Análisis de riesgos

Daniel Cruz Allende

PID_00177810

Universitat Oberta de Catalunya
www.uoc.edu

Índice

Introducción

En la actualidad, muchas organizaciones son capaces de dedicar grandes recursos a su seguridad, incluso invierten dinero en realizar cambios en la seguridad de la organización. A la hora de la verdad, si se les pregunta por qué han gastado esos recursos en protegerse de alguna forma, sus respuestas no demuestran que estén demasiado convencidas de que con esa inversión vayan a reducir realmente los incidentes que estaban sufriendo.

Eso nos informa de que las organizaciones hacen cambios e inversiones en seguridad sin auténtica convicción. Sorprende, en cambio, que no estén dispuestas a emplear recursos en estudiar realmente las carencias que tiene su organización.

Si se analizan cuáles son las necesidades de la organización, la posterior inversión en seguridad será mucho menor y más ajustada a la realidad de la organización. Este proceso se realiza mediante los denominados "análisis de riesgos".

Objetivos

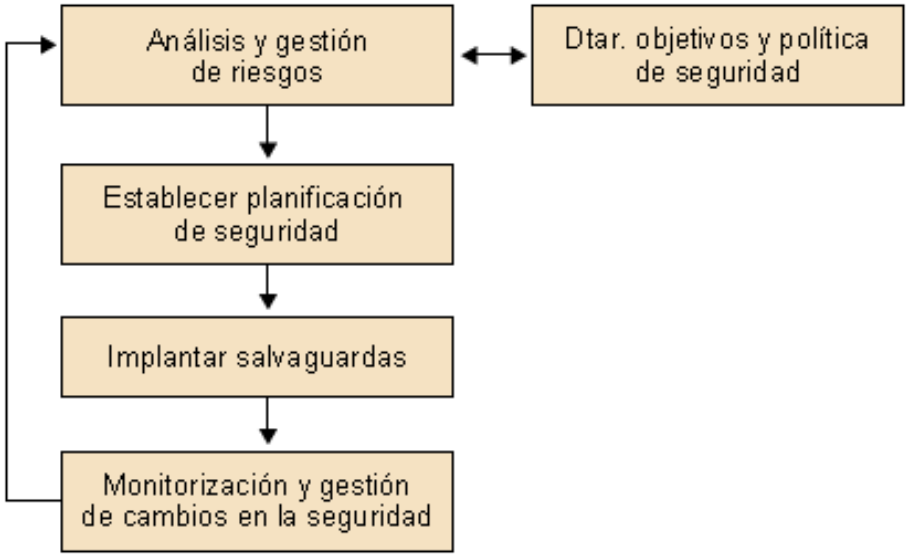
Al acabar de trabajar los materiales de este módulo, los participantes deberían alcanzar los siguientes objetivos:

1. Saber en qué consiste el proceso de análisis de riesgo.
2. Conocer las diferentes metodologías de análisis de riesgos.
3. Identificar los principios en los que se basan las diferentes metodologías de análisis de riesgos.
4. Ser capaces de llevar a cabo un análisis exhaustivo de riesgos aplicando alguna de las metodologías presentadas.

1. Ciclo de vida de la seguridad

Cuando se habla de la seguridad de la información hay que tener en cuenta que se trata de uno de los procesos que se llevan a cabo en una organización. Se trata, además, de un proceso vivo, en constante actualización y renovación, ya que, si esto no es así, no se conseguirán los resultados esperados.

El siguiente gráfico muestra cuál es el ciclo de vida correcto de la seguridad de la información:



En este gráfico se observan las diferentes etapas por las que se debería pasar cuando se habla de seguridad de la información.

La primera y más importante de las fases corresponde al **análisis de riesgos**, que nos servirá para descubrir qué necesidades de seguridad tiene la organización tras detectar cuáles son nuestros agujeros en seguridad así como las amenazas a las que nos encontramos expuestos.

Esta primera fase debe estar siempre muy relacionada con los **objetivos de la organización**; es decir, la seguridad que nosotros creamos debe estar siempre encaminada a que los objetivos que tenga fijados nuestra organización se puedan cumplir. Nunca una medida de seguridad deberá constituirse en obstáculo para la realización de las actividades propias de la organización.

También dentro de esta primera fase está la **gestión de riesgos**, que consistirá en saber elegir la mejor solución de seguridad para afrontar los riesgos a los que se encuentra expuesta la organización y que a su vez permitan cumplir los objetivos de ésta.

Una vez que ya tenemos claro qué peligros nos acechan y cómo nos tenemos que proteger, se pasa a la segunda fase, conocida como **planificación de la seguridad**, que corresponde al proceso de priorización de las diferentes medidas de seguridad que se han detectado como necesarias para mejorar la seguridad de la organización. Siempre se debe tratar de minimizar en primer lugar los mayores riesgos, y en segundo lugar el resto. Nunca al revés.

La tercera fase corresponde propiamente a la implantación de las diferentes medidas que hemos decidido adoptar, ya sean procedimentales, organizacionales o técnicas. En este punto sabemos qué tenemos que hacer para protegernos de las situaciones a las que estamos expuestos.

El problema radica en que, una vez que tenemos implantadas nuestras medidas de seguridad, no podemos detenernos ahí y pensar que, sin hacer nada más, estaremos totalmente seguros durante un tiempo ilimitado. Es precisamente lo contrario: a partir de este momento se debería entrar en la fase de **monitorización y de gestión de cambios de la seguridad**, que consiste en disponer de mecanismos que nos aporten evidencias de que las medidas de seguridad que hemos implantado están evitando los incidentes de seguridad que pretendíamos eludir. Asimismo, si se detecta algún tipo de cambio para mejorar la seguridad, también se debería analizar.

Tanto si se ha detectado con esta monitorización que los incidentes de seguridad continúan produciéndose como si se tiene que realizar algún cambio en alguna de las medidas, se debería entrar en la primera de las fases, es decir, se debería realizar de nuevo el análisis de riesgos, para que dicho cambio no provoque problemas de seguridad.

Se debe realizar un constante proceso de renovación y actualización de las medidas de seguridad de una organización, teniendo como punto de partida el análisis de riesgos, alineado con los objetivos de la organización.

Ejemplo

Pongamos por caso una organización que ha concluido que necesita un antivirus para evitar las posibles infecciones de sus sistemas informáticos. Decide implantarlo, pero, una vez que lo hace, se olvida de su actualización, porque considera que con la instalación del antivirus es más que suficiente para evitar los incidentes de seguridad. Con el paso del tiempo, la aparición de nuevos virus y la falta de actualizaciones de su sistema antivirus suponen que la organización no dispone un sistema antivirus realmente operativo; de hecho, es como si no lo tuviese instalado. En resumen, no hay que olvidar el punto de monitorización y actualización de todas las medidas de seguridad que tiene una organización.

2. Análisis de riesgos

Como se ha comentado anteriormente, el análisis de riesgos corresponde a la primera fase que una organización debería realizar para mejorar su seguridad.

Un análisis de riesgos corresponde, desde el punto de vista de la seguridad, al proceso de identificación de éstos, determinando su magnitud e identificando las áreas que requieren medidas de protección.

Análisis de riesgos

Un análisis de riesgos equivale a realizar una fotografía de una organización, desde el punto de vista de la seguridad, que muestre los aspectos que con una mayor probabilidad podrían provocar un incidente de seguridad.

Cabe destacar que un proceso de análisis de riesgos da como resultado una información y no una medida de seguridad como tal; es decir, el proceso en sí no va a evitar que la organización sufra incidentes de seguridad, sino que permitirá identificar los peligros a los que aquélla se encuentra expuesta. Eso quiere decir que, si tenemos perfectamente identificados los peligros, le será más fácil a la organización protegerse de aquellas situaciones que representan un mayor riesgo.

De hecho, un análisis de riesgos nos va a permitir responder a las tres grandes preguntas sobre la seguridad de la información en una organización para, con posterioridad, poder realizar un análisis y estar en disposición de tomar decisiones basándose en situaciones concretas. Las tres preguntas son las siguientes:

- ¿Qué hay que proteger? Se identifican los elementos que la organización debe tratar de asegurar.

- ¿De qué o de quién nos tenemos que proteger, y por qué? Se identifican los peligros que pueden afectar a la organización y el motivo por el que podría producirse una incidencia.

- ¿Cómo nos queremos proteger? Después de un análisis exhaustivo, se opta por la mejor protección para que los peligros no lleguen a materializarse.

