde un valor potencial a un valor residual.

¿ Qué es el Riesgo Residual ?

Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de riesgo que se denomina residual. Se dice que hemos modificado el riesgo, desde un valor potencial a un valor residual.

¿Existe Metodología ?

MAR.1: Caracterización de los activos

El objetivo de estas tareas es reconocer los activos que componen el sistema, definir las dependencias entre ellos, y determinar que parte del valor del sistema se soporta en cada activo. Podemos resumirlo en la expresión "conócete a ti mismo".

MAR.11: Identificación de los activos

Objetivos. Identificar los activos que componen el sistema, determinando sus características, atributos y clasificación en los tipos determinados

Productos de entrada
- Inventario de datos manejados por el sistema
- Inventario de servicios prestados por el sistema
- Procesos de negocio
- Diagramas de uso
- Diagramas de flujo de datos
- Inventarios de equipamiento lógico
- Inventarios de equipamiento físico
- Locales y sedes de la Organización
- Caracterización funcional de los puestos de trabajo

Productos de salida
- Relación de activos a considerar
- Caracterización de los activos: valor propio y acumulado
- Relaciones entre activos

Técnicas, prácticas y pautas
- Diagramas de flujo de datos
- Diagramas de procesos
- Entrevistas (ver "Guía de Técnicas")
- Reuniones

MAR.12: Dependencias entre activos

Objetivos. Identificar y valorar las dependencias entre activos, es decir la medida en que un activo de orden superior se puede ver perjudicado por una amenaza materializada sobre un activo de orden inferior

Productos de entrada
- Resultados de la tarea MAR.11, Identificación
- Procesos de negocio
- Diagramas de flujo de datos
- Diagramas de uso

Productos de salida
- Diagrama de dependencias entre activos

Técnicas, prácticas y pautas
- Diagramas de flujo de datos
- Diagramas de procesos
- Entrevistas (ver "Guía de Técnicas")
- Reuniones
- Valoración Delphi (ver "Guía de Técnicas")

MAR.13: Valoración de los activos

Objetivos. Identificar en qué dimensión es valioso el activo y valorar el coste que para la Organización supondría la destrucción del activo

Productos de entrada
- Resultados de la tarea MAR.11, Identificación de los activos
- Resultados de la tarea MAR.12, Dependencias entre activos

Productos de salida
- Modelo de valor: informe de valor de los activos

Técnicas, prácticas y pautas
- Entrevistas (ver "Guía de Técnicas") Reuniones
- Valoración Delphi (ver "Guía de Técnicas")

MAR.2: Caracterización de las amenazas

El objetivo de estas tareas es caracterizar el entorno al que se enfrenta el sistema, qué puede pasar, qué consecuencias se derivarían y cómo de probable es que pase. Podemos resumirlo en la expresión "conoce a tu enemigo".

MAR.21: Identificación de las amenazas

Objetivos Identificar las amenazas relevantes sobre cada activo

Productos de entrada
- Resultados de la actividad MAR.1, Caracterización de los activos
- Informes relativos a defectos en los productos. Esto es, informes de vulnerabilidades.

Productos de salida
- Relación de amenazas posibles

Técnicas, prácticas y pautas
- Catálogos de amenazas (ver "Catálogo de Elementos")
- Árboles de ataque (ver "Guía de Técnicas")
- Entrevistas (ver "Guía de Técnicas")
- Reuniones
- Valoración Delphi (ver "Guía de Técnicas")

MAR.22: Valoración de las amenazas

Objetivos. Estimar la frecuencia de ocurrencia de cada amenaza sobre cada activo y estimar la degradación que causaría la amenaza en cada dimensión del activo si llegara a materializarse

Productos de entrada
- Resultados de la tarea MAR2.1, Identificación de las amenazas
- Series históricas de incidentes
- Informes de defectos en los productos
- Antecedentes: incidentes en la Organización

Productos de salida
- Mapa de riesgos: informe de amenazas posibles, caracterizadas por su frecuencia de ocurrencia y la degradación que causarían en los activos

Técnicas, prácticas y pautas
- Árboles de ataque (ver "Guía de Técnicas")
- Entrevistas (ver "Guía de Técnicas")
- Reuniones
- Valoración Delphi (ver "Guía de Técnicas")

La siguiente tabla muestra el mapa metodológico de las actividades, productos y técnicas que hay que llevar a cabo para completar la fase de análisis del Riesgo.

