2. BASE TEÓRICA

2.1. Introducción

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) va a ser el referente teórico usado para el desarrollo del proyecto, ya que es la metodología seguida en la empresa donde se implantará la aplicación (Isotrol).

A continuación se hace una breve introducción de la metodología usada así como una extracción de los conceptos más interesantes.

2.2. MAGERIT

El Consejo Superior de Administración Electrónica (CSAE) ha elaborado Magerit como respuesta a la percepción de que la Administración, y en general la sociedad, depende de forma creciente de las tecnologías de la información para la consecución de sus objetivos de servicio. La razón de ser de Magerit está directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemático, que supone unos beneficios evidentes, pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en el uso de tales medios.

Esta metodología interesa a todos aquellos que trabajan con información mecanizada y los sistemas informáticos que la tratan. Si dicha información o los servicios que se prestan gracias a ella son valiosos, esta metodología les permitirá saber cuánto de este 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. El gran reto al que nos enfrentamos, es que hay muchos elementos que considerar y que, si no se es riguroso, las conclusiones serán de poco fiar. Es por ello que se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

2.3. Introducción al análisis y gestión de riesgos

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

Las tareas de análisis y gestión de riesgos no son un fin en sí mismas sino que se encajan en la actividad continua de gestión de la seguridad.

El análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegidos se encuentran los activos. En coordinación con los objetivos, estrategia y política de la organización, las actividades de gestión de riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que se acepta en la Dirección.

La implantación de los controles de seguridad requiere una organización gestionada y la participación informada de todo el personal que trabaja con el sistema de información. Es este personal el responsable de la operación diaria, de la reacción ante incidencias y de la monitorización en general del sistema para determinar si satisface con eficacia y eficiencia los objetivos propuestos.

Este esquema de trabajo debe ser repetitivo pues los sistemas de información rara vez son inmutables; más bien se encuentran sometidos a evolución continua tanto propia (nuevos activos) como del entorno (nuevas amenazas), lo que exige una revisión periódica en la que se aprende de la experiencia y se adapta al nuevo contexto.

El análisis de riesgos proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas, y es la piedra angular para controlar todas las actividades con fundamento. La gestión de riesgos es la estructuración de las acciones de seguridad para satisfacer las necesidades detectadas por el análisis.

2.4. ¿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 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 datos no están bien ordenados en términos relativos, su interpretación es imposible.

En resumen, que 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.

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 de la actividad, pasando por las decisiones de adquisición de salvaguardas técnicas y de selección y capacitación del personal.

Por precepto legal

El análisis de riesgos puede venir requerido por precepto legal. Tal es el caso del Real Decreto 263/1996, de 16 de Febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado. En su artículo 4 (Garantías generales de la utilización de soportes, medios y aplicaciones electrónicas, informáticas y telemáticas) dice así:

> *"Cuando se utilicen los soportes, medios y aplicaciones referidos en el apartado anterior, se adoptarán las medidas técnicas y de organización necesarias que aseguren la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información. Dichas medidas de seguridad deberán tener en cuenta el estado de la tecnología y ser proporcionadas a la naturaleza de los datos y de los tratamientos y a los riesgos a los que estén expuestos."*

De forma similar, en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, en su artículo 9 (Seguridad de los datos) dice así:

> *"El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural."*

Texto que se recoge de nuevo en el preámbulo al 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. En este decreto se recoge la obligación de elaborar un documento de seguridad:

> *"El responsable del fichero elaborará e implantará la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información."*

Difícilmente se puede desarrollar dicho documento sin un análisis previo de los riesgos sobre los datos, análisis que nos lleve a determinar las medidas de seguridad pertinentes.

En conclusión, se procede a 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.

2.5. Realización del análisis y de la gestión

Este apartado expone de forma conceptual en qué consiste el análisis de riesgos y su gestión, qué se busca en cada momento y qué conclusiones se derivan.

