Universidad Rey Juan Carlos

Escuela Superior de Ingeniería Informática

INGENIERÍA INFORMÁTICA

Curso Académico 2010/2011

Proyecto Fin de Carrera

Estudio del Análisis de Riesgos TIC mediante una Visión Probabilística

Autores:

José Antonio Almena Muñoz

Guillermo Ortega Gallardo

Tutores:

David Ríos Insua

José Antonio Rubio Blanco

20 de junio de 2011

Agradecimientos

Agradecer especialmente a David Ríos y a José Antonio Rubio su ayuda, consejo y guía durante el desarrollo de este proyecto.

También agradacemos la ayuda prestada desde varias de las instituciones consultadas, las cuales nos han ofrecido de manera desinteresada la información de la que disponían, resultando de gran utilidad.

Por último, nos gustaría dar las gracias especialmente a todas las amistades que se han preocupado por el avance de nuestro estudio, a María por ser uno de los apoyos más importantes y un empuje continuo para seguir adelante con el proyecto, y a nuestras familias por todo el ánimo que nos han hecho llegar.

Resumen

El siguiente estudio aborda el campo del análisis de riesgos desde una perspectiva probabilística con la que poder afrontar el carácter dinámico de las amenazas actuales que afectan a los entornos TIC. El objetivo del mismo será proporcionar una alternativa necesaria para las infraestructuras informáticas presentes, pues cuentan únicamente con marcos de análisis y gestión de riesgos estáticos. Éstas no hacen un estudio adecuado de las interdependencias entre los diversos activos, así como de las amenazas potenciales a las que se pueden ver afectados.

En concreto, se mostrará una comparativa con la metodología MAGERIT, que cuenta con gran difusión en el ámbito nacional. Se mostrará cómo este tipo de herramientas aportan una valiosa ayuda para agrupar los distintos activos, amenazas y salvaguardas que tienen lugar en una institución cualquiera. No obstante, una vez realizado dicho análisis previo de modelización, se requiere un enfoque probabilístico más profundo que sea capaz de cuantificar en mayor grado la seguridad de nuestros sistemas. En este proyecto se expondrá dicho enfoque, pudiendo ver que es la forma más natural y eficaz para afrontar este complejo problema.

Índice general

Agradecimientos I

Resumen II

1. Introducción 1

2. Estado del arte 4

2.1. MAGERIT: Metodología de Análisis y Gestión de Riesgos 5

2.2. Análisis crítico de la metodología MAGERIT 22

2.3. Alternativas a MAGERIT 26

3. Modelo Discreto 29

3.1. Análisis de riesgos 34

4. Fuentes de datos para un Modelo Continuo 60

4.1. Amenazas 60

4.2. Resultados globales del estudio 85

5. Conclusiones y trabajos futuros 87

Bibliografía 90

Capítulo 1

Introducción

Actualmente se viene dando una gran importancia al llamado análisis de riegos en general y, en particular, en el campo de las TIC, ya que gracias al mismo se pueden estructurar y cuantificar todos los riesgos asociados a los activos de una infraestructura tecnológica dada. Con estas bases, se puede realizar una toma de decisiones más fundada en lo relativo al ciclo de vida de estos sistemas y, más concretamente, sobre las posibles debilidades o amenazas que se pueden presentar. Por otro lado, se puede establecer como un hecho probado la idea de que los riesgos TIC no sólo dependen de la seguridad de los sistemas informáticos por sí misma, ya que otros factores pueden producir un suceso anómalo en nuesto sistema.

Si tuviéramos que segmentar dichas amenazas que pueden tener cierto impacto en nuestra infraestructura TIC, a nivel muy general podríamos establecer los siguientes grupos:

- Amenazas internas y externas realizadas por atacantes (Seguridad)
- Políticas de TIC (Cumplimiento de normativas)
- Desastres naturales y fallos del sistema (Disponibilidad)
- Rendimiento de las aplicaciones y rendimiento TIC (Rendimiento)

Ante tal abundancia de elementos complejos a considerar, y teniendo en cuenta la necesidad de dichos estudios explícitamente para sistemas TIC críticos (ej. sistemas de abastecimiento eléctrico, control nuclear, gobierno electrónico, etc), la realidad es que se están usando metodologías o procesos que no se encuentran a la altura de su criticidad. Esto se debe a que los mismos, aun considerando de forma muy aguda cuestiones como la identificación de activos, amenazas o contramedidas, se plantean desde una óptica estática que deja de lado cuestiones importantes, como el carácter dinámico de los sistemas o la necesidad de mejorar los modelos de cuantificación del riesgo. De igual modo, es un

hecho constatado que la seguridad presente en la mayoría de las organizaciones privadas e instituciones públicas peca de tremendas debilidades, que dejan en entredicho la supuesta profesionalidad de los equipos de trabajo presentes en ellas. Así, nos encontramos ante un panorama en el que una gran multitud de sistemas críticos no cuentan siquiera con unos riesgos residuales acordes al posible impacto que tendría lugar en caso de que tales activos se vieran afectados. Es decir, dichos entes no han procedido a dimensionar adecuadamente sus parámetros de seguridad, con lo que la supervivencia de sus negocios podría peligrar en cualquier momento.

Para intentar paliar esta problemática, dentro del campo de la informática, surgió la rama de la Ingeniería del Software, la cual realmente no ha conseguido alcanzar una respuesta suficientemente eficaz frente a los retos tecnológicos que se dan en el día a día. Ante este hecho, algunos expertos indican que la informática es una ciencia aún demasiado joven, no pudiéndose comparar con otras de mayor historia y, por tanto, achacando a dicha inexperiencia la raíz de un panorama tan poco halagüeño. De igual modo, nos encontramos con que en multitud de empresas y proyectos profesionales la seguridad se deja claramente a un lado, dando demasiada prioridad a las funcionalidades y plazos a cumplir, con lo que el problema se arrastra una y otra vez sin llegar a una solución.

Por otro lado, en el campo de la seguridad y del análisis de riesgos no se cuenta, en muchos casos, con el reconocimiento que merece, dándose la situación de que hallar profesionales debidamente cualificados es una labor realmente complicada. Ante esta tarea pendiente, si se quiere conseguir enfrentrarse a las amenazas tecnológicas existentes con una seguridad real, se debe alcanzar un debida concienciación y especialización, esto será lo único que hará posible el repunte del sector.

De igual modo, y muy ligado a lo anteriormente comentado, hemos de tener en cuenta que la mayoría de los sistemas de seguridad existentes en el mercado actual no son capaces de dar una respuesta eficaz e integral a todos los riesgos que se dan en los entornos profesionales (European Commission, 2002) . Ejemplo de ello son las probadas ineficacias de elementos como los firewalls, que requieren en muchos casos de una labor de diseño sumamente ardua, ya que el conjunto de reglas que ha de estar presente en su núcleo requiere de una actualización constante, lo cual no suele ser la norma en muchas instituciones. Asimismo, los Sistemas de Detección de Intrusos (IDS) pueden quedar sobrepasados si nuestro perímetro ya ha sido contaminado por elementos tales como páginas Web maliciosas o redes inalámbricas desprotegidas, por lo que podemos incluso tener una engañosa imagen de seguridad cuando, en verdad, tenemos agujeros de seguridad no detectados, lo cual es todavía más peligroso.

A su vez, factores limitantes como el alto coste de estas herramientas en su despliegue

corporativo, la posible carga que pueden acarrear en las infraestructuras existentes, los falsos positivos o, incluso, la inexistencia de un presupuesto acorde a las necesidades de seguridad reales hacen de la gestión de este dominio un problema de control complejo.

De este modo, queda patente la necesidad de contar con una visión introspectiva, gracias a la cual se pueda saber con certeza toda la información concerniente a nuestros activos, los posibles riesgos a los que se pueden ver sometidos, así como a las salvaguardas existentes para mitigar dichas incidencias (Anderson, 2001).

En definitiva, necesitamos un paradigma capaz de producir elementos de control claros y eficaces para gestionar correctamente la seguridad de nuestras TICs. Aún así, el presente campo del análisis de riegos no ha sabido sacar todo el potencial a los diversos dominios de conocimiento existentes por lo que, en muchos casos, nos encontramos ante meros estudios cualitativos, en los cuales las valoraciones extraídas son poco tangibles, justamente por el carácter poco concreto de las observaciones y estudios llevados a cabo.