MAR.3: Caracterización de las salvaguardas

El objetivo de estas tareas es doble: saber qué necesitamos para proteger el sistema y saber si tenemos un sistema de protección a la altura de nuestras necesidades.

MAR.31: Identificación de las salvaguardas pertinentes

Objetivos. Identificar las salvaguardas convenientes para proteger el sistema

Productos de entrada
- Modelo de activos del sistema
- Modelo de amenazas del sistema
- Indicadores de impacto y riesgo residual
- Informes de productos y servicios en el mercado

Productos de salida
- Declaración de aplicabilidad: relación justificada de las salvaguardas necesarias
- Relación de salvaguardas desplegadas

Técnicas, prácticas y pautas
- Catálogos de salvaguardas (ver "Catálogo de Elementos")
- Árboles de ataque (ver "Guía de Técnicas")
- Entrevistas (ver "Guía de Técnicas")
- Reuniones

MAR.32: Valoración de las salvaguardas

Objetivos. Determinar la eficacia de las salvaguardas pertinentes

Productos de entrada
- Inventario de salvaguardas derivado de la tarea MAR.31

Productos de salida
- Evaluación de salvaguardas: informe de salvaguardas desplegadas, caracterizadas por su grado de efectividad
- Informe de insuficiencias (o vulnerabilidades): relación de salvaguardas que deberían estar pero no están desplegadas o están desplegadas de forma insuficiente

Técnicas, prácticas y pautas
- Entrevistas (ver "Guía de Técnicas")
- Reuniones
- Valoración Delphi (ver "Guía de Técnicas")

MAR.4: Estimación del estado de riesgo

El objetivo de estas tareas es disponer de una estimación fundada de lo que puede ocurrir (impacto) y de lo que probablemente ocurra (riesgo).

MAR.41: Estimación del impacto

Objetivos. Determinar el impacto potencial al que está sometido el sistema y determinar el impacto residual al que está sometido el sistema

Productos de entrada
- Resultados de la actividad MAR.1, Caracterización de los activos
- Resultados de la actividad MAR.2, Caracterización de las amenazas
- Resultados de la actividad MAR.3, Caracterización de las salvaguardas

Productos de salida
- Informe de impacto (potencial) por activo
- Informe de impacto residual por activo

Técnicas, prácticas y pautas
- Análisis mediante tablas (ver "Guía de Técnicas")
- Análisis algorítmico (ver "Guía de Técnicas")

MAR.42: Estimación del riesgo

Objetivos. Determinar el riesgo potencial al que está sometido el sistema y determinar el riesgo residual al que está sometido el sistema

Productos de entrada
- Resultados de la actividad MAR.1, Caracterización de los activos
- Resultados de la actividad MAR.2, Caracterización de las amenazas
- Resultados de la actividad MAR.3, Caracterización de las salvaguardas
- Resultados de la actividad MAR.4, Estimaciones de impacto

Productos de salida
- Informe de riesgo (potencial) por activo
- Informe de riesgo residual por activo

Técnicas, prácticas y pautas
- Análisis mediante tablas (ver "Guía de Técnicas")
- Análisis algorítmico (ver "Guía de Técnicas")

El Tratamiento del Riesgo

A la vista de los impactos y riesgos a que está expuesto el sistema, hay que tomar una serie de decisiones condicionadas por la gravedad de los mismos y por las obligaciones a las que esté sometida la Organización por ley, reglamento sectorial o por contrato

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 y requiere atención urgente
2. Es grave y 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

Las opciones 1,2 y 3 requieren tratamiento técnico del riesgo.

La opción 4, aceptación del riesgo, siempre es arriesgada y hay que tomarla con prudencia y justificación cuando el impacto y el riesgo residual es asumible o cuando el coste de las salvaguardas oportunas es desproporcionado en comparación al impacto y riesgo residuales.

El Proceso de Evaluación

Impacto y riesgo residual son una medida del estado presente, desde 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.

Aceptación de los Riesgos

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

Para tomar una u otra decisión hay que enmarcar los riesgos soportados por el sistema de información dentro de un contexto más amplio que evalúe los aspectos intangibles del negocio.

Tratamiento de los riesgos

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)

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.

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.

Eliminación del Riesgo

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. 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.

Mitigación del Riesgo

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 se traducen en el despliegue de más equipamiento. Estos nuevos activos estarán a su vez sujetos a amenazas que pueden perjudicar a los activos esenciales. Hay 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.