Analizando las preguntas fundamentales

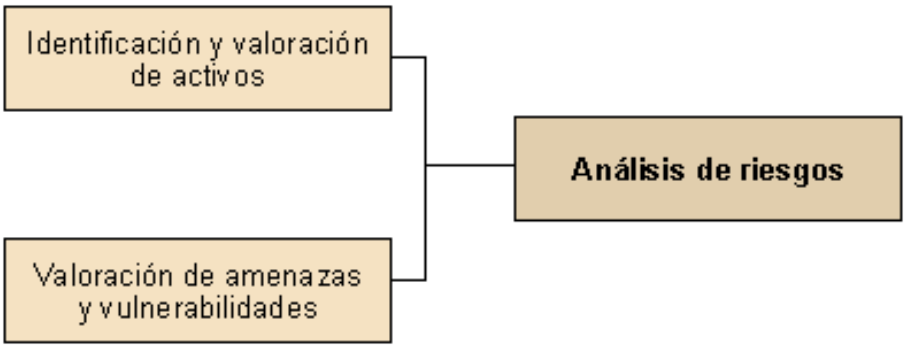
Si una organización no realiza el proceso de detenerse a analizar estas preguntas fundamentales, no se podrá justificar la instalación de una determinada medida de seguridad ni se tendrán las evidencias necesarias para hacerlo. Y esa es la principal ventaja y utilidad de realizar un análisis de riesgos: la de detectar todas las situaciones que deberían protegerse para tratar de evitar los incidentes de seguridad.

2.1. Proceso de análisis de riesgos

En la actualidad, existen diferentes metodologías válidas para realizar un análisis de riesgos. Cada una de ellas tiene una serie de características propias, pero básicamente todas ellas se fundamentan en los mismos procesos y, aunque con matices, trabajan sobre los mismos elementos:

- Activos: elementos que deben protegerse
- Amenazas: situaciones de las que deben protegerse los activos
- Vulnerabilidades: aspectos que facilitan la materialización de las amenazas

El riesgo consiste en la relación de estos tres elementos. Combinándolos entre sí se obtienen los diferentes tipos de riesgos a los que se haya expuesta una organización:



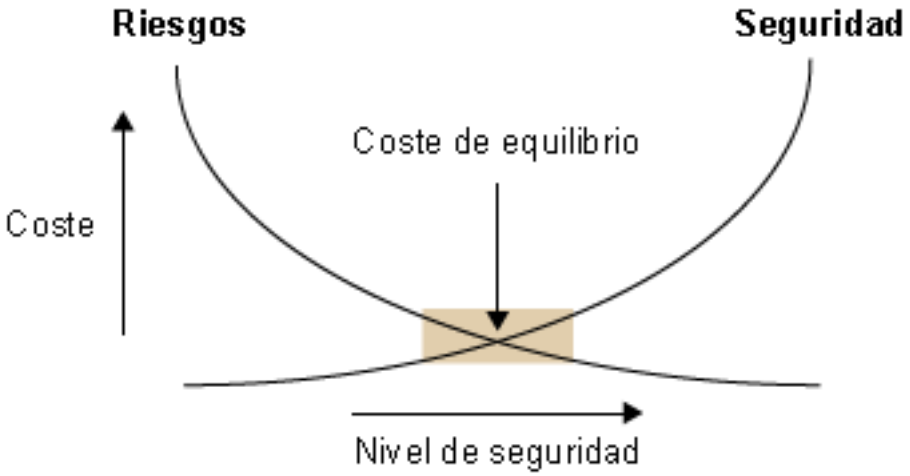
Una vez realizado este proceso de análisis de riesgos se procede a la siguiente fase, y última: la gestión de riesgos, en la que se decide qué medidas de protección deben implantarse para evitar que los riesgos detectados lleguen a afectar a la organización, y todo ello invirtiendo el menor número posible de recursos.

Este proceso de gestión de riesgos ha de equilibrar el coste de protección y el coste de exposición de una organización.

- Coste de protección: coste que supone a la organización protegerse de una situación detectada previamente.
- Coste de exposición: coste que representaría que la situación analizada llegara a darse y la organización careciese de protección.

El punto al que se debería llegar es al de encontrar el coste de equilibrio; es decir, no se debe gastar más de lo que representaría recuperarse de la situación analizada.

Es entonces cuando se debe determinar el denominado **umbral de riesgo**, que será el punto a partir del cual todo riesgo debería ser reducido por lo menos hasta situarse en el punto justamente inferior al marcado por cada organización.



Y en esta fase de gestión de riesgo se debe elegir entre alguna de las siguientes opciones:

- **Aceptarlo**. Esta decisión consiste en que la organización ha detectado que se encuentra expuesta a un riesgo importante que debería ser reducido por debajo del umbral de riesgo marcado. Para ello debería invertir una serie de recursos, pero la protección frente al riesgo detectado representa un coste tan elevado, y su probabilidad de que llegue a suceder es tan improbable, que no resulta posible la inversión para protegerse ante esta situación. La decisión es que la organización trabaje aceptando que está expuesta al riesgo y, llegado el caso de que se produzca un incidente, improvisando una respuesta.

  Esperando un terremoto

  Imaginemos que una organización detecta que está expuesta al riesgo de sufrir un terremoto y que el hecho de que esta situación llegue a suceder representa un riesgo superior al umbral de riesgo determinado por esta organización. Pero el coste de "disponer de un segundo edificio" es demasiado costoso teniendo presente la probabilidad de que llegue a suceder. Ante esta situación, la organización decide aceptar este riesgo y continúa trabajando de la misma manera.

- **Asignarlo a terceros**. Corresponde a la situación en la que una organización determina que tiene algún riesgo por encima de su umbral de riesgo. Además, considera que no puede asumirlo, por su gravedad, pero que a su vez no puede reducirlo, ya sea porque no tiene la capacidad de hacerlo o porque no tiene los recursos necesarios. En estos casos, se decide contratar a un tercero que sí posea esa capacidad para reducir y gestionar el riesgo de tal modo que quede por debajo del umbral de riesgo.

Asignación de riesgos a terceros

Los ejemplos más habituales serían los de contratación de pólizas de seguro o los de contratación de terceras organizaciones para que gestionen alguna determinada área que por defecto debería gestionar la propia organización; por ejemplo, las empresas especializadas en la gestión de la red de una organización.

- **Reducirlos o evitarlos**. Corresponde a la situación en la que una organización ha detectado un riesgo elevado, por encima de su umbral de riesgo, y decide implantar algún control o salvaguarda para reducirlo; al menos, hasta situarlo por debajo del umbral de riesgo determinado.

  Sin ningún género de dudas, lo ideal siempre es tratar de evitar o reducir un riesgo, ya que supone que la propia organización controla y dispone de las medidas de seguridad adecuadas que le permitan tratar de evitar dichos riesgos.

3. Análisis de riesgos. Justificación y estudio

Sabemos ya que un análisis de riesgos debería ser la primera y principal tarea que una organización ha de realizar cuando se plantea mejorar en cualquier aspecto la seguridad de la información.

3.1. ¿Por qué realizarlo?

Los motivos por los que se debe realizar un análisis de riesgos son los siguientes:

- Permite identificar los diferentes riesgos a los que se encuentra expuesta la organización desde el punto de vista de la seguridad y que podrían afectar al desarrollo de las diferentes actividades de negocio de la organización.

- Permite a la organización realizar una selección de medidas de seguridad que se deben implantar en ella, mucho más ajustada a las necesidades de la misma.

- Permite realizar y elaborar los planes de contingencias de una organización. Esto quiere decir que un análisis de riesgo nos va a presentar las situaciones que pueden provocar un incidente de seguridad y que, a su vez, no pueden ser reducidos a través de la implantación de las medidas de seguridad. Ha de servir, por tanto, como base para la elaboración de los planes de contingencias.

- Las organizaciones que tengan previsto implantar las diferentes normativas de seguridad (ISO 27001) y crear un sistema de gestión de la seguridad de la información (SGSI), con la intención de conseguir certificarlo, deberán poseer un análisis de riesgos, que será el auténtico punto de partida de todo el proceso de certificación.

El sistema de gestión de la seguridad de la información corresponde al proceso de implantación de una serie de medidas indicadas en las normativas y buenas prácticas de seguridad de la información.

3.2. Tipos de análisis

Dependiendo de los objetivos que se pretenden conseguir y del enfoque que se tenga a la hora de realizar un análisis de riesgo, se pueden realizar dos tipos diferentes de procesos de análisis de riesgos:

- **Análisis de riesgos intrínseco**. Es el estudio que se realiza sin tener en consideración las diferentes medidas de seguridad que ya están implantadas en una organización. Este proceso da como resultado un riesgo intrínseco.