Es por eso, de cara a dar mayor credibilidad y sofisticación a este campo, nos proponemos renovar y mejorar las actuales técnicas y métodos de análisis de riesgos mediante el uso de técnicas probabilísticas, pudiendo así medir de una forma mucha más veraz y eficaz las dimensiones del riesgo en nuestros activos y procesos de negocio. De igual modo, al realizar un análisis cuantitativo estaremos en condiciones de medir con exactitud las posibles pérdidas a que estamos sometidos, así como evaluar el mejor uso de nuestro presupuesto en función de las salvaguardas a considerar. Todo un reto que puede ayudar al avance en áreas poco desarrolladas, como los planes directores de seguridad o las directrices de monitorización, evaluación y mejora de los sistemas TIC.

Por todo ello, el presente trabajo ofrece una solución para unir las ramas de las Ciencias de la Decisión y el análisis de riesgos en las TIC, pudiendo así alcanzar una respuesta a la problemática que viene dañando la profesionalidad y eficacia de las infraestructuras informáticas actuales. En el capítulo que viene a continuación se mostrará la visión actual que se está utilizando este campo, poniendo de ejemplo la conocida metodología MAGERIT. En él se detallarán sus virtudes y sus debilidades, éstas últimas son las que intentaremos cubrir en este estudio. En el capítulo tercero se presentarán ejemplos concretos donde nuestro enfoque probabilístico funciona de manera mucho más eficiente. En un cuarto capítulo afrontaremos el modelo recientemente expuesto, aportando en este caso datos extraídos de la vida real. Por último, y para finalizar, expondremos unas conclusiones al respecto de este campo comentando el trabajo futuro a desarrollar.

Capítulo 2

Estado del arte

Según se entiende en la actualidad, el análisis de riesgos TIC cuenta con un ciclo de vida propio, en el que, primero, encontramos una fase de análisis per se, donde se identificarán todos los activos presentes en la institución bajo estudio. Posteriormente, se elaborará de igual modo el necesario mapa de dependencias entre todos estos activos, de cara a saber con exactitud las posibles relaciones que se pudieran producir en las operaciones de negocio. Por otro lado, se procederá a identificar las posibles vulnerabilidades a que pueden estar expuestos tales activos, teniendo así una clara visión de los posibles incidentes a los que nos podemos enfrentar.

Una vez realizado dicho estudio, pasaríamos a realizar la fase de evaluación de riesgos donde, con ayuda de los interesados, se vería la ponderación exacta de cada uno de los activos y procesos, ya que su criticidad variará de cara al negocio en función del impacto que pueda suponer su caída. Por otro lado, se estudiarán las salvaguardas que ofrece el mercado, con las que construir adecuadamente un plan de contingencia capaz de preservar la supervivencia de nuestra organización. Finalmente, una vez que contamos con todos estos elementos, estaremos en condiciones de decidir qué plan director de seguridad hemos de seguir, ya que, en función de nuestro presupuesto y de las valoraciones extraídas anteriormente, se implantarán unas u otras medidas. En esta última fase de gestión se procederá a implantar dichos objetivos, procediendo a su monitorización y evaluación continua, con la que mantener un ciclo de mejora continuo.

En ENISA (European Network and Information Security Agency) podemos encontrar la información concerniente a diversas metodologías existentes de análisis y gestión de riesgos en TIC en la dirección Web http://www.enisa.europa.eu/act/rm. Algunos ejemplos son EBIOS, de uso en Francia; CRAMM, procedente de la administración pública británica; o MAGERIT, que fue diseñado para el Ministerio de Administraciones Públicas de España. Todas ellas poseen, en mayor o menor medida, métodos y técnicas para identificar y clasificar el total de los activos pertenecientes a cualquier tipo de organización,

así como para valorar sus dependencias entre sí y la importancia de éstos para el correcto funcionamiento de los sistemas informáticos involucrados. Una vez identificados dichos elementos, se nos dan indicaciones para calcular parámetros como el impacto y el riesgo acumulados.

A continuación se verá en mayor detalle cuáles son los componentes que conforman la metodología MAGERIT (Ministerio de Administraciones Públicas, 2006), ya que al hacer uso de todos los planteamientos y métodos estándar propios del campo del análisis de riesgos nos servirá para presentar una adecuada imagen de cómo se trata actualmente esta problemática en el sector.

2.1. MAGERIT: Metodología de Análisis y Gestión de Riesgos

La Administración española viendo que los sistemas de información son parte esencial de nuestra forma rutinaria de trabajar, decidió diseñar una metodología que facilitara el poner bajo control la explotación de estos sistemas. Por otro lado, se ha visto cómo dichos elementos han pasado de estar bajo la amenaza de unos pocos ataques a ser el blanco de infinidad de ellos, donde los posibles actores, malintencionados o no, no hacen sino crecer con el transcurso del tiempo.

Así, la faceta de seguridad ha pasado de ser un aspecto más a controlar a convertirse en un parámetro crítico, sin el cual el día a día de los servicios TIC no podría desempeñarse en la forma esperada. Para controlar todos estos componentes, aplicaciones, sistemas operativos o instalaciones físicas, se vio claramente la necesidad de contar con una metodología capaz de gestionar de forma integral todo la dimensión relativa a la seguridad. Una tarea ingente pero que, bien enfocada, fue arrojando resultados tangibles, con los cuales empezar a arrojar luz a este panorama tan complejo y dinámico. En primer lugar, se llegó al concepto de riesgo, el cual requería ser definido con mayor precisión y eficacia. Se entendió que éste era motivado por la aparición de incidentes, los cuales degeneraban en consecuencias negativas de mayor o menor grado. Así, se introdujo el término de impacto, que indica, simplemente, la posibilidad de que un hecho no esperado ocurra en nuestras operaciones TIC.

Entre este riesgo e impacto mediaba un factor de incertidumbre, el cual venía a indicarnos que si un evento dado puede ocurrir con cierta probabilidad y que si el Impacto causado puede llegar a ser importante resultaba convertirse en un riesgo de cierta criticidad. En cambio, si la probabilidad de aparición fuese baja y el impacto mínimo, dicho riesgo seguiría existiendo, pero sus consecuencias vendrían a ser consideradas como de ba-

ja importancia. Estos incidentes ocurren en los llamados activos de información o activos del sistema que, según su naturaleza, pueden ser más o menos vulnerables ante ciertas amenazas o incidentes. Según éstos, podríamos dilucidar la medida de degradación de los activos, que pueden quedar arruinados o, simplemente, sufrir algunas consecuencias menores según la problemática afrontada. Asimismo, estos activos pueden estar más o menos expuestos al gran número de amenazas existentes, ya que no es lo mismo hablar de un sistema que tiene lugar bajo un entorno protegido, a otro que no dispone en absoluto de medidas disuasorias. Por otro lado, esta metodología también incluyó en su núcleo el concepto de valor, ya que, según la criticidad de los activos, éstos tendrán un valor más o menos elevado, siendo esta información de vital importancia para poder hacer una correcta planificación de la seguridad en nuestros sistemas. En definitiva, si no supiéramos con exactitud cuáles son los activos más importantes de las infraestructuras TIC no podríamos centrar nuestros esfuerzos en su protección, con lo que, seguramente, no seríamos capaces de reducir las potenciales vulnerabilidades que puedan tener lugar. Una incorrecta visión que haría que estuviéramos contantemente en situaciones de alto riesgo, al no tener verdadera consciencia de la situación real de nuestras infraestructuras TIC. Por todo ello, el riesgo, en caso de no ser tratado, puede considerarse como un coste potencial que requiere ser minimizado de forma dinámica, no siendo nunca superior al posible beneficio de los activos a los que se refiere. Para llevar a cabo tal proceso de minimización, deberemos desplegar toda una serie de salvaguardas que transformen nuestro escenario actual en un entorno más seguro y controlado, ya sea mediante la reducción de las vulnerabilidades o bien limitando el impacto, en caso de que ocurrieran. Dentro de este panorama podríamos, por fin, hablar de un riesgo reducido o riesgo residual, que será uno de los principales objetivos a conseguir por medio de MAGERIT.

Teniendo en cuenta todos estos elementos, la Administración española entendió que conseguiría una herramienta acorde a estas necesidades, para lo cual sumó de igual modo a esta metodología los conceptos típicos de:

- *Disponibilidad:* disposición de los servicios para ser usados en cualquier momento. Es decir, la imposibilidad de que existan interrupciones del servicio, con las consecuentes pérdidas de productividad.

- *Integridad:* mantenimiento de las características de completitud y corrección de los datos. Se evitan así manipulaciones indeseadas sobre la información que afecten al correcto desempeño de las funciones de una organización.

- *Confidencialidad:* mantenimiento privado de la información para que sólo llegue a las personas autorizadas. En esta dimensión de seguridad se evitan las fugas y

filtraciones de datos, así como los accesos indebidos a nuestros sistemas.