Compartición del 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 en la 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.

Financiación del Riesgo

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.

Técnicas de valoración y estimación del Riesgo

En la documentación oficial de Magerit, existe un documento específico con la descripción de las principales técnicas utilizadas en el proceso de Gestión de Riesgos.

Se considera técnica a un conjunto de algoritmos heurísticos y procedimientos que ayudan a alcanzar los objetivos propuestos.

Todas las técnicas pueden utilizarse sin ayudas automatizadas, pero su aplicación repetitiva o compleja recomienda el empleo de herramientas específicas para facilitar la homogeneización de las mismas en todo el proceso.

En la guía se describen dos tipos de técnicas:

las específicas de los proyectos de análisis y gestión de riesgos, que no se utilizan en otros contextos de trabajo, como son:

- uso de tablas para la obtención sencilla de resultados
- técnicas algorítmicas para la obtención de resultados elaborados
- árboles de ataque para complementar los razonamientos de qué amenazas se ciernen sobre un sistema de información

otras técnicas generales, de propósito más amplio al mero análisis de riesgos, pero que son identificadas a lo largo de la metodología del proceso, como son:

- técnicas gráficas: histogramas, diagramas de Pareto y de tarta
- sesiones de trabajo: entrevistas, reuniones y presentaciones
- valoraciones Delphi

Cada una de estas técnicas se describen brevemente en los siguientes apartados. Para un mayor detalle se aconseja acudir al Libro III del Método Magerit - Guía de Técnicas.

Análisis mediante tablas

En el análisis de riesgos hay que trabajar con múltiples elementos que hay que combinar en un sistema para ordenarlo por importancia sin que los detalles, muchos, perjudiquen la visión de conjunto.

La experiencia ha demostrado la utilidad de métodos simples de análisis llevados a cabo por medio de tablas que, sin ser muy precisas, sí aciertan en la identificación de la importancia relativa de los diferentes activos sometidos a amenazas.

Sea la escala siguiente útil para calificar el valor de los activos, la magnitud del impacto y la magnitud del riesgo: MB: muy bajo; B: bajo; M: medio; A: alto; MA: muy alto.

Se puede calcular el impacto en base a tablas sencillas de doble entrada, en función del valor del

activo y del porcentaje de degradación

		Degradación		
		1%	10%	100%
Valor del Activo	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Y a partir de ahí calculamos el riesgo en función de otra tabla de doble entrada entre el impacto y la probabilidad:

		Probabilidad				
		Muy raro	Poco probable	Posible	Probable	Casi Seguro
Impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Algoritmo Cualitativo

En este modelo se posicionan los activos en una escala de valor relativo, definiendo arbitrariamente un valor “v0” como frontera entre los valores que preocupan y los que son despreciables.

Sobre esta escala de valor se mete tanto el valor del activo, propio o acumulado, como el impacto de una amenaza cuando ocurra y el riesgo al que está expuesto.

Mientras el impacto mide el valor de la desgracia potencial, el riesgo pondera ese impacto con la frecuencia estimada de ocurrencia de la amenaza. El impacto es la medida del coste si ocurriera mientras que el riesgo mide la exposición en un determinado periodo de tiempo.

Las estimaciones de impacto y riesgo residual incorporan la eficacia de las salvaguardas para enfrentarse a la amenaza, bien limitando el impacto, bien reduciendo la probabilidad.

El modelo combina los siguientes parámetros de análisis:

- calibración del valor del activo por medio de una escala discreta
- calibración de la degradación que supone una amenaza como un porcentaje
- calibración de la probabilidad de ocurrencia de la amenaza por medio de una escala discreta
- vertebración de un paquete de salvaguardas
- calibración de la eficacia de las salvaguardas por medio de un porcentaje

Parámetros todos ellos que permiten moverse arriba y abajo por las escalas de valores.

Algoritmo Cuantitativo

Se modela el grado de dependencia entre activos como un continuo entre 0,0 (activos independientes) y 1,0 (activos absolutamente dependientes; lo que ocurre sobre el inferior repercute contundentemente sobre el superior).

Se mide tanto el valor del activo, propio o acumulado, como el impacto de una amenaza cuando ocurra y el riesgo que supone.

Mientras el impacto mide el valor de la desgracia potencial, el riesgo pondera ese impacto con la frecuencia estimada de ocurrencia de la amenaza. El impacto mide el coste si ocurriera mientras que el riesgo es la medida de la exposición en un periodo de tiempo.