- **Análisis de riesgos residual**. Es el estudio que se realiza teniendo en consideración las medidas de seguridad que la organización ya tiene implantadas. Como resultado de este proceso se obtiene un riesgo real.

La decisión entre realizar un análisis de riesgos intrínseco o residual depende de si una organización pretende analizar si la inversión que ha realizado en seguridad ha sido la correcta o si, por el contrario, lo que pretende es estudiar la situación real en la que se encuentra. Lo más habitual es realizar el análisis de riesgos residual, puesto que, si una organización ya posee unas medidas de seguridad implantadas y pretende mejorar su seguridad, deberá contemplar estas soluciones teniendo en cuenta la situación actual en la que se encuentra, ya que, aunque la inversión no haya sido la correcta, no podrá recuperarla.

De todas formas, teniendo en cuenta que existen diferentes metodologías para realizar análisis de riesgos, es posible que el nombre que le pongan a cada una de ellas sea distinto, siendo su esencia sea la misma:

- Existe un estudio que refleja la situación inicial o sin medidas de seguridad.
- Existe un estudio que refleja los riesgos y las medidas de protección que se deben implantar.

Independientemente de la metodología que se utilice, tal y como se ha comentado anteriormente, el resultado de todos los análisis será el mismo, ya que todos ellos se fundamentan en los mismos elementos.

3.3. Elementos del análisis

Todos los análisis de riesgos se fundamentan en los mismos elementos y, aunque existan diferentes metodologías, en todas ellas se tienen en consideración los mismos aspectos y deben dar resultados similares independientemente del modo de expresarlo.

Los elementos que se tienen en consideración en los procesos de análisis de riesgos son los siguientes:

- **Activos**: son todos aquellos elementos que posee la organización y que serán analizados durante el proceso. Cabe destacar que por activo se entiende todo tipo de elemento que requiere la organización para poder realizar las actividades de negocio que le son propias.

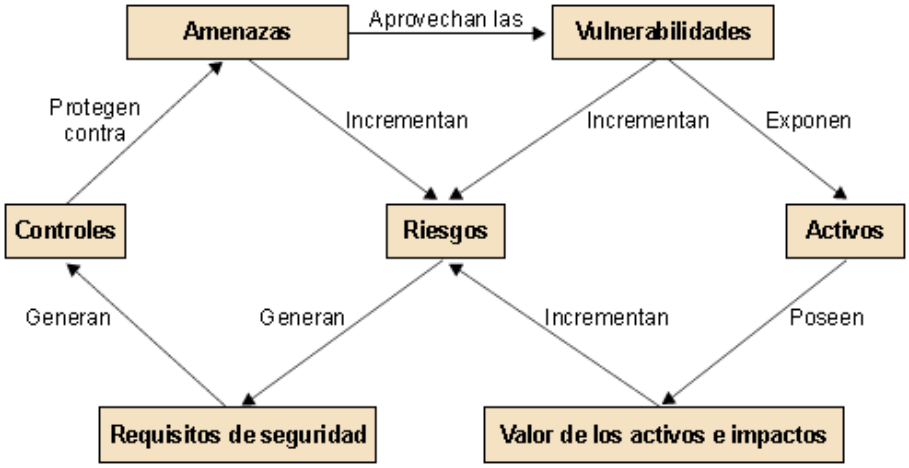
- **Amenazas**: son todas aquellas situaciones que podrían llegar a suceder en una organización y que podrían dañar a los activos, provocando que éstos

no funcionen correctamente o que no puedan utilizarse del modo correcto para poder llevar a cabo la actividad de negocio de la organización.

- **Vulnerabilidades**: son las diferentes debilidades que presentan los activos anteriormente identificados y que son aprovechados por las amenazas para provocar un daño.

- **Impactos**: son las consecuencias que se producen en la organización cuando una amenaza aprovecha una vulnerabilidad para dañar a un activo.

Todos estos elementos son la base para cualquier análisis de riesgos, y en ellos se fundamenta todo el estudio. A partir de éstos, se estiman los riesgos a los que se encuentra expuesta la organización y que con posterioridad deberán ser tratados en el proceso de gestión de los riesgos. De hecho, dentro de todo proceso de análisis y gestión de riesgos se crean una serie de relaciones:



El gráfico muestra las relaciones que se crean cuando se habla de seguridad de la información y cuando se pretende minimizar los **riesgos** a los que se encuentra expuesta una organización.

Hay que tener en cuenta que una organización está expuesta a una serie de **amenazas** que son los causantes de los riesgos y a su vez de los posibles daños. Las amenazas aprovechan las **vulnerabilidades** para dañar los activos; de hecho, si no existen vulnerabilidades, las amenazas no podrán dañar a una organización. Estas amenazas exponen a los **activos** y son éstos los que poseen realmente **valor** para una organización: es decir, que son los elementos que necesita una organización para poder desarrollar sus actividades.

Tanto las amenazas como las vulnerabilidades y el propio valor de los activos hacen que los riesgos aumenten de modo que las organizaciones tengan que plantearse medidas de protección.

Estos riesgos son los que generan **requerimientos de seguridad**. A su vez, estos requerimientos acaban generando **controles** de seguridad, que son finalmente los que se implantan en las organizaciones para poder reducir los riesgos. Estos controles tratan de proteger contra las amenazas anteriormente listadas.

La gráfica que acabamos de presentar muestra que todas las metodologías de análisis de riesgos, independientemente de la que se haya utilizado, se rigen por las relaciones anteriores.

4. Metodologías

En la actualidad, existen diversas metodologías en el mercado. Todas ellas ofrecen resultados similares si se aplican de una forma correcta a las mismas organizaciones. Las diferencias entre unas y otras radican en la forma en la que presentan los resultados.

4.1. MAGERIT

Esta metodología fue elaborada por el MAP (Ministerio de Administraciones Públicas) con el fin de ayudar a todas las administraciones públicas del Estado español a mejorar diversos aspectos. Con posterioridad ha sido aplicable a cualquier organización.

Esta metodología puede ser aplicada a cualquier organización, independientemente de que se encuentre en el Estado español o en otro país. Al mismo tiempo, esta metodología ha desarrollado una herramienta que ayuda a su aplicación.

Con el paso del tiempo se ha ido desarrollando una nueva versión de esta metodología y durante el año 2005 se presentó la segunda versión, con una nueva herramienta. En esencia, la normativa no ha cambiado y los aspectos que tiene en consideración siguen siendo los mismos de la original.

Esta metodología tiene como característica fundamental que los riesgos que se plantean para una organización se expresan en valores económicos directamente, lo que una ventaja y un inconveniente:

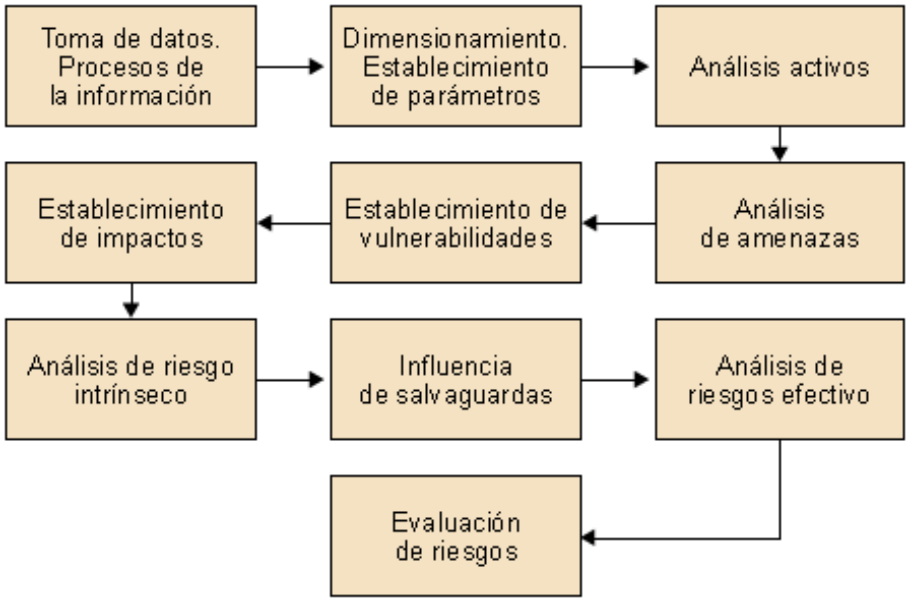
- El aspecto positivo de esta metodología es que el resultado se expresa en valores económicos. Esto hace que las decisiones que deban tomarse y que tengan que ser validadas por la dirección estarán fundamentadas y serán fácilmente defendibles.