- *Autenticidad:* certeza de quién actúa en cada momento sobre la información y servicios, pudiendo así anular cualquier tipo de fraude que pudiera tener lugar. De igual modo, con esta característica de seguridad se lucha contra el repudio, factor necesario para el correcto desempeño del comercio electrónico o la administración electrónica.

Asimismo, las metodologías actuales de análisis y gestión de riesgos tienen muy en cuenta las interdependencias existentes entre los diversos activos de un sistema, ya que, debido a la creciente complejidad de las infraestructuras TIC, existen flujos de información compartidos por un gran número de vías que, a priori, podrían no ser consideradas (Kunreuther, H. y Heal, G. , 2003) . Por el mismo motivo, los componentes puramente tangibles, como instalaciones físicas, personal humano o equipamiento electrónico, también han de considerarse con sumo cuidado, ya que las operaciones de infinidad de servicios dependen directa o indirectamente de ellos.

También merece un apartado especial la forma de realizar las valoraciones sobre los diversos aspectos, ya que no se ha de realizar a la ligera. Por ejemplo, se cometería un grave error si directamente se pensara que un sistema costoso ha de merecer mayor consideración que otro barato, ya que el coste de interrupción de este último podría llegar a superar el perjuicio económico que si el activo afectado fuese el primero. Por ello, en MAGERIT, al igual que en el resto de las principales metodologías de análisis de riesgos TIC existentes, se hace una valoración cuantitativa respecto a:

- Costes de reposición de equipamiento, instalaciones y personas
- Costes por pérdida de productividad
- Costes por tareas de recuperación: horas extra, contratación adicional, etc
- Coste por lucro cesante: pérdida de negocio
- Coste por incumplimiento legal, regulatorio o contractual, así como de otros valores más intangibles asociados a:
- La pérdida de competitividad
- La credibilidad frente a usuarios, clientes, la sociedad, etc
- La capacidad de perseguir el fraude o el abuso de los medios

Una vez tenidas en cuenta estas valoraciones, habrá que compararlas posteriormente con el coste de las salvaguardas, viendo si son proporcionales al riesgo que conjuran o si, por el contrario, son desproporcionadas. Así, una vez tengamos en nuestro poder toda esta información, estaremos en disposición de comparar dichos costes económicos con la valoración cuantitativa de dicho sistema o componente dentro de los servicios finales existentes.

De igual modo, y como ya se ha comentado brevemente, los incidentes de seguridad ocurren sobre los componentes del sistema: los equipos se rompen, las cuentas se asaltan, las líneas de comunicación se interceptan, los locales se queman, las personas no están disponibles, etc. Por ello, hemos de analizar nuestro despliegue de activos para determinar las vulnerabilidades existentes para cada tipo de amenaza y cómo éstas tienen un impacto y riesgo global sobre los servicios TIC en su conjunto. Algunas ecuaciones que usa MAGERIT, donde se considera el valor acumulado sobre los activos, son las siguientes:

- impacto = valor acumulado x degradación resultante
- riesgo = impacto x probabilidad del incidente

Así, sabremos que un cierto activo está sometido a un cierto riesgo a consecuencia de que:

- Sobre él reside una parte importante del valor exterior del sistema
- La degradación causada por un incidente sería grande
- La probabilidad de que el incidente ocurra es elevada

Conociendo el riesgo acumulado en los activos, podremos tomar decisiones concretas para salvaguardarlos. Es más, si la valoración fuese cuantitativa, se podría comparar el coste de las salvaguardas y justificar su necesidad.

Como estas valoraciones en algunos momentos pueden llegar a resultar demasiado técnicas, MAGERIT intenta bajar hasta cierto punto al nivel de negocio, para poder comunicarse de forma más eficaz con la Dirección. En este caso, se entiende que los incidentes se producen sobre un cierto activo, el cual, a su vez, soporta unos servicios exteriores conocidos, teniendo así que proceder a calcular el impacto y el riesgo sobre el valor de los activos indirectamente afectados:

- impacto repercutido = valor propio x degradación consecuencia del incidente
- riesgo repercutido = impacto repercutido x probabilidad del incidente

De este modo, sería más fácil interpretar los resultados en términos de negocio, con una clara perspectiva de organización. Así ésta podría considerar que un riesgo elevado es asumible si en verdad no afecta a la supervivencia de la institución, mientras que incidentes técnicamente residuales pueden suponer un grave perjuicio, no debiendo ser admitidos.

También son muy importantes dentro de estas metodologías los conceptos de actuación respecto al riesgo, ya que éstos se pueden afrontar desde distintas perspectivas:

- Evitándolo: no siempre es posible ya que la actividad de una organización consiste en asumir unos ciertos riesgos a cambio de abrir unas ciertas expectativas.
- Reduciéndolo: se decide convivir con el riesgo, pero cambiando su perfil. Se adoptan una serie de salvaguardas que reducen el impacto posible, o que directamente imposibiliten o hagan improbable tales incidentes.
- Transfiriéndolo: se convive con los incidentes pero se pasan las consecuencias a otra organización. De este modo se externalizan servicios, como la propia gestión de la seguridad, o se contratan seguros que nos resarzan de pérdidas en caso de que ocurran tales hechos. Esta transferencia no es gratis, por lo que siempre hay que cotejar el riesgo residual con el incremento de coste derivado de la transferencia.
- Asumiéndolo: en última instancia, el riesgo puede que parezca proporcionado a los beneficios que se esperan, con lo que se pasa tal riesgo al capítulo de costes operativos de la organización.

Otro factor que se repite en todas las metodologías de análisis y gestión de riesgos existentes es la clara compartimentación del problema en sucesivas fases que se retroalimentan. Cada una conlleva la puesta en práctica de unas determinadas actividades, gracias a las cuales se irá profundizando cada vez más en la naturaleza de los riesgos a tratar, así como en las tareas más granulares a desempeñar. Estas fases son las que siguen:

1. Planificar. En esta fase encaja el análisis de riesgos ya que se realiza la identificación y estimación, así como la calificación en términos de negocio. De esta fase se concluye un plan, que puede ser de mejora y, en todo caso, ha de incluir siempre las operaciones a desempeñar.
2. Implantar y operar. En esta fase seguimos el plan de seguridad, quizás con sus actividades de mejora de la seguridad y siempre con el plan rutinario de operación, mantenimiento y gestión de incidencias.

3. Monitorizar y evaluar. No basta con desplegar las salvaguardas. Es necesario cerciorarse de que cumplen con su misión eficaz y eficientemente. Primero, porque una salvaguarda que no mitigue el riesgo es dinero y esfuerzo perdidos. Segundo, porque la salvaguarda puede resultar más costosa que el riesgo que mitiga (en coste técnico, pérdida de productividad, pérdida de oportunidades, etc). Tercero porque el análisis teórico de los riesgos puede no corresponderse exactamente con la realidad, por lo que es necesario hacer una monitorización lo más exacta y fiable posible.

4. Mantenimiento y mejora: la experiencia propia y la experiencia de otras organizaciones similares a la nuestra nos deben llevar a repensar lo que estamos haciendo. No incorporar la mejora del conocimiento a la planificación del siguiente período sería un grave error y podría condenar a la organización a su desaparición.

Para este conjunto de cuestiones, MAGERIT ofrece una guía metódica y estructurada para concienciar a los responsables de sistemas TIC de la existencia de riesgos y de la necesidad de atajarlos a tiempo, así como para analizar dichos riesgos de forma sistemática. Con ello se ayudaría a descubrir y planificar las medidas oportunas para mantener tales amenazas bajo control, preparando a la organización para cualquier tipo de proceso de evaluación, auditoría, certificación o acreditación.

A nivel técnico, los métodos más sofisticados que usa MAGERIT son análisis mediante tablas y árboles de ataque. Por otro lado, se ofrecen análisis de coste-beneficio, diagramas de flujos de datos, técnicas de planificación de procesos o valoraciones Delphi. En cualquier caso, esta metodología, como la mayoría de las existentes en la actualidad, sólo busca ofrecer una imagen del estado actual sin profundizar demasiado, con lo que es en este punto donde se requiere de la introducción de métodos más sofisticados y robustos, que sean capaces de afrontar el carácter dinámico del problema.

El marco general de MAGERIT se describe en la figura 2.1, donde vemos cómo se parte de los activos, que se valoran según su nivel de importancia, detallando asimismo las amenazas a que están sujetos. Éstas, según MAGERIT, crearían un grado potencial de degradación que daría lugar a un impacto medible. Finalmente, en la imagen se aprecia cómo en función de la frecuencia de dichos incidentes y del impacto citado se obtendría el riesgo posible para cada activo del sistema bajo estudio.