Hay dos grandes tareas a realizar:

- Análisis de Riesgos
- Gestión de Riesgos

- **Análisis de riesgos**, que permite determinar qué elementos forman parte o afectan a la organización, y estima qué eventos pueden tener lugar.

  Elementos:

  1. *activos*, que son los elementos del sistema de información (o estrechamente relacionados con éste) que aportan valor a la organización.
  2. *amenazas*, que son eventos que pueden afectar negativamente a los activos causando un perjuicio a la organización.
  3. *salvaguardas* (controles o contra medidas), que son elementos de defensa desplegados 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.

- **Gestión de riesgos,** que permite organizar la defensa concienzuda y prudentemente, protegiendo 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.

  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.

Nota:
En este proyecto nos centraremos en el análisis de riesgos exclusivamente, dejando la labor de la gestión de riesgos al equipo de seguridad de la empresa, que sacará las conclusiones pertinentes tras la evaluación de los resultados obtenidos en el primer paso.

2.6. Análisis de Riesgos

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 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 expectación de materialización) de la amenaza.

La siguiente figura recoge este primer recorrido, cuyos pasos se detallan en los siguientes apartados:

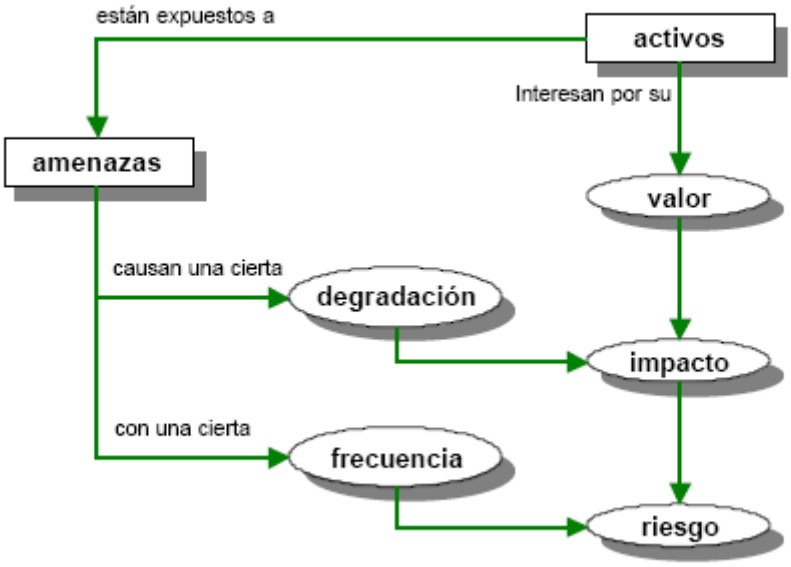


Ilustración 2.1

2.6.1. Paso 1: Activos

Se denominan activos los recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente.

El activo esencial es la información que maneja el sistema; o sea los datos. Y alrededor de estos datos se pueden identificar otros activos relevantes:

- Los servicios que se pueden prestar gracias a aquellos datos, y los servicios que se necesitan para poder gestionar dichos datos.
- 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.

Dependencias

Los activos más llamativos suelen ser los datos y los servicios; pero estos 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 medida en que un activo *superior* se vería afectado por un incidente de seguridad en un activo *inferior*.

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. O, dicho en otras palabras, cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior. Informalmente puede interpretarse que los activos inferiores son los pilares en los que se apoya la seguridad de los activos superiores.

Valoración

Valor propio de un activo se refiere a la estimación numérica de la importancia que tiene dicho bien para la organización.

En el valor acumulado, se considera tanto el valor propio de un activo como el valor de los activos que dependen de él. Se dice que los activos inferiores en un esquema de dependencias, acumulan el valor de los activos que se apoyan en ellos.

Así:

Valor acumulado (B) = Σ valoración (Ai) * dependencia (Ai→ B)

En un árbol de dependencias, donde los activos superiores dependen de los inferiores, es imprescindible valorar los activos superiores, los que son importantes por sí mismos. Automáticamente este valor se acumula en los inferiores, lo que no es óbice para que también puedan merecer, adicionalmente, su valoración propia.