- Por el contrario, el hecho de tener que traducir de forma directa todas las valoraciones en valores económicos hace que la aplicación de esta metodología sea realmente costosa.

4.1.1. Fases de MAGERIT

Esta metodología, como se ha comentado anteriormente, posee una herramienta –aunque no imprescindible– que permite la aplicación de MAGERIT de una forma directa.

MAGERIT sigue un proceso hasta llegar a la elaboración e identificación de todos los riesgos de una organización. Las fases son las siguientes:



Toma de datos y procesos de información

En esta primera fase –la más importante de toda la metodología–, debe definirse el alcance que se ha de estudiar o analizar, ya que, dependiendo de éste, será más o menos costoso el proceso. A mayor alcance, mayor es el número de riesgos analizables.

Otro factor que debe tenerse en cuenta es que, en esta primera fase, han de analizarse los procesos que lleva a cabo la organización, puesto que los riesgos que se tienen que estudiar son aquellos que pudieran interferir en los procesos críticos. No hay que olvidar que el objetivo de toda seguridad es siempre garantizar que los procesos propios de la organización puedan realizarse de la mejor manera posible.

Existen amenazas que no van a provocar interferencias en las actividades de la organización y que no han de ser analizadas, puesto que protegerse contra ellas no tiene sentido, ya que no le afectarán nunca.

En esta primera fase también hay que tener presente un factor importantísimo: la granularidad.

La **granularidad** tiene que ver con la definición de las unidades que se pretende analizar. Quiere decir que se ha de determinar el nivel de detalle al que se quiere llegar. Cuanto más detalle (bajo nivel), más elementos tendrán que analizarse y más costoso será el análisis de riesgos.

Establecimiento de parámetros

La segunda fase es la más importante en la metodología MAGERIT. Consiste en el establecimiento de parámetros que se utilizarán durante todo el proceso de análisis de riesgos.

Debe tenerse presente que los parámetros que se identifiquen en esta fase tendrán que ser utilizados durante todo el proceso de análisis de riesgos y, que si esto no se cumple, los resultados que se obtendrán no podrán ser comparados, de modo que el resultado no mostrará los riesgos reales de una organización.

Los parámetros que deben identificarse son los siguientes:

- Valor de los activos
- Vulnerabilidad
- Impacto
- Efectividad del control de seguridad

Veámoslos en detalle:

- **Valor de los activos**. Este parámetro tiene el objeto de asignar una valoración económica a todos los activos de una organización que se pretenden analizar.
  Los activos que han de ser analizados son aquellos que requiere la organización para llevar a cabo los procesos propios de la misma.
  Cuando se trata de asignar valoraciones económicas a los activos, no sólo hay que tener presente su valor de compra, sino también su valor según la importancia que tenga para la tarea que se utiliza.
  Para llevar a cabo la valoración deben establecerse diferentes grupos de activos según su valor. A cada uno de estos rangos se le asigna un valor estimado que será el que se utilice para todos los activos cuya valoración económica se corresponda con ese rango de valores.
  Cada organización ha de dictaminar cuáles serán los rangos de valores que pretenderá utilizar durante el estudio. No es recomendable establecer más de cinco rangos, puesto que cuantos más se establezcan más complicada será la asignación de cada activo al nivel adecuado.
  A la hora de asignar una valoración a cada activo debe tenerse en consideración lo siguiente:
  – El **valor de reposición** es el valor que tiene para la organización reponer ese activo en el caso de que se pierda o de que no pueda ser utilizado.

  – El **valor de configuración** es el tiempo que se necesita desde que se adquiere el nuevo activo hasta que se configura o se pone a punto para que pueda utilizarse para la función que desarrollaba el anterior activo.

– El **valor de uso del activo** es el valor que pierde la organización durante el tiempo que no puede utilizar dicho activo para la función que desarrolla.

– El **valor de pérdida de oportunidad** es el valor que pierde potencialmente la organización por no poder disponer de dicho activo durante un tiempo.

Valor de un portátil

Imaginemos que se trata de analizar el valor que tiene un portátil para dos organizaciones diferentes. Una de ellas únicamente utiliza ese equipo para realizar presentaciones. En cambio, la otra organización utiliza ese equipo (que tiene el mismo precio en el mercado) como servidor o como repositorio de información. A la hora de realizar su estimación, el valor del portátil para la segunda organización será superior, aunque el precio del equipo sea el mismo para las dos.

Procedimiento de valoración

Valoración	Rango	Valor
Muy alta	valor > 200.000 €	300.000 €
Alta	100.000 € < valor > 200.000 €	150.000 €
Media	50.000 € < valor > 100.000 €	75.000 €
Baja	10.000 € < valor > 50.000 €	30.000 €
Muy baja	valor < 10.000 €	10.000 €

En este ejemplo debe considerarse que, durante el proceso de análisis de riesgos, el valor máximo de todos los activos que se han de analizar, independientemente del valor definitivo que éstos puedan tener, será de 300.000 €.

- **Vulnerabilidad**. Para MAGERIT, las vulnerabilidades se entienden como una frecuencia de ocurrencia de una amenaza; es decir, la frecuencia con la que puede una organización sufrir alguna amenaza en concreto.
  Esta frecuencia de ocurrencia, o vulnerabilidad, también se plasma en una escala de valores (no se recomiendan más de cinco niveles) que tendrán que ser utilizados para todo el estudio.
  Una vez que hemos determinado la escala de valores que utilizaremos durante el análisis de riesgos, habrá que traducir estas vulnerabilidades a números, para poder trabajar con ellos. Esta valoración numérica se realiza mediante estimaciones anuales, es decir, asignando un número de veces por año:

  Vulnerabilidad = Frecuencia estimada / Días del año

Vulnerabilidad

Son agujeros que posee la organización desde el punto de vista de la seguridad de la información.

Clasificación de la vulnerabilidad

Vulnerabilidad	Rango	Valor
Frecuencia extrema	1 vez al día	1
Frecuencia alta	1 vez cada 2 semanas	26/365 = 0,071233
Frecuencia media	1 vez cada 2 meses	6/365 = 0,016438
Frecuencia baja	1 vez cada 6 meses	2/365 = 0,005479
Frecuencia muy baja	1 vez al año	1/365 = 0,002739

Suposición: el año tiene 52 semanas.

En este ejemplo, la organización ha estimado que, en el peor de los casos (a lo que será más vulnerable, o con más frecuencia), la situación se dará una vez al día. Esto, extrapolado al año, representará el 100% de vulnerabilidad:

$$\text{Vulnerabilidad} = 365/365 = 1$$

El segundo caso representa que se estima que ocurrirá una vez cada dos semanas, que representaría unas veintisiete veces al año, lo que resulta un valor de 0,071. Y de este modo se extraerían el resto de valores.

Cabe añadir que, a la hora de elaborar el análisis de riesgos, lo más correcto no sería pensar en los conceptos de "una vez al año" o "una vez al mes", sino en si una situación, en virtud de las características de la organización, tiene una frecuencia de ocurrencia extrema, alta, media, baja o muy baja, y a partir de esa clasificación trabajar con la numeración que se ha extraído para ese nivel de vulnerabilidad.

Debe quedar claro que no pueden ir modificándose los valores durante el estudio, sino que han de mantenerse de este modo para todos los activos y para todas las amenazas que tengan que analizarse. Si se cambian las escalas en mitad del estudio, los resultados no serán adecuados y no podrán ser comparables.

- **Impactos**. Para MAGERIT, se entiende por **impacto** el tanto por ciento del valor del activo que se pierde en el caso de que suceda un incidente sobre él.

  Para realizar este análisis a priori, también debe realizarse una estimación por rango de impactos; es decir, hay que pensar en los diferentes niveles de impacto que se quieren utilizar, y a partir de ahí asignar el porcentaje de valor que se estima que puede perderse en cada caso.

Impacto

Es la consecuencia del hecho de que una amenaza, aprovechando una vulnerabilidad, dañe un activo.

Valoración de los impactos

Impacto	Valor
Muy alto	100 %
Alto	75 %
Medio	50 %
Bajo	20 %
Muy bajo	5 %

En este ejemplo se estima que, en el caso de que se sufra el incidente con el impacto más grande posible, se llegaría a perder el 100% del valor de ese activo; en el caso de que el impacto sea alto (pero sin llegar a ser el más alto) se perdería el 75% del valor del activo, y así para cada uno de los niveles establecidos.