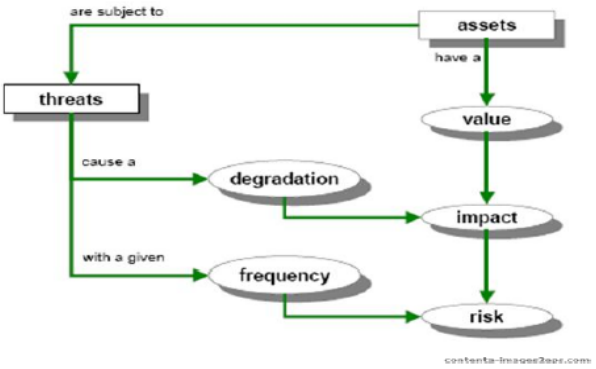


Figura 2.1: Marco de MAGERIT

En cuanto a contribuciones positivas de MAGERIT, nos encontramos con que suministra un catálogo muy detallado de posibles activos y amenazas, que ahorra una gran cantidad de tiempo a los responsables TIC encargados de elaborar el análisis y la gestión de riesgos.

Identificación de activos

Según se contempla en el catálogo de elementos de MAGERIT los activos que están tipificados de forma jerárquica son los siguientes:

1. Servicios
    - Servicios anónimos
    - Servicios al publico en general
    - Servicios a usuarios externos
    - Servicios internos
    - Servicios contratados a terceros
    - World Wide Web
    - Acceso remoto a cuenta local
    - Correo electrónico
    - Almacenamiento de ficheros
    - Transferencia de ficheros
    - Intercambio electrónico de datos
    - Servicio de directorio
    - Gestión de identidades

- Gestión de privilegios
- Infraestructura de clave pública

2. Datos

- Datos vitales
- Datos de interés comercial
- Datos de interés para la administración pública
- Datos de gestión interna
- Voz
- Multimedia
- Código fuente
- Código ejecutable
- Datos de configuración
- Logs
- Datos de prueba
- Datos de carácter personal de nivel básico, medio o alto
- Datos clasificados

3. Aplicaciones

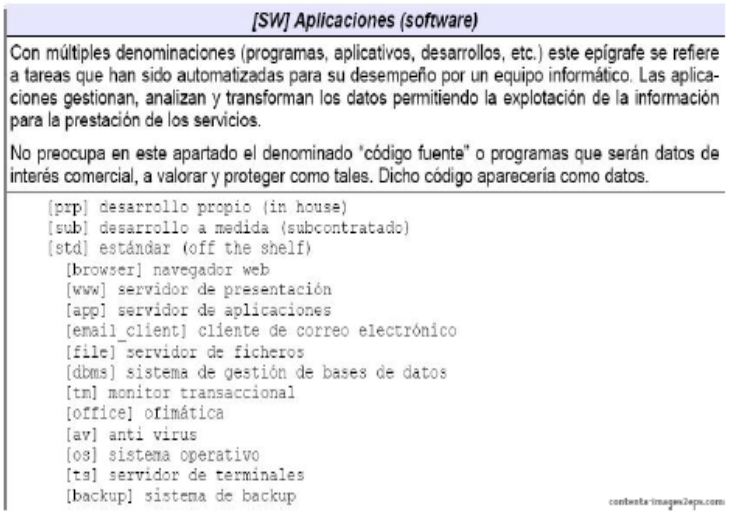
- Desarrollo propio
- Desarrollo a medida
- Desarrollo estándar
- Navegador web
- Servidor de presentación
- Servidor de aplicaciones
- Cliente de correo
- Servidor de ficheros
- Sistema de gestión de bases de datos
- Monitor transaccional
- Ofimática

- Antivirus
- Sistema operativo
- Servidor de terminales
- Sistema de backup

4. Equipos Informáticos
   - Ordenadores
   - Informática móvil
   - Agendas electrónicas
   - Periféricos
   - Medios de impresión
   - Escáneres
   - Dispositivos criptográfocos
   - Dispositivos de red
   - Cortafuegos
   - Centralita telefónica
5. Redes de comunicaciones
   - Red telefónica
   - ADSL
   - Red inalámbrica
   - Red privada virtual
6. Soportes de información
   - Discos
   - Almacenamiento en red
   - Dispositivos USB
   - CDs y DVDs
   - Cintas magnéticas
   - Tarjetas de memoria
   - Material impreso

7. Equipamiento auxiliar
    - Fuentes de alimentación
    - Sistemas de alimentación ininterrumpida
    - Generadores eléctricos
    - Equipos de climatización
    - Cableado
    - Robots de cintas y discos
    - Equipos de destrucción de soportes de información
    - Mobiliario
    - Cajas fuertes
8. Instalaciones
    - Emplazamiento
    - Edificio
    - Local
    - Plataformas móviles
9. Personal
    - Usuarios externos
    - Usuarios internos
    - Operadores
    - Administradores de sistemas
    - Administradores de comunicaciones
    - Administradores de BBDD
    - Desarrolladores
    - Subcontratas
    - Proveedores

A continuación se muestran algunos ejemplos de activos específicos, según se describen en MAGERIT:



[SW] Aplicaciones (software)

Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este epígrafe se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.

No preocupa en este apartado el denominado "código fuente" o programas que serán datos de interés comercial, a valorar y proteger como tales. Dicho código aparecería como datos.

- [prp] desarrollo propio (in house)
- [sub] desarrollo a medida (subcontratado)
- [std] estándar (off the shelf)
  - [browser] navegador web
  - [www] servidor de presentación
  - [app] servidor de aplicaciones
  - [email_client] cliente de correo electrónico
  - [file] servidor de ficheros
  - [dbms] sistema de gestión de bases de datos
  - [tm] monitor transaccional
  - [office] ofimática
  - [av] anti virus
  - [os] sistema operativo
  - [ts] servidor de terminales
  - [backup] sistema de backup

Figura 2.2: Ejemplo activo aplicaciones

[COM] Redes de comunicaciones

Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.

- [PSTN] red telefónica
- [ISDN] rdsi (red digital)
- [X25] X25 (red de datos)
- [ADSL] ADSL
- [pp] punto a punto
- [radio] red inalámbrica
- [sat] por satélite
- [LAN] red local
- [MAN] red metropolitana
- [Internet] Internet
- [vpn] red privada virtual

Figura 2.3: Ejemplo activo redes de comunicaciones

Figura 2.4: Ejemplo activo instalaciones

Amenazas

En cuanto a las amenazas más usuales, MAGERIT describe las siguientes:

1. Desastres naturales
   - Fuego
   - Daños por agua
   - Desastres naturales (tormenta eléctrica, terremoto, ciclones, etc)
2. De origen industrial
   - Desastres industriales (explosiones, derrumbes, contaminación química, etc)
   - Contaminación mecánica
   - Contaminación electromagnética
   - Avería de origen físico o lógico
   - Corte del suministro eléctrico
   - Condiciones inadecuadas de temperatura y/o humedad
   - Fallo de servicios de comunicaciones
   - Interrupción de otros servicios y suministros esenciales
   - Degradación de los soportes de almacenamiento de la información
   - Emanaciones electromagnéticas

3. Errores y fallos no intencionados
    - Errores de los usuarios
    - Errores del administrador
    - Errores de monitorización
    - Errores de configuración
    - Deficiencias en la organización
    - Difusión de software dañino
    - Errores de encaminamiento
    - Errores de secuencia
    - Escapes de información
    - Alteración de la información
    - Introducción de información incorrecta
    - Degradación de la información
    - Destrucción de información
    - Divulgación de información
    - Vulnerabilidades de los programas
    - Errores de mantenimiento y actualización de programas
    - Errores de mantenimiento y actualización de equipos
    - Caída del sistema por agotamiento de recursos
    - Indisponibilidad del personal
4. Ataques intencionados
    - Manipulación de la configuración
    - Suplantación de la identidad del usuario
    - Abuso de privilegios de acceso
    - Uso no previsto
    - Re-encaminamiento de mensajes
    - Alteración de secuencia
    - Acceso no autorizado
    - Análisis de tráfico

- Repudio
- Interceptación de información
- Modificación de la información
- Introducción de falsa información
- Corrupción de la información
- Destrucción de la información
- Manipulación de programas
- Denegación de servicio
- Robo
- Ataque destructivo
- Ocupación enemiga
- Indisponibilidad del personal
- Extorsión
- Ingeniería social

Algunos ejemplos de amenazas, según se describen en MAGERIT, son los siguientes:

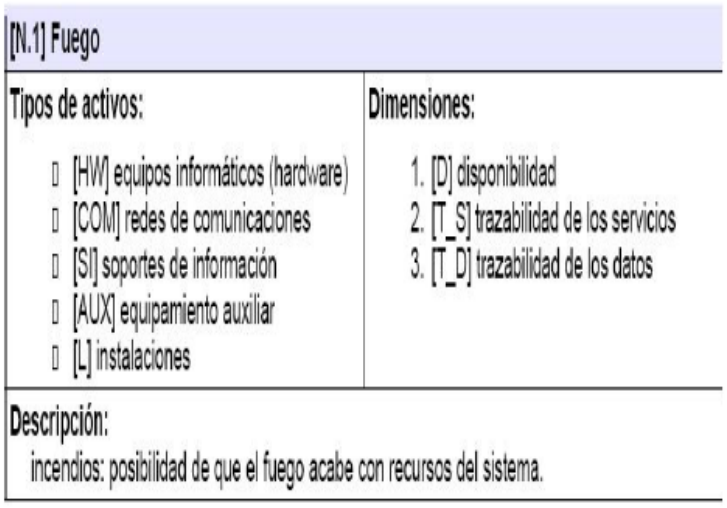
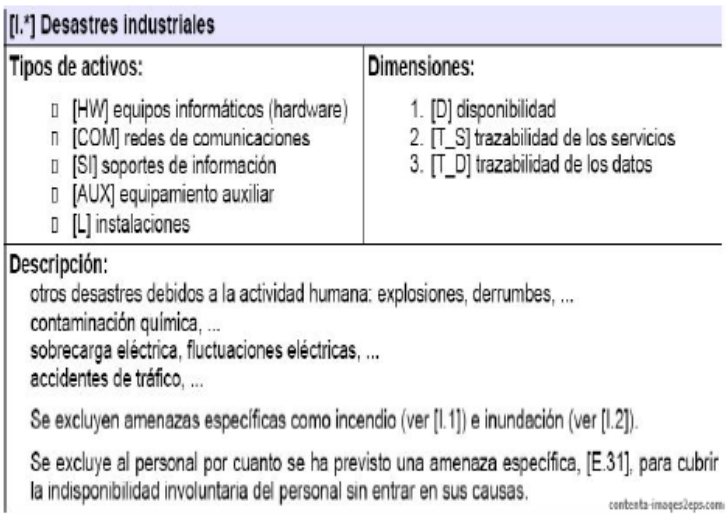


Figura 2.5: Ejemplo amenaza fuego



[I.*] Desastres industriales

Tipos de activos:	Dimensiones:
[HW] equipos informáticos (hardware) [COM] redes de comunicaciones [SI] soportes de información [AUX] equipamiento auxiliar [L] instalaciones	1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos

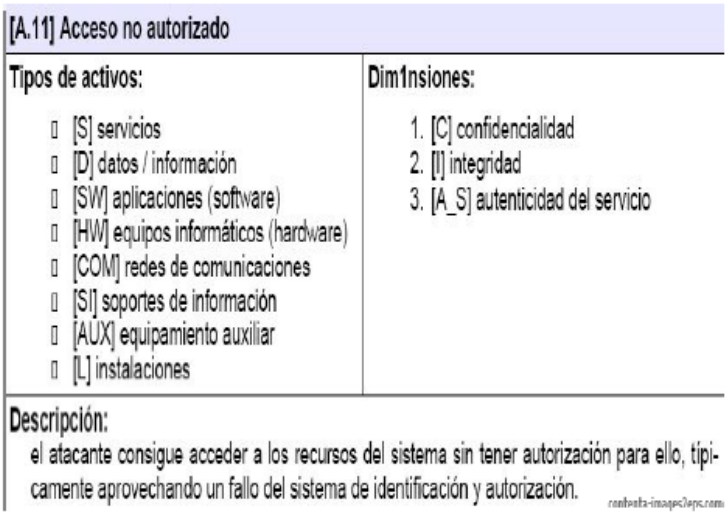
Descripción:

otros desastres debidos a la actividad humana: explosiones, derrumbes, ...
contaminación química, ...
sobrecarga eléctrica, fluctuaciones eléctricas, ...
accidentes de tráfico, ...

Se excluyen amenazas específicas como incendio (ver [I.1]) e inundación (ver [I.2]).

Se excluye al personal por cuanto se ha previsto una amenaza específica, [E.31], para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas.

Figura 2.6: Ejemplo amenaza desastres industriales



[A.11] Acceso no autorizado

Tipos de activos:	Dim1nsiones:
[S] servicios [D] datos / información [SW] aplicaciones (software) [HW] equipos informáticos (hardware) [COM] redes de comunicaciones [SI] soportes de información [AUX] equipamiento auxiliar [L] instalaciones	1. [C] confidencialidad 2. [I] integridad 3. [A_S] autenticidad del servicio

Descripción:

el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

Figura 2.7: Ejemplo amenaza acceso no autorizado

Salvaguardas

En cuanto a la inclusión de salvaguardas en MAGERIT, éstas introducen un nuevo elemento de sumo interés, ya que gracias a ellas podremos dar un tratamiento adecuado a todas las contingencias que pudieran tener lugar en nuestras infraestructuras. Según la solvencia de dichas contramedidas de seguridad, el impacto y los riesgos procedentes de ciertas amenazas se verán mitigados o totalmente contrarrestados como se puede ver en la figura 2.8. En la imagen se muestra cómo en función de las salvaguardas implantadas pasaríamos a hablar de una degradación y una frecuencia residual de las amenazas contempladas con lo que, en principio, las consecuencias de estas amenazas decrecerían, lo

cual se reflejaría de igual modo en el impacto y riesgo residual.

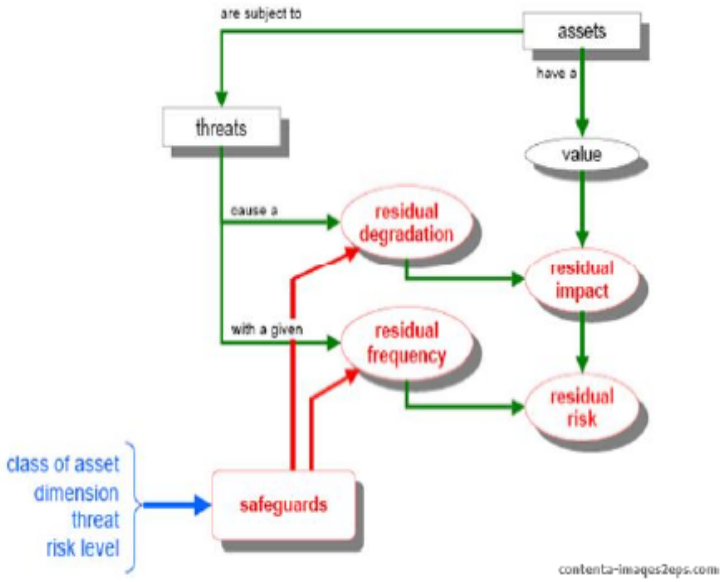


Figura 2.8: Consideración de salvaguardas

1. Salvaguardas de tipo general
   - Organización de la seguridad: roles, comités, etc
   - Política corporativa de seguridad de la información
   - Gestión de privilegios: adjudicación, revisión y terminación
   - Procedimientos de escalado y gestión de incidencias
   - Procedimientos de continuidad de operaciones: emergencia y recuperación
   - Auditoría, registro (certificación) y acreditación del sistema
   - Contratación de seguros
2. Salvaguardas para la protección de los servicios
   - Control de acceso
   - Registro de actuaciones
   - Registro de incidencias
   - Plan de continuidad
3. Salvaguardas para la protección de los datos
   - Control de acceso

- Firma electrónica
- Registro de actuaciones
- Registro de incidencias
- Copias de respaldo
- Detección y recuperación
- Cifrado

4. Salvaguardas para la protección de las aplicaciones
   - Protección frente a código dañino
   - Control de acceso
   - Registro de actuaciones
5. Salvaguardas para la protección de los equipos
   - Configuración de seguridad
   - Detección de intrusiones
   - Registro de actuaciones
   - Gestió de privilegios
   - Control de acceso
6. Salvaguardas para la protección de las comunicaciones
   - Plan de continuidad
   - Garantías de integridad
   - Cifrado
   - Control de acceso
   - Registro de actuaciones
7. Seguridad física
   - Protección frente a accidentes naturales
   - Protección frente a accidentes industriales
   - Protección frente a emanaciones electromagnéticas
   - Protección del recinto: edificios, locales y áreas de trabajo

- Control de acceso: entrada y salida de personas, equipos, soportes de información, etc.

8. Salvaguardas relativas al personal
   - Responsabilidades en seguridad
9. Externalización
   - SLAs
   - NDAs
   - Identificación y calificación del personal encargado
   - Procedimientos de escalado y resolución de incidencias
   - Procedimiento de terminación
   - Asunción de responsabilidades y penalizaciones por incumplimiento

2.2. Análisis crítico de la metodología MAGERIT

Resumiendo, MAGERIT hace uso de métodos cualitativos y algunas técnicas analíticas específicas que no alcanzan el nivel de precisión deseado para el correcto tratamiento del riesgo, por lo que el estado del arte en este campo requerirá de una revisión completa.