Si la valoración del activo es económica (coste monetario que significaría su pérdida total y absoluta), el impacto calculado es el coste inducido por la amenaza y el riesgo calculado es la cantidad que hay que prever como pérdidas anuales. El modelo cuantitativo permite pues comparar el gasto en salvaguardas con la disminución de pérdidas.

Las estimaciones de impacto y riesgo residual incorporan la eficacia de las salvaguardas para enfrentarse a la amenaza.

Si la valoración del activo es económica, el modelo cuantitativo permite comparar el gasto en salvaguardas con la disminución de pérdidas.

El modelo pues combina los siguientes parámetros de análisis:

- calibración del valor del activo por medio de una cantidad numérica
- calibración de la dependencia entre activos por medio de un porcentaje
- calibración de la degradación que supone una amenaza por medio de un porcentaje
- calibración de la frecuencia de ocurrencia de la amenaza por medio de una frecuencia
- vertebración de un paquete de salvaguardas
- calibración de la eficacia de las salvaguardas por medio de un porcentaje

Parámetros todos ellos que permiten moverse arriba y abajo por la escala de valores.

Ejemplo.

Sea un activo valorado en 1.000.000, que es víctima de una amenaza que lo degrada un 90%. El impacto es de cuantía

impacto = 1.000.000 x 90% = 900.000

Si la frecuencia anual estimada es de 0,1, el riesgo es de cuantía

riesgo = 900.000 x 0,1 = 90.000 = pérdida anual estimada

Si las salvaguardas tienen un 90% de eficacia sobre el impacto, el impacto residual es

impacto residual = 900.000 x (1 – 90%) = 90.000

Si las salvaguardas tienen un 50% de eficacia sobre la frecuencia, la eficacia combinada de las salvaguardas es

frecuencia residual = 0,1 x (1 – 50%) = 0,05

y el riesgo residual es

riesgo residual = 90.000 * 0,05 = 4.500 (pérdida anual estimada)

Si las cantidades son euros y las frecuencias anuales, la pérdida posible es de 90.000 euros y la pérdida anual se estima en 4.500 euros.

Árboles de ataque

Los árboles de ataque son una técnica para modelar las diferentes formas de alcanzar un objetivo. Aunque han existido durante años con diferentes nombres, se hicieron famosos a partir de los trabajos de B. Schneier que propuso sus sistematización en el área de los sistemas de información.

El objetivo del atacante se usa como raíz del árbol. A partir de este objetivo, de forma iterativa e incremental se van detallando como ramas del árbol las diferentes formas de alcanzar aquel objetivo, convirtiéndose las ramas en objetivos intermedios que a su vez pueden refinarse. Los posibles ataques a un sistema se acaban modelando como un bosque de árboles de ataque.

Veamos un ejemplo ilustrativo sobre como usar fraudulentamente (sin pagar) un servicio de pago.

Ejemplo

1. Objetivo: usar sin pagar (OR)
    1. suplantar la identidad de un usuario legítimo
    2. soslayar la identificación de acceso al servicio
    3. abusar del contrato (AND)
        1. ser un usuario legítimo
        2. conseguir que no se facture el servicio (OR)
            1. que no queden trazas de uso
            2. que se destruyan las trazas antes de facturación (OR)
                1. las destruyo yo
                2. engaño al operador para que las borre
                3. manipulo del sw para que no las sume
            3. repudiar las trazas
            4. dar datos de cargo falsos

Lo más habitual para alcanzar un objetivo o subobjetivo es que se disponga de varias maneras alternativas (nodos OR); aunque en ocasiones se requiere la concurrencia de varias actividades (nodos AND). En conjunto, se consigue un esquema de las diferentes maneras en las que un usuario podría usarlo sin pagar por ello.

Identificadas las diferentes maneras de alcanzar un objetivo, los nodos del árbol se pueden enriquecer con información de detalle, que puede ser de muy diferentes tipos; por ejemplo:

- conocimientos que se requieren del atacante: cualquiera, alguna experiencia, un ingeniero, un hacker profesional, etc.
- inversión del atacante: cantidad de dinero y tiempo que tendría que desembolsar para realizar la acción
- riesgo para el atacante: si es capturado, ¿qué consecuencias afrontaría?