- **Efectividad del control de seguridad**. Este parámetro consiste en ver la influencia que tendrán las medidas de protección ante los riesgos que vamos a detectar, es decir, en pensar en cómo las diferentes medidas de seguridad que podamos implantar nos pueden reducir el riesgo detectado.
  A la hora de reducir un riesgo, hay que tener en cuenta que las medidas de seguridad tienen dos modos de actuar contra él: o bien reducen la vulnerabilidad (la frecuencia de ocurrencia), o bien reducen el impacto que provoca dicho riesgo.
  Para este parámetro, también debe realizarse una clasificación de niveles válida para todo el estudio.

Clasificación de niveles

Variación impacto/vulnerabilidad	Valor
Muy alto	95%
Alto	75%
Medio	50%
Bajo	30%
Muy bajo	10%

Según la tabla, la organización estima que, en caso de utilizar la mejor medida de seguridad para un determinado riesgo, ésta le ayudará a reducir su riesgo inicial en un 95%, y así para cada uno de los niveles que ha establecido.

Una vez más hay que destacar que todos estos parámetros son los que deben ser **utilizados durante todo el análisis de riesgos.** No pueden ir modificándose dependiendo del activo que se analice o de la amenaza que pueda afectar.

Análisis de activos

Esta fase del estudio consiste en identificar cuáles son los activos que posee la organización y que necesita para llevar a cabo sus actividades. En esta fase es muy importante haber dejado claramente identificado el alcance del análisis de riesgos, puesto que solamente se deberían analizar aquellos activos que estén dentro de dicho alcance.

Cabe recordar que es importante tener claro el nivel de granularidad al que se quiera llegar, puesto que, cuanto más bajo sea éste, mayor será el listado de activos analizables.

Cuando se habla de activos analizables hay que pensar en los siguientes tipos de activos:

- **Activos físicos**. Serían todos los activos de tipo *hardware* que se utilizan en la organización: ordenadores, servidores, portátiles, PDA, teléfonos móviles, impresoras, etc.

- **Activos lógicos**. Serían todos los elementos de *software* que se utilizan: sistemas operativos, aplicaciones propias, paquetes cerrados de mercado, procesos *bach*, etc.

- **Activos de personal**. Son las personas, desde el punto de vista de roles o perfiles que intervienen en el desarrollo de las actividades de la organización: responsable de seguridad, administrador de la red, personal de administración, secretarios, usuarios, etc.

- **Activos de entorno e infraestructura**. Son todos los elementos que posee la organización y que necesita para que el resto pueda funcionar correctamente. Son, por ejemplo, los sistemas de aire acondicionado o el cableado de datos y de corriente eléctrica, etc.

- **Activos intangibles**. Son aquellos elementos que directamente no posee la organización pero que son importantes para ella, como pueden ser la imagen corporativa, la credibilidad, la confianza de los clientes, el *know how*, etc.

Deben clasificarse según los valores que se han establecido previamente como parámetros, para lo cual cabe recordar que debe tenerse en cuenta lo siguiente:

- Valor de reposición
- Valor de configuración o puesta a punto
- Valor de uso del activo
- Valor de pérdida de oportunidad

Análisis de amenazas

Amenazas son aquellas situaciones que podrían llegar a darse en una organización y que desembocarían en un problema de seguridad.

Conviene tener presente que las amenazas dependen mucho de la organización, así como de las características de ésta, en el sentido de que hay que analizar las amenazas que afectarían a los activos que posee una organización en concreto.

Diversidad de amenazas

Las amenazas que puede sufrir una multinacional no tienen nada que ver con las que puede sufrir una pyme, ni tampoco una organización que se dedica al comercio electrónico está sometida a las mismas amenazas que las que acechan a una empresa que se dedica a la fabricación de cualquier producto y que ni siquiera tiene conexión a Internet.

MAGERIT clasifica las amenazas que pueden afectar a una organización en cuatro grandes grupos, y dentro de cada uno de ellos identifica amenazas más concretasm, que son las que deben contemplarse:

- **Accidentes**. Son aquellas situaciones no provocadas voluntariamente y que muchas veces no pueden evitarse, sino que suceden por efectos naturales. Dentro de esta categoría de accidentes existen diferentes tipos, como son:
  - Accidente físico (inundación, incendio, terremoto, explosión, etc.)
  - Avería
  - Interrupción de los servicios esenciales (cortes en el suministro eléctrico, en las telecomunicaciones, etc.)
  - Accidentes mecánicos o electromagnéticos (choque, caída, radiación, etc.)
- **Errores**. Son aquellas situaciones que son cometidas de forma involuntaria, por el propio desarrollo de las actividades diarias de la organización, ya sea por desconocimiento o por descuido del personal de ésta o de terceros que son contratados por la propia organización. Entre las cuales podemos citar las siguientes:
  - Errores en la utilización de los sistemas, provocados por un mal uso
  - Errores en el diseño conceptual de las aplicaciones
  - Errores en el desarrollo de las aplicaciones
  - Errores de actualización o parcheado de los sistemas o aplicaciones

  - Errores en la monitorización
  - Errores de compatibilidad entre aplicaciones
  - Errores inesperados (virus, troyanos, etc.)

- **Amenazas intencionales presenciales**. Son las provocadas por el propio personal de la organización de forma voluntaria al realizar acciones que sabe que provocan un daño, tanto desde el punto de vista físico como desde el lógico. Entre las cuales podemos citar las siguientes:
  - Acceso físico no autorizado, ya sea con destrucción o con sustracción de la información
  - Acceso lógico no autorizado, interceptación pasiva de la información o sustracción o alteración de la información en tránsito
  - Indisponibilidad de recursos, ya sean humanos (bajas, vacaciones, abandono, enfermedad, etc.) o técnicos (bloqueo de sistema, etc.)
  - Filtración de datos a terceras organizaciones, ya sean datos personales (LOPD) o técnicos.

- **Amenazas intencionales remotas**. Amenazas provocadas por terceras personas, es decir, por personas ajenas a nuestra organización y que consiguen dañarla. Entre las cuales podemos citar las siguientes:
  - Acceso lógico no autorizado. Acceso de un tercero no autorizado, que explota una vulnerabilidad del sistema para utilizarla en su propio beneficio.
  - Suplantación del origen. Interceptación de una comunicación escuchando y/o falseando los datos intercambiados.
  - Gusanos. Virus que utilizan las capacidades de servidores y clientes para propagarse por Internet.
  - Denegación de servicio, ya sea contra el ancho de banda (consumir todo el ancho de banda de la máquina que se quiere atacar) o contra los recursos del sistema (consumir toda la memoria y los recursos de la máquina utilizada para ofrecer un servicio).

Como se puede observar, todos los peligros que podemos imaginar pueden englobarse en alguno de los tipos de amenazas que hemos analizado. La metodología MAGERIT ofrece un listado de toda una serie de amenazas correspondientes a cada uno de estos niveles, listado que puede ser de utilidad para la realización de los análisis de riesgos independientemente de la metodología que se utilice.

Establecimiento de las vulnerabilidades

Recordemos que por vulnerabilidades se entienden aquellos agujeros que tenemos en nuestra seguridad y que permiten que una amenaza pueda dañar un activo. Es importante tener claro que, sin vulnerabilidad, la amenaza no puede dañar nuestros activos y también que las vulnerabilidades por sí mismas no provocan daños, sino que éstos son siempre provocados por las amenazas.

En MAGERIT, a pesar de que no es necesario listar las vulnerabilidades, sí que es necesario tenerlas en cuenta para poder estimar la frecuencia de ocurrencia de una determinada amenaza sobre un activo.

Riesgo de incendio

Supongamos que estamos analizando el riesgo que tiene una organización de sufrir un incendio en su servidor situado en una sala (CPD –centro de proceso de datos–) que posee un sistema de extinción automática de incendios por gas halón, así como detectores de humos y detectores de temperatura. La frecuencia de ocurrencia, es decir, la vulnerabilidad que tendrá ante la amenaza de incendio, será menor que en el caso de que no disponga de estos elementos.

Este análisis debe realizarse a la hora de identificar las vulnerabilidades de MAGERIT.

Valoración de impactos

Los impactos se definen como las consecuencias que provoca en la organización el hecho de que una cierta amenaza, aprovechando una determinada vulnerabilidad, afecte a un activo.