Así pues, se dejará de lado la visión frecuentista de MAGERIT para dar paso a enfoques más sofisticados que pongan en práctica técnicas más avanzadas basadas en métodos probabilísticos con los que medir el desarrollo de los sistemas y sus amenazas. De este modo, el marco general de MAGERIT, mostrado en la figura 2.1, debería de reestructurarse de cara a adoptar un enfoque mucho más moderno.

Por tanto, si analizamos por partes y comenzando con los costes de los activos, éstos se tratan de una forma muy superficial, lo que provoca muy poca confianza a la hora de utilizarse para una cuantificación en entornos de trabajo reales. En el siguiente gráfico se puede observar cómo MAGERIT cuantifica los costes por interrupción del servicio de los distintos activos mediante escalones, que aún pudiendo guardar cierta similitud con la realidad, son muy poco específicos y nada precisos.

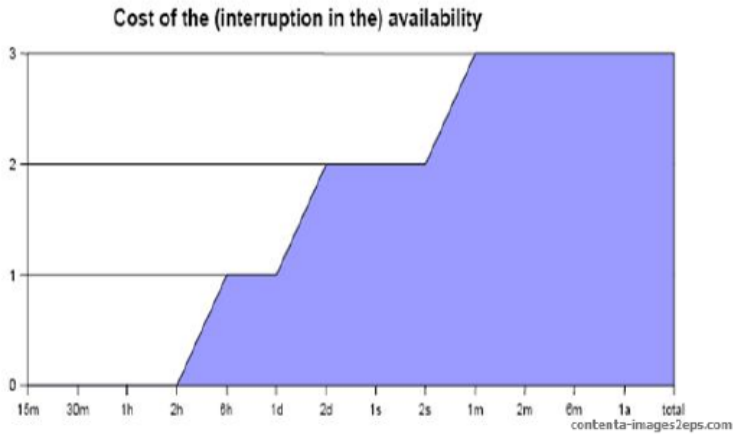


Figura 2.9: Cuantificación de costes

Asimismo, el tratamiento de la probabilidad de ocurrencia de las amenazas se queda muy lejos de lo deseado, dado que no va más alla de un breve planteamiento frecuentista. Está claro que esta visión no es eficaz a la hora de medir la situación actual en el campo de la seguridad y, teniendo en cuenta la cantidad de conocimientos y datos de los que se dispone actualmente para gestionar el riesgo, el tratamiento que realiza MAGERIT ha quedado desactualizado.

100	very frequent	daily
10	frequent	monthly
1	normal	annually
1/10	infrequent	every few years

Figura 2.10: Visión frecuentista de las amenazas

Con los impactos asociados a las amenazas sucede algo similar, se realiza a partir de valores cualitativos impidiendo así una visión profunda y precisa de la situación que se quiere medir.

impact		degradation		
		1%	10%	100%
value	VH	M	H	VH
	H	L	M	H
	M	VL	L	M
	L	VL	VL	L
	VL	VL	VL	VL

contenta-images2eps.com

Figura 2.11: Establecimiento de impactos

En el apartado de los riesgos, vuelve a suceder lo mismo. MAGERIT vuelca toda la responsabilidad de cómo priorizar los riesgos y cómo elegir las medidas reales a tomar, completamente sobre los mediadores TIC, ya que éstos se encuentran ante unos resultados muy poco concretos puesto que esta metodología no se preocupa de profundizar en este campo.

risk		frequency			
		PF	FN	F	MF
impact	VH	H	VH	VH	VH
	H	M	H	VH	VH
	M	B	M	H	VH
	L	VL	L	M	H
	VL	VL	VL	L	M

contenta-images2eps.com

Figura 2.12: Establecimiento de riesgos

Para la modelización de dependecias entre activos, MAGERIT usa un conjunto de funciones de redondeo triviales que asumen un gran conocimiento a priori, esto no es más que un grave error de modelización. Para el estudio de mundo real, hay que tener en cuenta la gran complejidad de las dependencias entre activos y hay que recurrir a herramientas que se acerquen lo máximo posible a los valores reales que existen, para ello se debe recurrir a técnicas de redes probabilísticas.

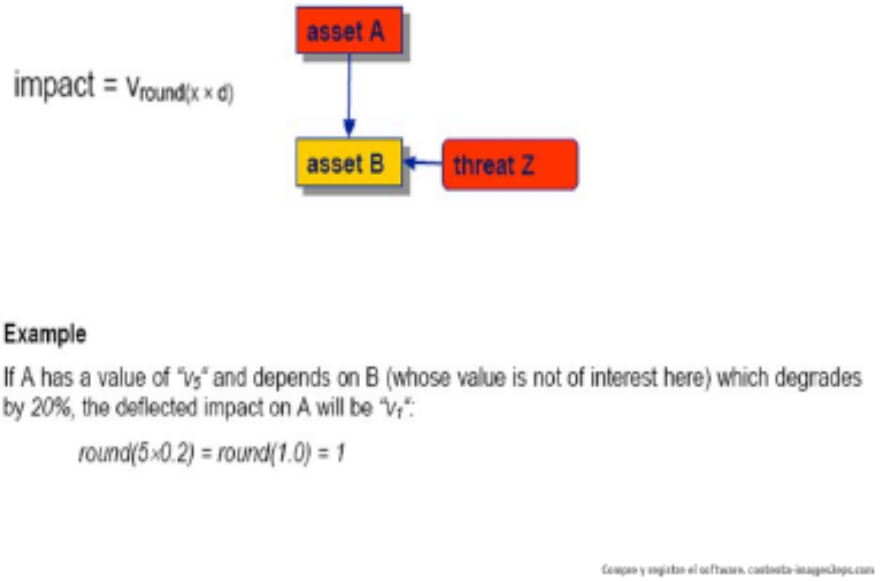


Figura 2.13: Cálculo del impacto acumulado

En cuanto a la inclusión de las salvaguardas, a pesar de que en MAGERIT se tienen en cuenta indicando el riesgo que aún se puede tener incluso después de haber implantado algunas de ellas, el enfoque estático que sigue utilizando para su estudio no hace más que limitar la veracidad de sus resultados ya que no tiene en cuenta el carácter dinámico de este escenario.

En definitiva, las labores que requieren de ingeniería tratadas adecuadamente en MAGERIT, serían las siguientes:

- Identificación de amenazas: fuego, virus, etc.
- Identificación de activos: equipos y suministros; edificios e inmobiliario; ordenadores y aplicaciones; comunicaciones, etc.
- Identificación de los criterios de valoración: costes de reemplazamiento; adquisición e instalación; costes laborales invertidos en la recuperación de los activos; pérdidas de ingresos durante dichos plazos; pérdida de capacidad de operación; penalizaciones debidas a incumplimientos con leyes y regulaciones; daños a personas o al medioambiente, etc.
- Identificación de salvaguardas: firewalls, seguridad física, extintores de incendios, etc.

Pero siempre dejando sin cubrir adecuademente todas aquellas cuestiones derivadas del comportamiento dinámico de los activos, amenazas y salvaguardas siendo la principal

deficiencia de este método de análisis y gestión de riesgos.

2.3. Alternativas a MAGERIT

Existe numerosas alternativas a la propuesta por MAGERIT, aparte de las referenciadas por ENISA en su sitio web, lo cual es un claro indicador de que el Análisis de Riesgos es un campo de investigación muy vivo en la actualidad. Una de estas alternativas es la desarrollada en Corea del Sur por Jae Lee y Chung (Building a framework to measure and minimize Information Risks, 2008). Esta alternativa busca establecer un marco de trabajo desde el que se tratará de evaluar y minimizar riesgos en la industria TIC.

El método diferencia en tres categorías los posibles riesgos:

- Riesgos naturales.
- Riesgos humanos, ya sean accidentales o deliberados.
- Riesgos tecnológicos.

A la hora de evaluar estos riesgos, es necesario tener en cuenta dos dimensiones, la probabilidad de que un riesgo determinado ocurra y el impacto de dicho riesgo en términos de pérdidas potenciales. Para ello, proponen una escala de probabilidad de riesgos con cinco niveles: Muy alto (26-99 %); Alto (11-25 %); Moderado (6-10 %); Bajo (1-5 %); Muy bajo (1 %). Una diferencia importante respecto a otros métodos es que éste especifica una base periódica de un año para la gestión de riesgos de la información.