Dimensiones

Un aspecto, diferenciado de otros posibles aspectos, respecto del que se puede medir el valor de un activo en el sentido del perjuicio que causaría su pérdida de valor. De un activo puede interesar calibrar las siguientes dimensiones:

Disponibilidad: Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

Integridad: Garantía de la exactitud y completitud de la información y los métodos de su procesamiento. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una organización

Confidencialidad: Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso. Previene contra la divulgación no autorizada de activos, fugas y filtraciones de información, así como 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 leyes y compromisos contractuales relativos a la custodia de los datos.

Autenticidad: Aseguramiento de la identidad u origen. Esta valoración es típica de servicios (autenticidad del usuario) y de los datos (autenticidad de quien accede a los datos para escribir o, simplemente, consultar). Logra conseguir 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 se dan suplantaciones y engaños que buscan realizar un fraude. La autenticidad es la base para poder luchar contra el repudio y, como tal, fundamenta el comercio electrónico o la administración electrónica, permitiendo confiar sin papeles ni presencia física.

Trazabilidad: Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. Se puede calibrar tanto la trazabilidad del uso del servicio (¿qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo?), como la trazabilidad del acceso a los datos (¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?).

2.6.2. Paso 2: Amenazas

El siguiente paso consiste en determinar las amenazas que pueden afectar a cada activo. Las amenazas son eventos que pueden provocar daños en los activos. Y, de todo lo que puede ocurrir, 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 el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos. Hay amenazas causadas por las personas, bien errores, bien ataques intencionados.

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.

Valoración de las amenazas

Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía. Una vez determinado que una amenaza puede perjudicar a un activo, hay que estimar cuán vulnerable es el activo, en dos sentidos:

- *degradación*: pérdida de valor de un activo como consecuencia de la materialización de una amenaza.
- *frecuencia*: tasa de ocurrencia de una amenaza.

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera. 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".

Cuando las amenazas no son intencionales, probablemente baste conocer la fracción físicamente perjudicada de un activo para calcular la pérdida proporcional de valor que se pierde. Pero cuando la amenaza es intencional, no se puede pensar en proporcionalidad alguna pues el atacante puede causar muchísimo daño de forma selectiva.

La frecuencia pone en perspectiva aquella degradación, pues una amenaza puede ser de terribles consecuencias pero de muy improbable materialización; mientras que otra amenaza puede ser de muy bajas consecuencias, pero tan frecuente como para acabar acumulando un daño considerable. La frecuencia se modela como una tasa anual de ocurrencia, siendo valores típicos:

100	muy frecuente	a diario
10	frecuente	mensualmente
1	normal	una vez al año
1/10	poco frecuente	cada varios años

Ilustración 2.2

2.6.3. Paso 3: Determinación del impacto

Se denomina impacto a la medida del daño que sobre un activo tiene la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que éstas tendrían sobre el sistema.

La única consideración que queda hacer es relativa a las dependencias entre activos. Es frecuente que el valor del sistema de información se centre en los servicios que presta y los datos que maneja, al tiempo que las amenazas suelen materializarse en los medios.

Impacto acumulado de una amenaza sobre un activo

Es la pérdida de valor acumulado de un activo. Se calcula teniendo en cuenta:

- su valor acumulado (el propio más el acumulado de activos que dependen de él).
- las amenazas a que está expuesto.

El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada.

El impacto es tanto mayor:

- cuanto mayor es el valor propio o acumulado sobre un activo.
- cuanto mayor sea la degradación del activo atacado.

Así:

Impacto acumulado de una amenaza Z sobre un activo A = valor acumulado del activo A* degradación que sufre activo A debido a la amenaza Z

Impacto repercutido de una amenaza sobre un activo

Es el calculado sobre un activo teniendo en cuenta:

- su valor propio.
- las amenazas a que están expuestos los activos de los que depende.

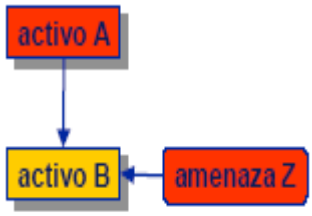
El impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio y de la degradación causada.