A la hora de analizar los impactos deberían tenerse en consideración los siguientes aspectos:

- El resultado de la agresión de una amenaza sobre un activo
- El efecto sobre cada activo para poder agrupar los impactos en cadena según la relación de activos,

Incendio de un servidor

Al analizar el impacto del incendio de un servidor, hay que tener en cuenta que el incendio no sólo afecta a la disponibilidad del equipo, sino también a la información que éste contiene, aunque no sea el activo que se está analizando de por sí.

- El valor económico representativo de las pérdidas producidas en cada activo
- Las pérdidas cuantitativas o cualitativas

Análisis de riesgos intrínseco

A partir de este punto, y con los valores que hayamos identificado para cada situación, ya se puede realizar el estudio de los riesgos actuales a los que está sometida una organización.

Para este estudio, únicamente es necesario realizar una multiplicación de los valores que hemos indicado hasta ahora:

$$\text{Riesgo} = \text{Valor del activo} \times \text{Vulnerabilidad} \times \text{Impacto}$$

Para MAGERIT, el estudio de la situación actual es el análisis de riesgos intrínseco, es decir, el análisis de la situación en la que se encuentra la organización en el momento del estudio aunque ya posea medidas de seguridad implantadas.

Recordemos que definimos los **riesgos intrínsecos** como aquellos a los que estamos expuestos sin tener en cuenta las medidas de seguridad que podamos implantar. En el caso de MAGERIT, se entiende como **intrínseca** la situación en la que nos encontramos teniendo en consideración todos los elementos que posee la organización.

Influencia de las salvaguardas

Una vez que tenemos identificados los riesgos actuales a los que se encuentra expuesta la organización, se entra en la fase de **gestión de riesgos**, que consiste en tratar de escoger la mejor solución de seguridad que me permita reducirlos.

Para ello existen dos tipos fundamentales de controles de seguridad o salvaguardas:

- **Preventivas**. Son aquellas medidas de seguridad que reducen las vulnerabilidades (la frecuencia de ocurrencia).

  $$\text{Nueva vulnerabilidad} = \text{Vulnerabilidad} \times \text{Porcentaje de disminución de vulnerabilidad}$$

- **Correctivas**. Son aquellas medidas de seguridad que reducen el impacto de las amenazas.

  $$\text{Nuevo impacto} = \text{Impacto} \times \text{Porcentaje de disminución de impacto}$$

Ejemplos de salvaguardas

Como ejemplos de cada uno de estos dos tipos de controles de seguridad tenemos los siguientes:

- Un *firewall*. Como medida preventiva, lo que hace es reducir la frecuencia de ocurrencia de intrusiones en nuestra red. Pero, en el caso de que llegue a producirse una intrusión, no puede hacer nada para reducir los daños que provocaría.

- Una copia de seguridad. Lo que hace es reducir el impacto que provocaría una pérdida de información. En cambio, no reduce la posibilidad de que alguien pueda borrar la información de la organización.

Para reducir cada uno de los riesgos que hemos identificado en nuestra organización, sería necesario que se buscaran las soluciones de seguridad que existen en el mercado, ya sean preventivas o curativas.

Análisis de riesgos efectivos

Será el resultado de estudiar cómo se reducirían los riesgos con cada una de las medidas de protección (controles o salvaguardas) que hemos identificado; es decir, se debería calcular el riesgo definitivo, dándose como resultado el riesgo efectivo que tendría la organización para cada una de las amenazas identificadas.

En resumen, el estudio sería el siguiente:

- Riesgo intrínseco
  Valor activo × Vulnerabilidad × Impacto

- Riesgo efectivo
  Valor efectivo × Nueva vulnerabilidad × Nuevo Impacto = Valor activo × (Vulnerabilidad × Porcentaje de disminución de vulnerabilidad) × (Impacto × Porcentaje de disminución de impacto) = Riesgo intrínseco × Porcentaje de disminución de vulnerabilidad × Porcentaje de disminución de impacto

Gestión de riesgos

Esta última fase consiste en la toma de decisiones por parte de la organización sobre las medidas de seguridad que debe escoger entre el listado de salvaguardas que permiten reducir los riesgos en aquélla.

Umbral de riesgos

Es el punto en el que una organización considera que los riesgos a los que se encuentra expuesta no son aceptables.

Aquí hay que tener en cuenta que las organizaciones deben pretender disminuir todos los riesgos que han detectado hasta situarlos por debajo del denominado "umbral de riesgos", que en cada organización será o podrá ser diferente.

A la hora de gestionar los riesgos, deben escogerse aquellas medidas de seguridad que permitan reducir los riesgos intrínsecos de la organización hasta situarlos por debajo del umbral de riesgos con un menor coste para la organización.

Recordemos que, a la hora de gestionar los riesgos en una organización, existen tres decisiones que pueden tomarse:

- Reducirlos
- Transferirlos
- Aceptarlos

Plan de acción

Es un documento en el que se describen las conclusiones del análisis de riesgos, así como las medidas que llevará a cabo la organización para reducirlos.

A la hora de gestionar riesgos debe elaborarse un **plan de acción**, que contendrá la siguiente información:

- Establecimiento de prioridades. Consiste en designar aquellos riesgos que tendrán que ser reducidos en primer lugar debido a que son los más elevados para la organización.

- Planteamiento del análisis de coste/beneficio. Consiste en estudiar, para cada una de las medidas que se pueden implantar, qué coste le supondría a la organización y en qué porcentaje reduciría los riesgos detectados.

- Selección de controles definitivos. Una vez analizado el coste/beneficio de todos los controles, hay que seleccionar definitivamente los que tendrá que implantar la organización para reducir los riesgos hasta situarlos por debajo de su umbral de riesgo.

- Asignación de responsabilidades. Consiste en asignar los responsables dentro de la organización de llevar a cabo la implantación de los controles. Es importante tener identificadas a estas personas ya que, si no, existe el peligro de que las decisiones que se tomen acaben por no ser implantadas.

- Implantación de controles. Consiste en realizar la implantación de los controles de seguridad designados. Hay que tener en cuenta que no forzosamente los controles que se implanten han de ser técnicos, sino que podrían ser controles organizativos o procedimentales.

Ejemplo de MAGERIT

A pesar de que, como se ha comentado, MAGERIT aporta una herramienta para la realización de estos procesos de análisis de riesgos, puede hacerse sin necesidad de dicha herramienta, aunque puede ser laborioso.

Imaginamos una organización que tiene una serie de activos y que realiza su análisis de riesgos utilizando MAGERIT. El resultado sería algo similar al que se expone a continuación.

Resumen. Vulnerabilidad/impacto y riesgo intrínseco 22.502

					4		5		6		
			Personal de desarrollo de software y hardware		PC de desarrollo		PC de hardware		PC de entorno de pruebas		Año
			EN-003		SI-001		SI-002		SI-003		
Número	**Código**	**Nombre**	50.000		10.000		10.000		2.500		
1	A1-001	Incendio en oficinas			0,003*	50%**	0,003	50%	0,003	50%	
					13,70		13,70		3,42		30,82
3	A2-001	Avería hardware			0,005	50%	0,005	50%	0,005	50%	
					27,40		27,40		6,85		61,65
5	P1-002	Acceso físico a oficinas			0,003	5%	0,003	5%	0,003	5%	
					1,37		1,37		0,34		3,08
6	P2-001	Acceso lógico interno a los sistemas			0,005	50%	0,005	50%	0,005	50%	
					27,40		27,40		6,85		61,65
8	P5-002	No disponibilidad de personal	0,0020	50%							
			68,48								68,49
Riesgo intrínseco anual por activo			68,48€		69,87€		69,87€		17,46€		225,68

* Vulnerabilidad; para el cálculo, utilizar el valor con seis decimales, es decir, 0,002739.
** Impacto.

En este estudio, lo primero que se ha realizado sería la identificación de los activos de la organización, que están listados en la fila superior. Previamente se han identificado y establecido los parámetros que se utilizarán durante todo el estudio.

Posteriormente, se han valorado estos activos, sobre la base del parámetro que se ha marcado. Tal vez, el grupo de los PC de desarrollo tienen un valor superior a los PC de *hardware* (entornos diferentes dentro de la organización), pero no lo suficiente como para saltar a otro rango de valores dentro de los parámetros establecidos por la organización.

A continuación, se han buscado las amenazas que podrían llegar a afectar a los activos anteriores y se han listado en la columna de la izquierda.

El siguiente paso consiste en identificar las vulnerabilidades que existen entre cada amenaza y cada uno de los activos anteriores (corresponde al valor que aparece primero en cada amenaza para cada activo).