Probability Rating	Rate of Occurrence	Probability Estimate
5	More than once in a four-year period	26% to 99%
4	Once in four to 10 years	11% to 25%
3	Once in 10 to 20 years	6% to 10%
2	Once in 20 to 100 years	1% to 5%
1	Less than once in 100 years	1%

Figura 2.14: Escala de calificación según la probabilidad

De la tabla anterior se desprende la siguiente fórmula para el cálculo de la probabilidad de ocurrencia de una cierta amenaza:

$$Score_{RPj} = (\sum n_i * P_i)/N$$

$Score_{RPj}$: probabilidad para la amenaza j

n_i : número de encuestados que eligen la escala de calificación i

P_i : probabilidad de la escala de calificación (1,2,3,4,5)

N: número total de encuestados

También han desarrollado una escala para calcular el impacto según el riesgo. Dicho impacto depende del nivel de interrupción que se produzca, así como de la duración de ésta. La siguiente fórmula trata de evaluarlo:

$$Score_{RIj} = (\sum n_i * I_i)/N$$

$Score_{RIj}$: impacto para la amenaza j

n_i : número de encuestados que eligen la calificación i

I_i : valoración del impacto (0,1,2,3)

N: número total de encuestados

En la siguiente tabla representa la escala de evaluación de impacto.

Impact Rating	Impact Severity	Duration of Interruption to Operations
3	Very serious	More than 48 hours – relocation of operations necessary
2	Serious	8 - 48 hours
1	Significant	Up to 8 hours
0	Minor	No interruption of operations

Figura 2.15: Escala de calificación según el impacto

La propuesta de Lee y Chung también se centra en la selección de métodos de tratamiento. Cada tipo de amenaza objeto de medida puede encuadrarse en una de las siguientes categorías:

- Baja probabilidad, bajo impacto (I).
- Baja probabilidad, alto impacto (III).
- Alta probabilidad, bajo impacto (II).

- Alta probabilidad, alto impacto (IV).

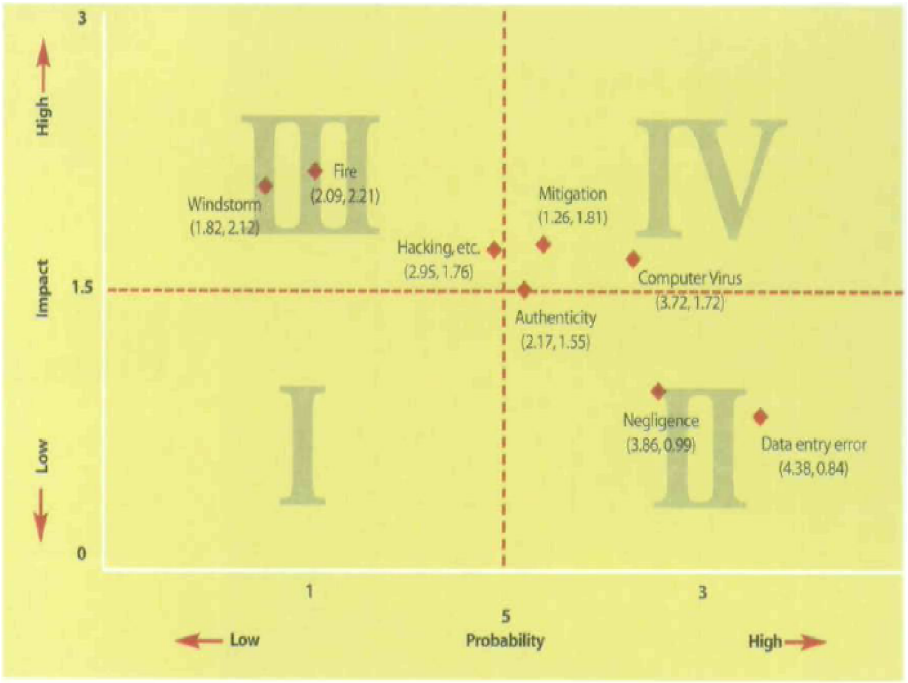


Figura 2.16: Cuadrante de riesgos y respuestas sugeridas

A través de su estudio, Lee y Chung, tratan de mostrar la relevancia del análisis de riesgos en los entornos TIC, proveyendo a su vez de un modelo sencillo en el que basar este análisis. Pero, en ningún caso, este estudio llega al nivel de complejidad y detalle que ofrece la metodología MAGERIT.

Capítulo 3

Modelo Discreto

Una vez llegados a este punto, nuestro objetivo es potenciar el componente probabilístico en este tipo de problemas. De esta manera, seremos capaces de mejorar la toma de decisiones en lo que se refiere a los sitemas de seguridad utilizados. Dejaremos de trabajar en un marco estático para el análisis y la gestión de riesgos pasando a trabajar en un marco dinámico, teniendo en cuenta valores como las utilidades esperadas que serán seguro bien apreciados por los analistas de decisiones (Clemen, 1997). Utilizaremos la base de datos propuesta por MAGERIT para seleccionar las posibles amenazas hacia un servicio concreto. Dichas amenazas tendrán asociada una probabilidad de ocurrencia así como un coste asociado, denominado coste extra, que indicará su impacto y se utilizará para calcular los costes asociados a cada una de las amenazas que pueden tener lugar. La figura 3.1 ilustra este modelo.

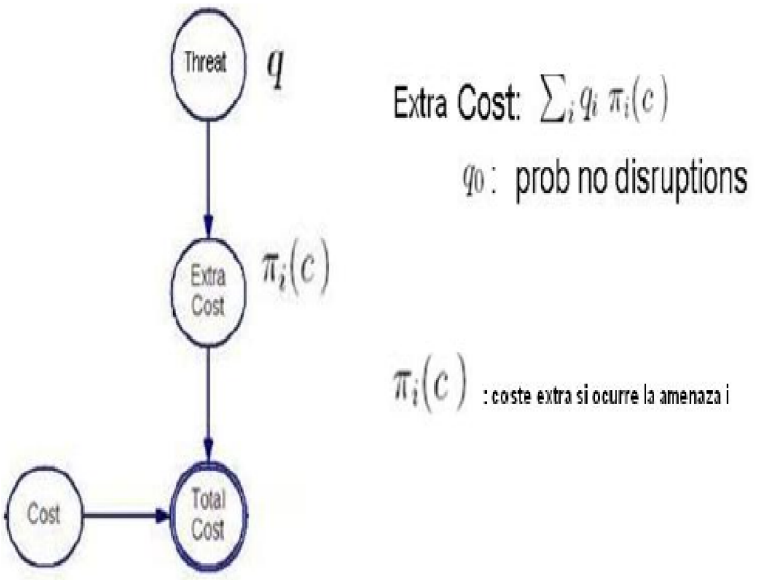
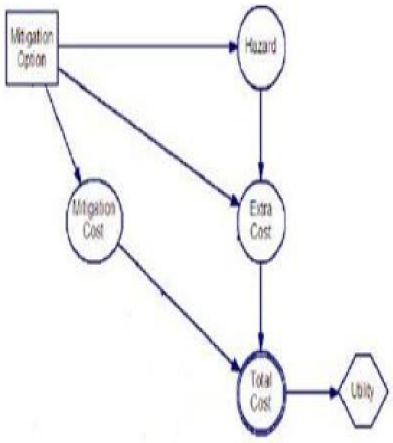


Figura 3.1: Propuesta de cálculo de riesgos

Nuestra propuesta para la gestión de riesgos contempla la inclusión de acciones que mitiguen los efectos perniciosos del las posbiles amenazas que puedan dañar los activos tenidos en cuenta. A estas acciones, hay que asociar el coste de su implementación, el cual afectaría directamente al coste derivado del impacto de las amenazas, haciéndolo disminuir. De la misma manera, las salvaguardas utilizadas reducirían la probabilidad de una amenaza determinada pueda tener lugar. Por lo tanto, a partir de un presupuesto determinado, nos será posible calcular qué salvaguardas serán óptimas para contrarrestar un conjunto determinado de amenazas.



$$\psi_m = \max_{m \in \mathcal{M}} \psi_r(m)$$

$$\psi_r(m) = \sum_i q_i(m) \int u(c)\pi_i(c|m)\, dc.$$

$\mathcal{M}$: conjunto de salvaguardas (satisfaciendo las restricciones de presupuesto)

Figura 3.2: Propuesta de gestión de riesgos

Es importante, llegados a este punto, tratar de modelizar de manera adecuada lo concerniente a la probabilidad de aparición de una amenaza, así como obtener una estimación de la duración de un incidente causado por dicha amenaza.