Si la información del árbol con estos atributos se procesa automáticamente, podemos obtener escenarios simplificados de ataque:

- usuarios inexpertos pero con bastante dinero
- atacantes profesionales pero sin capacidad de inversión (o sin necesidad de realizar una inversión adicional para perpetrar este ataque)

- atacantes que quedarían impunes
- etc.

Para alcanzar estos escenarios especializados basta eliminar del árbol las ramas que no satisfagan una condición cualitativa o cuantitativa. Sobre un árbol con atributos es posible determinar el ataque más probable, simplemente extrayendo aquel ataque que requiere menos medios y menos conocimiento por parte del atacante. También es posible determinar cuál será la línea de acción de un posible perfil de atacante (que se determina en base al tipo de servicio o información que estamos protegiendo): aquel que con menos coste satisfaga los conocimientos mínimos para realizar el ataque.

Cuando se han desplegado salvaguardas, su efecto puede reflejarse sobre el árbol de ataque:

- incrementando el conocimiento que el atacante necesitaría para alcanzar su objetivo pese a las salvaguardas desplegadas: idealmente debería ser imposible por mucho que supiera
- incrementando el desembolso que el atacante tendría que realizar para alcanzar su objetivo a la vista de las salvaguardas desplegadas: idealmente el coste debería ser superior al beneficio para el atacante

Un sistema ideal de salvaguardas eliminaría todas las ramas del árbol. Un sistema real suele llevar los atributos a niveles elevados de conocimiento e inversión que reducen la posibilidad de que el ataque se materialice a un nivel residual aceptado por la Dirección.

Los árboles de ataque constituyen una documentación extremadamente valiosa para un atacante, especialmente cuando incorporan el estado actual de salvaguardas, pues facilitan en extremo su trabajo. Por ello deberán extremarse las medidas de protección de su confidencialidad.

Su principal inconveniente se encuentra en que es explosivo por la cantidad de árboles y detalle que pueden ser necesarios para recopilar todas las amenazas posibles sobre un sistema medianamente complejo. Por ello cabe esperar su uso como complemento a un análisis de riesgos, permitiendo profundizar en algunas líneas de ataque y dramatizar sus consecuencias.

Valoración Delphi

Es una técnica netamente cualitativa que relativamente permite tratar con alta precisión problemas técnicamente complejos.

Está planteada como una reflexión organizada de expertos sobre un tema concreto, reflexión que permite recoger las ideas y opiniones más cualificadas en el ámbito de la seguridad (valoración de activos e identificación de amenazas e impactos).

Se desarrolla a partir de un cierto escenario inicia‘ de modo que permita una adecuada recapitulación e identificación de los problemas que ya existen actualmente.

Desarrolla una prospectiva mucho más rica que la mera identificación de la opinión mayoritaria, por medio de un proceso de convergencia de opiniones que se consigue mediante rondas

sucesivas de entrevistas.

Garantiza satisfactoriamente la limpieza de la investigación, impidiendo el predominio de unos expertos sobre otros por razones ajenas a la calidad de sus opiniones.

La técnica Delphi es un instrumento de uso múltiple que se utiliza con muy variados objetivos:

- Identificar problemas.
- Desarrollar estrategias para la solución de problemas, fijando un rango de alternativas posibles.
- Identificar factores de resistencia en el proceso de cambio.
- Establecer previsiones de futuro sobre la evolución de las tendencias que se observan en un determinado campo o sector.
- Contrastar opiniones en un tema abarcando un amplio campo de disciplinas o sectores.

El procedimiento es como sigue:

1. Se prepara un cuestionario con los temas cuya valoración se desea conocer. Este punto es crítico para el éxito de los siguientes pasos. Para la elaboración de un buen cuestionario se requiere experiencia y conocimiento del tema que se desea investigar.
2. Se distribuye entre los sujetos que tienen una opinión relevante en el tema a investigar: los expertos.
3. Con las respuestas recibidas, se prepara un histograma indicando cuántos entrevistados se decantan por cada nivel de valoración.
4. Si hay una clara concentración de respuestas en torno a un único valor, el proceso ha acabado: hay un claro consenso en el valor buscado.
5. Si hay diferencias importantes de opinión, se remite de nuevo el mismo cuestionario; pero esta vez acompañado del histograma. Si se han apreciado ambigüedades en el primer cuestionario, deben aclararse en esta segunda ronda. A los entrevistados se les inquiere sobre si consideran que deben mantener su primera opinión o prefieren modificarla.
6. Si el histograma de esta segunda ronda sigue sin mostrar una respuesta clara, se pueden realizar nuevas rondas o convocar a los entrevistados en una reunión conjunta para llegar a un consenso.
7. Ante un histograma disperso, siempre hay que preguntarse si se ha hecho la pregunta correcta a las personas correctas, si la pregunta estaba claramente expresada o si, por el contrario se debe volver a empezar con nuevas preguntas y/o nuevos entrevistados.