Una vez acabado el anterior paso, se estima el impacto que provocaría dicha amenaza en la organización en el caso de que llegue a ocurrir, y se introduce en la casilla que hay a la derecha de la de vulnerabilidad.

Por último, se multiplican los tres valores y obtenemos el riesgo (es el valor que aparece en la casilla inferior para cada cruce de activo y amenaza) que posee cada activo. Este resultado es el valor anual, puesto que las vulnerabilidades están expresadas en número de veces de ocurrencia por año.

Cuando ya tenemos estos riesgos identificados, se realiza la suma de todos ellos tanto en horizontal (riesgo al que se está expuesto por cada amenaza) como en vertical (riesgos que posee cada uno de los activos de la organización).

A partir de este momento, ya tenemos los riesgos intrínsecos, y se debería proceder a determinar el umbral de riesgo que marca la organización y analizar, para cada una de las situaciones anteriores, especialmente o prioritariamente aquellas que sobrepasan dicho umbral de riesgo, qué controles de seguridad van a permitir reducir dichos riesgos, cuánto menos se situarían por debajo del umbral y, de entre todas las posibles soluciones, seleccionar aquella que reduce el riesgo en un mayor porcentaje con un menor coste para la organización.

Conclusiones de MAGERIT

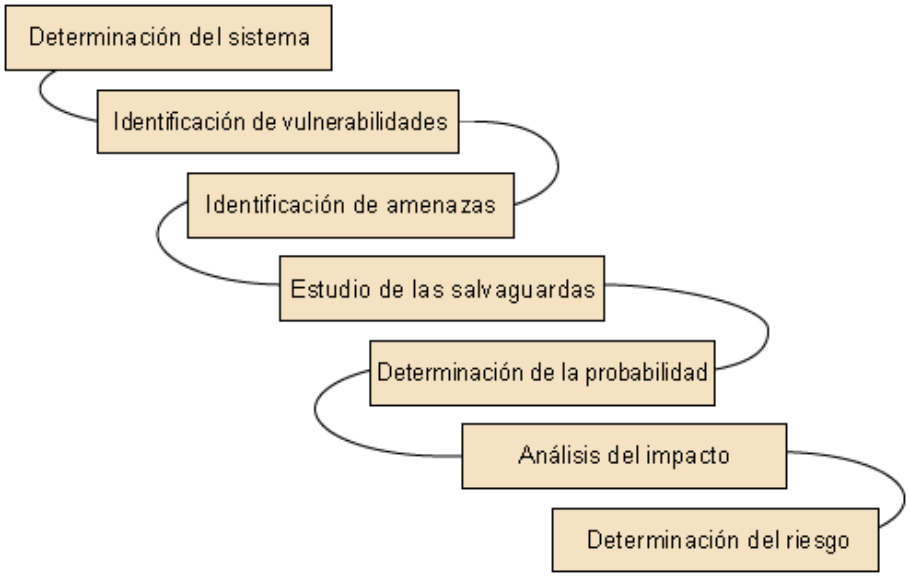
Como hemos visto, la metodología MAGERIT tiene como gran virtud que los resultados que se ofrecen están expresados económicamente. Esto tiene como ventaja que es fácilmente defendible ante la dirección, puesto que es ésta la que tiene que aceptar y asumir los riesgos a los que se encuentra expuesta la organización y la que tiene que gastar unos recursos determinados para reducir dichos riesgos.

Por el contrario, su principal inconveniente es que tratar los activos sobre la base de su valoración económica hace que el método sea más costoso, ya que realizar la estimación económica de determinados activos es laborioso.

4.2. NIST

Esta metodología es de origen americano, y tiene la ventaja de que las valoraciones que se realizan no son económicas, sino que son más cualitativas.

Las fases de este análisis de riesgos son las siguientes:



En el fondo, estas etapas son las mismas que en la metodología MAGERIT, con la diferencia de que las vulnerabilidades no se entienden como frecuencia de ocurrencia, sino como auténticos agujeros de seguridad, y durante el estudio se realiza la identificación de dichas vulnerabilidades.

Para realizar el cálculo de los riesgos debe estimarse la frecuencia y el impacto en tres niveles: bajo, medio y alto. Y a partir de ahí se establece un cuadro de cruces que serán los riesgos que resultan de este estudio.

Probabilidad de la amenaza	**Impacto**		
	Bajo (10)	**Medio (50)**	**Alto (100)**
Alto (1,0)	Bajo	Medio	Alto
Medio (0,5)	Bajo	Medio	Medio
Bajo (0,1)	Bajo	Bajo	Bajo

Con posterioridad, se deberá marcar el umbral de riesgos, clasificándolos en tres niveles:

- **Riesgo alto**. Requerirá implantar alguna medida de seguridad para reducirlos.

- **Riesgo medio**. Requiere aplicar medidas para controlar el riesgo en un periodo de tiempo razonable, siempre y cuando no queden riesgos altos por reducir.

- **Riesgo bajo**. Se analiza si se acepta el riesgo o si se debe aplicar alguna medida de control.

Esta metodología se aplicaría, por ejemplo, de la siguiente forma:

Activo	Vulnerabilidad	Amenaza	Fuente			Característica			Riesgo	Impacto	Probabilidad
			Natural	Humana	Entorno	Disponibilidad	Confidencialidad	Integridad			
Director general	No cláusula de exclusividad	Oferta competencia		X		X	X		0,5	100	Media
Base datos cliente	Mala configuración	Publicación de datos privados		X			X		0,1	100	Baja
Imagen	Política *firewall* inadecuada	Cambio contenido web		X				X	0,1	100	Baja

En este ejemplo, primero se analizarían los activos de la organización (columna de la izquierda). Seguidamente, se identifican las vulnerabilidades que presentan estos activos y, en un tercer paso, se determinan las amenazas que podrían utilizar las vulnerabilidades identificadas.

El siguiente paso sería identificar el origen de estas amenazas, es decir, si han sido de origen humano, de origen natural o se han originado en el entorno.

Seguidamente, debe identificarse la característica de la seguridad de la información que se vería afectada por la situación: la integridad de la información, la confidencialidad o su disponibilidad.

A partir de ahí, se debería estimar la probabilidad de que esta situación llegara a darse, así como el impacto que podría provocar este cruce de amenaza y vulnerabilidad. Sobre la base del cruce de estos dos factores se determinará el riesgo al que la organización se encuentra expuesta.

Por último, se tendría que establecer el plan de acción para reducir estos riesgos.

4.2.1. Conclusiones de NIST

Esta metodología resulta mucho más sencilla que MAGERIT en cuanto a su aplicación, debido a que no es necesario hacer un estudio tan pormenorizado de cada activo para asignarle una valoración. Además, también es más sencillo asignar tanto la probabilidad como el impacto.

Sin embargo, esta metodología no permite designar demasiado claramente los riesgos reales a los que se encuentra expuesta la organización, puesto que únicamente indica tres niveles de riesgos: no clasifica, dentro de los que son considerados altos, cuál es más alto o cuál supone un mayor riesgo.

Una forma de aprovechar esta metodología podría ser utilizándola en grandes alcances para identificar con claridad los riesgos más altos a gran escala que posee la organización. Después se utilizaría una segunda metodología (MA-

GERIT o CRAMM) para analizar con más detalle los riesgos propios de estos activos que han sido identificados como aquellos que tienen los riesgos más elevados.

4.3. CRAMM

Esta metodología es de origen británico, y su característica principal es el uso de valoraciones numéricas para el cálculo de los riesgos a los que se encuentra expuesta una organización.

Los valores que se requieren para aplicar CRAMM son los siguientes:

- **Valoraciones de los activos**. Entendidas como el valor que tiene ese activo dentro del alcance que se está estudiando.

- **Estimación de las probabilidades**. Entendida como la probabilidad de que una amenaza, aprovechando una vulnerabilidad, dañe un determinado activo.

- **Estimación de los impactos**. Entendida como las consecuencias que tendría para la organización el hecho de que una amenaza aprovechara una vulnerabilidad para dañar a un activo.

Las valoraciones que deben asignarse al utilizar CRAMM suelen ser de 1 a 5, siendo el valor de 1 el activo con menor valor, o la probabilidad más baja de que una determinada amenaza afecte a la organización, o el menor impacto posible que pueda provocarse en una organización.