El impacto es tanto mayor:

- cuanto mayor es el valor propio de un activo.
- cuanto mayor sea la degradación del activo atacado.
- cuanto mayor sea la dependencia del activo atacado.

Así:

Impacto Repercutido de una amenaza Z sobre un activo A = Σ [valor propio de A*degradación que Z provoca en el activo B * grado (A→B)]



2.6.4. Paso 4: Determinación del riesgo

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la frecuencia de ocurrencia. El riesgo crece con el impacto y con la frecuencia.

Riesgo acumulado

Dícese del calculado tomando en consideración el valor propio de un activo y el valor de los activos que dependen de él. Este valor se combina con la degradación causada por una amenaza y la frecuencia estimada de la misma.

Así pues, es necesario tener en cuenta:

- el impacto acumulado sobre un activo debido a una amenaza y
- la frecuencia de la amenaza.

El riesgo acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado, la degradación causada y la frecuencia de la amenaza.

Así:

Riesgo Acumulado = Impacto Acumulado * frecuencia

Riesgo repercutido

Dícese del calculado tomando en consideración únicamente el valor propio de un activo. Este valor se combina con la degradación causada por un amenaza y la frecuencia estimada de la misma, medidas ambas sobre activos de los que depende.

Así pues, es necesario tener en cuenta:

- el impacto repercutido sobre un activo debido a una amenaza y
- la frecuencia de la amenaza.

El riesgo repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio, la degradación causada y la frecuencia de la amenaza.

Así:

Riesgo Repercutido = Impacto Repercutido * frecuencia

2.6.5. Paso 5: Salvaguardas

Se definen las salvaguardas, contra medidas o controles como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjuran

simplemente organizándose adecuadamente, otras requieres elementos técnicos (programas o equipos), otras seguridad física y, por último, está la política de personal.

En los pasos anteriores no se han tomado en consideración las salvaguardas desplegadas. Se miden, por tanto, los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto. En la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las salvaguardas presentes.

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

> *Reduciendo la frecuencia 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.

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

- es teóricamente idónea
- está perfectamente desplegada, configurada y mantenida
- se emplea siempre
- 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 están de adorno y el 100% para aquellas que son perfectas, se estimará un grado de eficacia real en cada caso concreto.

2.6.6. Revisión del paso 3: impacto residual

Es el impacto remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información. Si se han hecho todos los deberes a la perfección, el impacto residual debe ser despreciable. Si hay deberes a medio hacer (normas imprecisas, procedimientos incompletos, salvaguardas inadecuadas o insuficientes, o controles que no controlan) entonces se dice que el sistema permanece sometido a un impacto residual.

El cálculo del impacto residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación, se repiten los cálculos de impacto con este nuevo nivel de degradación.

La magnitud de la degradación tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

El impacto residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

Así:

Impacto Residual = Impacto * (1- eficacia de las salvaguardas frente al impacto)

2.6.7. Revisión del paso 4: riesgo residual

Es el riesgo remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información. Si se han hecho todos los deberes a la perfección, el riesgo residual debe ser despreciable. Si hay deberes a medio hacer (normas imprecisas, procedimientos incompletos, salvaguardas inadecuadas o insuficientes, o controles que no controlan) entonces se dice que el sistema permanece sometido a un riesgo residual.

El cálculo del riesgo residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación y la frecuencia de las amenazas, se repiten los cálculos de riesgo usando el impacto residual y la nueva tasa de ocurrencia.