El Esquema Nacional de Seguridad y la Gestión de Riesgos

Hasta la aparición del Esquema Nacional de Seguridad, la Gestión de Riesgos se consideraba una buena práctica identificada en las principales certificaciones de calidad, y gestión de la seguridad.

El análisis y gestión de los riesgos es un aspecto clave del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad.

Este RD, de obligado cumplimiento por las administraciones públicas en el ejercicio del acceso electrónico de los ciudadanos a la administración, implica que los sistemas bajo su ámbito deben estar obligatoriamente sujetos a una gestión activa de riesgos por parte de las organizaciones.

Esto convierte a Magerit en una metodología de Gestión de Riesgos que deben implantar las administraciones públicas en el ejercicio de sus funciones TIC.

Como ya se ha indicado anteriormente, la metodología y sus técnicas, pueden ser aplicadas - si así se desea - de forma manual, aunque lo más conveniente es utilizar herramientas diseñadas y preparadas para implantar el método de una forma homogénea en el tiempo.

Pilar/EAR es una herramienta que implementa la metodología MAGERIT de análisis y gestión de riesgos, desarrollada por el Centro Criptológico Nacional (CCN) y de amplia utilización en la administración pública española.

Se puede descargar del Portal del CCN-CERT en https://www.ccn-cert.cni.es.

Los organismos de la administración pública española pueden solicitar una licencia libre de cargos al Centro Criptológico Nacional.

En Pilar / EAR se analizan los riesgos en varias dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad (accountability). Para tratar el riesgo se proponen

- salvaguardas (o contramedidas)
- normas de seguridad
- procedimientos de seguridad

analizándose el riesgo residual a lo largo de diversas etapas de tratamiento.

La última versión incorpora, entre otras características:

- Perfil de evaluación para el Esquema Nacional de Seguridad.
- Perfiles de evaluación con control de aplicabilidad y obligatoriedad.
- Activos esenciales y valoración de dominios por activos esenciales.
- Salvaguardas para reflejar el uso de productos o algoritmos certificados.
- Biblioteca actualizada y ampliada de salvaguardas.

Contactos

José María Rodríguez
Socio / Director
+34 650 592 012
jmrodriguez@tithink.com
@chemapostigo

Ignacio Peralta
Socio / Director
+34 608 791 117
iperalta@tithink.com
@iperaltal

Sobre tiThink

En tiThink enfocamos nuestro asesoramiento hacia la Transformación del Comportamiento Tecnológico de las compañías, ayudándolas a alcanzar la madurez corporativa en la aplicación eficiente de las Tecnologías.

Somos una compañía de consultoría estratégica y servicios de seguridad de información, que ayuda a proteger y generar valor a sus clientes apalancando el cumplimiento de sus objetivos estratégicos, mediante el uso de metodologías estructuradas y adaptables.

Tenemos como meta, ser reconocidos como una empresa de consultoría con un portafolio de servicios de calidad, excelencia y respuesta integral. Además, deseamos ser percibidos como un aliado estratégico, representado en un excelente retorno de la inversión a través de la generación de valor y con un alto nivel de satisfacción de sus clientes, empleados y socios.

En el ámbito del Esquema Nacional de Seguridad desde tiThink te podemos ayudar en:

- Evaluar el “estado del arte” y definir el plan director o la hoja de ruta para la adecuación al ENS.
- Definir y formalizar las Políticas de Seguridad de la información, sus normas y su modelo organizativo.
- Catalogar los sistemas y servicios bajo tu responsabilidad y definir la Declaración de Aplicabilidad de medidas.
- Implantar la metodología de gestión de riesgos tecnológicos.
- Acompañar en el proceso de implantación de medidas de seguridad: selección de herramientas, definición de procedimientos, supervisión de proyectos de implantación de herramientas, etc.
- Realizar auditorías y pruebas de seguridad de los sistemas.
- Tutelar el proceso de adecuación al ENS bajo la figura de Oficina de Proyectos.

www.tithink.com