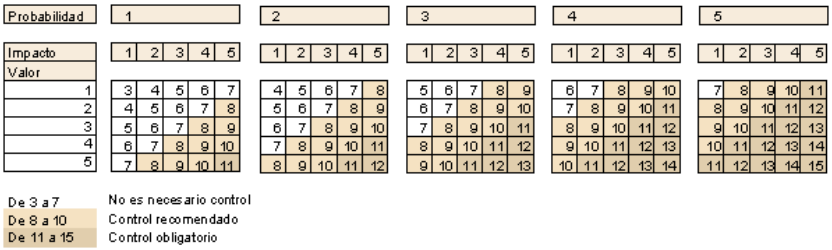
Y, de la misma forma, el valor de 5 será aquel activo que tenga el máximo valor para la organización, o aquella probabilidad más elevada de que llegue a suceder un incidente, o el mayor impacto posible que aquél pueda provocar.

Para calcular el riesgo al que está expuesto un activo ante esas amenazas y sus vulnerabilidades, lo único necesario sería realizar la suma de estos tres valores.

Valor + Probabilidad + Impacto

A raíz de estas posibilidades, el rango de valores para identificar los riesgos irá desde el menor de los posibles, que sería de 3, hasta el mayor, que equivaldría a 15.

El cuadro resultante de estos riesgos sería el siguiente:



Probabilidad	1	2	3	4	5
Impacto	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
Valor					
1	3 4 5 6 7	4 5 6 7 8	5 6 7 8 9	6 7 8 9 10	7 8 9 10 11
2	4 5 6 7 8	5 6 7 8 9	6 7 8 9 10	7 8 9 10 11	8 9 10 11 12
3	5 6 7 8 9	6 7 8 9 10	7 8 9 10 11	8 9 10 11 12	9 10 11 12 13
4	6 7 8 9 10	7 8 9 10 11	8 9 10 11 12	9 10 11 12 13	10 11 12 13 14
5	7 8 9 10 11	8 9 10 11 12	9 10 11 12 13	10 11 12 13 14	11 12 13 14 15

De 3 a 7	No es necesario control
De 8 a 10	Control recomendado
De 11 a 15	Control obligatorio

Según el gráfico anterior, lo que tendría que asignarse es el umbral de riesgos para cada organización. En este caso, la organización ha estimado que los riesgos inaceptables, y por lo tanto aquellos que obligatoriamente necesitan la implantación de una medida de seguridad, serán los valores que están entre el 11 y el 15 (ambos incluidos). Después, en un segundo nivel, vendrían los controles recomendables, es decir, aquellos que, una vez que la organización ha reducido todos los riesgos anteriores, debería tratar de implantar si es que tiene recursos para hacerlo. Serían los riesgos situados entre el valor 8 y el 10. Por último, quedarían los riesgos menores, que como tales no requerirían protección, ya que es posible que la propia protección fuese más costosa que el riesgo en sí (de 3 a 7).

En este sentido, debe quedar muy claro que lo prioritario de la gestión de los riesgos es reducir aquellos que están por encima del umbral de riesgos y que lo secundario, si es posible, es reducir los menos amenazantes. No es lógico que se reduzca un riesgo de segundo nivel si todavía quedan riesgos inaceptables por contrarrestar.

4.3.1. Valoraciones de CRAMM

Esta metodología tiene como gran ventaja el hecho de que es fácil de aplicar, ya que no entra en valoraciones económicas como MAGERIT, lo que hace que sea más sencillo asignar valores a los activos. Al mismo tiempo, identifica dentro de los diferentes niveles de los riesgos la priorización de cada uno de aquéllos, cosa que MAGERIT también permite pero no en cambio NIST.

El inconveniente es que los resultados que se expresan están indicados en números, lo cual no refleja realmente la dimensión del riesgo al que se encuentra expuesta una organización, puesto que, en comparación con MAGERIT, hablar de un riesgo de 12 no es lo mismo que hablar de un riesgo de 23.000 €. Por ello esta metodología lleva asociado un segundo proceso consistente en la traducción de esos riesgos a unas valoraciones económicas, de forma que sean defendibles ante la dirección.

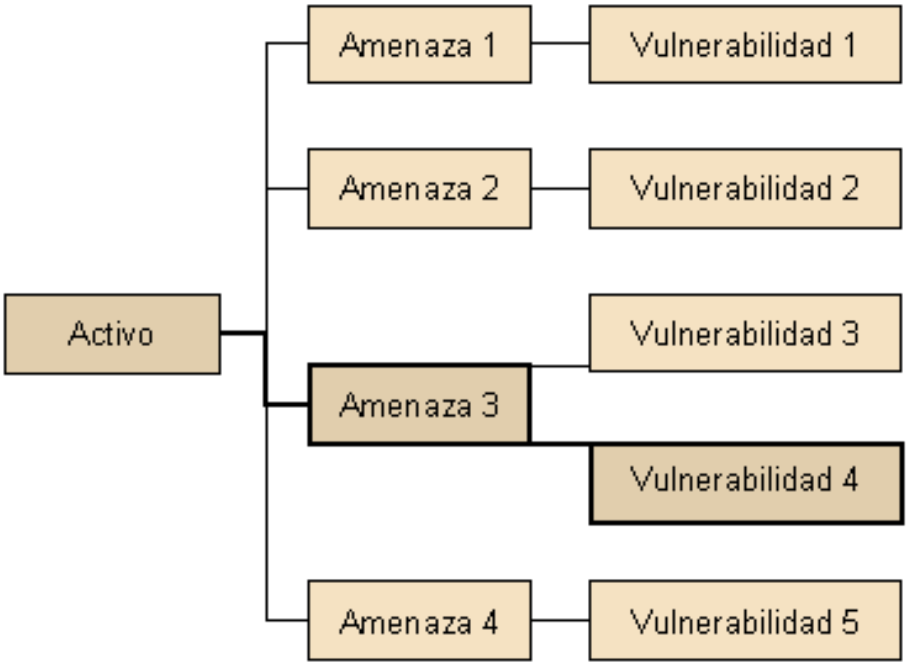
4.4. OCTAVE

Esta metodología es de origen británico, al igual que CRAMM, pero tiene un modo de representar los riesgos a los que se encuentra expuesta una organización totalmente diferente a las anteriores.

OCTAVE requiere entrar en un proceso iterativo de revisión para tratar de obtener una reducción de todos los riesgos a los que se encuentra expuesta una organización.

La metodología acaba traduciéndose en la construcción de un árbol de riesgos en el que queda marcado cuál es el camino más crítico ante el que la organización tiene que actuar primero. Una vez que se consigue reducir este riesgo, será necesario que se repita el estudio para volver a encontrar el siguiente camino crítico, y así sucesivamente hasta reducir todos esos riesgos.

El resultado acaba siendo el siguiente:



Después de su aplicación, OCTAVE nos indica la primera actuación que una organización debería llevar a cabo en el caso de que quiera reducir los riesgos a los que está sometida. No es que el resto de riesgos no sean importantes: simplemente indica que una determinada combinación es la que posee un riesgo más elevado.

4.4.1. Conclusiones OCTAVE

Esta metodología tiene como aspecto positivo que es necesario centrarse en analizar todas las situaciones con el detalle que otras metodologías requieren. En cambio, tiene como gran inconveniente que se debe completar un ciclo de revisión del análisis para acabar de identificar todos los riesgos que en cada ocasión son los más críticos.

Actividades

La empresa en la que trabajas, Servicios S. L, ha decidido poner en marcha un sistema de información que ofrecerá servicios de *hosting* y *housing* a sus clientes, ya que son servicios que se solicitan a menudo. Se ha pensado en dar un servicio 7 × 24:

- **Personal**
  - Responsable de proyecto
  - **3 + 3 operadores** (entre semana: 3 turnos diarios, en fin de semana: 3 personas, distribuidas según su conveniencia)
  - **2 becarios** (soporte)

- **Equipamiento:**
  - 4 estaciones de trabajo
  - 1 servidor que contiene: 1 servidor de DNS, 1 servidor de BBDD (MySQL), 1 servidor web (Apache), 1 impresora y 1 servidor de aplicaciones (Tomcat)
  - 1 aire acondicionado

Todo estará incluido dentro de la red corporativa como uno o varios segmentos de red más. La dirección quiere evaluar si es viable el proyecto con el presupuesto del que disponen, haciendo un análisis de riesgos realista. Además, quiere evitar el posible robo de información.

- Analiza los riesgos intrínsecos de este sistema y propón soluciones a los mismos.
- Analiza los riesgos residuales después de aplicar las contramedidas propuestas en el análisis de riesgos intrínsecos.

(El ejercicio debe realizarse escogiendo una de las metodologías explicadas en el módulo. Deben justificarse y explicarse las soluciones escogidas, así como las conclusiones obtenidas.)