La magnitud de la degradación se toma en consideración en el cálculo del impacto residual. La magnitud de la frecuencia tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

El riesgo residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

Así:

Riesgo Residual = Impacto Residual * Frecuencia Residual

Donde,

Frecuencia Residual = Frecuencia * (1- eficacia de la salvaguarda frente a la frecuencia)

El diagrama que ilustra todas estas relaciones es el siguiente:

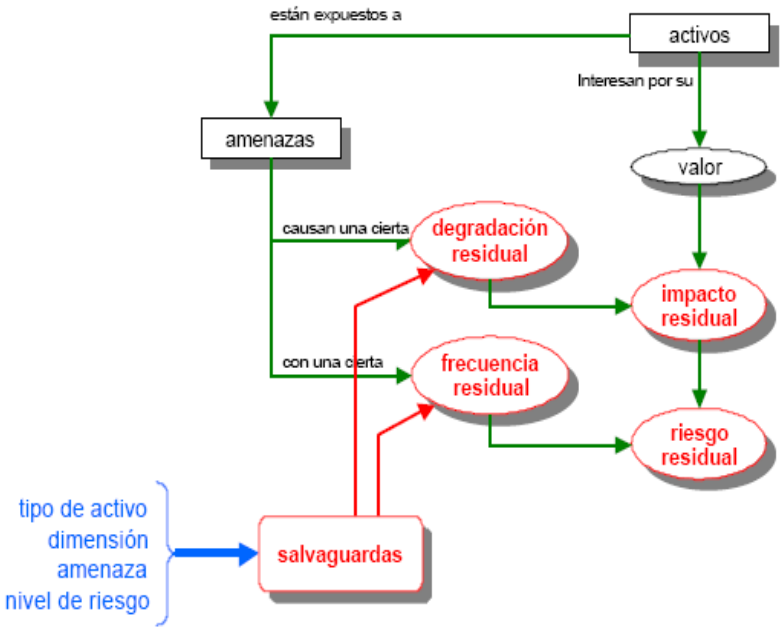


Ilustración 2.3

2.7. Referencia de otras alternativas

2.7.1. Metodologías alternativas

Algunas de las posibles metodologías para el análisis y la gestión de riesgos que nos podemos encontrar en la actualidad son:

- MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), promovida por el Ministerio de Administraciones Públicas de España.

- EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité). Metodología de gestión de los riesgos de seguridad de sistemas de información desarrollada por la "Direction Centrale de la Sécurité des Systèmes d'Information" francesa.

- CRAMM (CCTA Risk Analysis and Management Method). Metodología y herramienta de análisis y gestión de riesgos desarrollada por la "Central Computer and Telecommunications Agency" del Reino Unido y gestionada por "Insight Consulting Limited" (Grupo Siemens).

- MEHARI (Méthode Harmonisée d'Analyse de Risques). Método de análisis y gestión del riesgo desarrollado por el Clusif (Club de la Sécurité des Systèmes d'Information Français).

- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation). Metodología de evaluación de riesgos desarrollada por el Software Engineering Institute (SEI) de la Carnegie Mellon University.

- Risk management guide for information technology systems. Publicada por NIST (National Institute of Standards and Technology) de EEUU.

2.7.2. Normativas de Referencia

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

- ISO/IEC 17799:2005 Controles de Seguridad

- ISO 17799, Código de Prácticas para Gestión de la Seguridad de la Información. Áreas de cobertura, objetivos de control, y controles. Controles claves.

- La nueva familia 27000 alrededor de la ISO 27001 como norma de implementación de un SGSI; gestión de riesgos, métricas y mediciones.

- ISO 13335 (GMITS), ISO 18044 (Incidentes), ISO 21827 (Madurez de Sistemas de Información), ISO 15408 (CC, Criterios Comunes).

- ISO 27001. Estructura del Sistema de Gestión de Seguridad de la Información (ISMS/SGSI). Selección de controles de la ISO 17799, análisis gap. Implementación de controles de la ISO 17799 por medio de las especificaciones del SGSI. Alcance. Declaración de Aplicabilidad (SoA). Modelo PDCA de mejoramiento continuo, procesos de las cuatro fases. Certificación.

- ISO/IEC 27001:2005 Requisitos del Sistema de Gestión.

- Ministerio de Administraciones Públicas, "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información", MAP, versión 1.0, 1997

- UNE 71502:2004, "Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI)", 2004