- Para una amenaza dada, modeliza su número de apariciones en el tiempo. Por ejemplo, un fuego intencionado puede corresponderse con un proceso de Poisson no homogéneo $\lambda_1^f(t)$, mientras que un fuego debido a una imprudencia sería modelizado con $\lambda_2^f(t)$. Para modelizar otras amenazas, como sería un ataque de denegación de servicio, tambien se utilizaría un parámetro $\lambda^w(t)$.

- Obtener un modelo para estimar la duración de un incidente será importante ya que guarda una relación directa con los costes asociados. Si retomamos el ejemplo del fuego, la duración podría modelizarse con una distribución Gamma, y los activos se

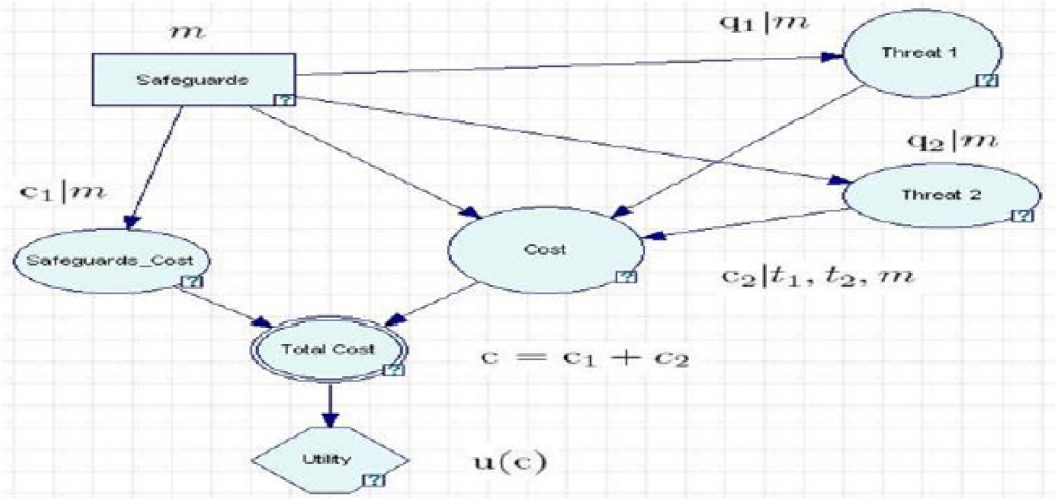
verían afectados basándose en una curva de incremento del coste $C_i(t)$, función del tiempo.

Continuando con el ejemplo de la amenaza fuego, la modelización del coste se haría sobre un tiempo horizonte T usando un proceso de Poisson. En este caso se ha contemplado tres tipos de activos que pueden verse afectados, así como la posibilidad de que dicha amenaza tenga lugar tanto de forma intencionada como por imprudencia.

Fire	Intentional	Imprudence
Furniture	$\sum_{K=0}^{\infty} m_1^f(T)\frac{(m_1^1(T))^K}{K!} \quad K \quad E(c_1^1(t))$	$\sum_{K=0}^{\infty} m_2^f(T)\frac{(m_2^1(T))^K}{K!} \quad K \quad E(c_2^1(t))$
Electricity	$\sum_{K=0}^{\infty} m_1^f(T)\frac{(m_1^2(T))^K}{K!} \quad K \quad E(c_1^2(t))$	$\sum_{K=0}^{\infty} m_2^f(T)\frac{(m_2^2(T))^K}{K!} \quad K \quad E(c_2^2(t))$
PCs	$\sum_{K=0}^{\infty} m_1^f(T)\frac{(m_1^3(T))^K}{K!} \quad K \quad E(c_1^3(t))$	$\sum_{K=0}^{\infty} m_2^f(T)\frac{(m_2^3(T))^K}{K!} \quad K \quad E(c_2^3(t))$

Figura 3.3: Modelización del coste asociado a la amenaza fuego

En la figura 3.4 se muestra el modelo de salvaguardas propuesto. En este modelo se tienen en cuenta tanto los costes derivados de estas salvaguardas como los costes asociados a la incidencia de ciertas amenazas. Para obtener la información que deseamos, debemos resolver un problema de optimización. Si maximizamos la utilidad respecto de los costes de las salvaguardas aplicadas y los costes derivados de las posibles amenazas, obtendremos dicha información.



$$\max_m \int \dots \int \mathrm{u}(c_1 + c_2) f(c_1|m) f(c_2|t_1, t_2, m) f(q_1|m) f(q_2|m) dq_1 dq_2 dc_1 dc_2$$

Figura 3.4: Modelo de salvaguardas

La figura 3.5 muestra algunos nodos del modelo planteado expandidos. De esta manera podemos apreciar importancia de la existencia de las salvaguardas elegidas, viendo como las probabilidades de incidencia de ciertas amenazas varían según la presencia o no de dichas salvaguardas. El modelo presentado permite no sólo representar la probabilidad de aparición de un incidente según las salvaguardas utilizadas, sino que también es posible apreciar los costes asociados.

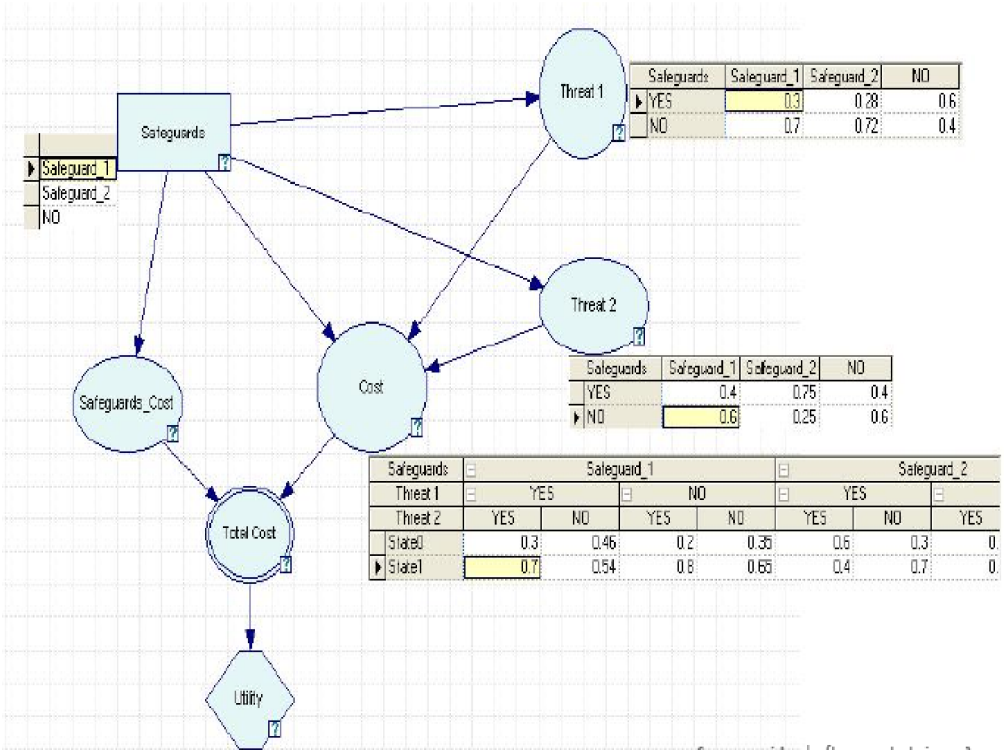


Figura 3.5: Modelo de salvaguardas expandido

Con lo visto hasta el momento queda notablemente remarcada la necesidad de realizar un análisis y gestión de riesgos apropiado. El modelo propuesto por la metodología MAGERIT será punto de referencia en nuestra propuesta, ya que hace un muy buen trabajo en lo descriptivo y en el establecimiento de las bases fundamentales. Es a nivel analítico donde el carácter eminentemente dinámico del problema que estamos tratando traspasa, en cierta manera, lo propuesto por MAGERIT. En nuestro caso, consideramos que este carácter dinámico es pieza fundamental del modelo.

En las siguientes secciones se plantea un problema concreto de análisis de riesgos el cual irá poco a poco ganando en complejidad, al contar con elementos adicionales de decisión. De este modo, se mostrará cómo afrontar un problema de toma de decisiones en este campo con unas características muy semejantes a las que podrían ocurrir en un problema real. Junto a la explicación del planteamiento realizado se mostrará el análisis del problema, pudiendo observarse así una herramienta de toma de decisiones en acción.

3.1. Análisis de riesgos

A continuación presentaremos el caso de una entidad abstracta, encuadrando el estudio en un período temporal de un año. Esta entidad dispone de servicios informáticos y bienes inmuebles aparte de otros activos que deben ser protegidos. Los distintos elementos fundamentales, en este caso, pueden observarse en la siguiente figura y serán debidamente explicados a continuación de la misma:

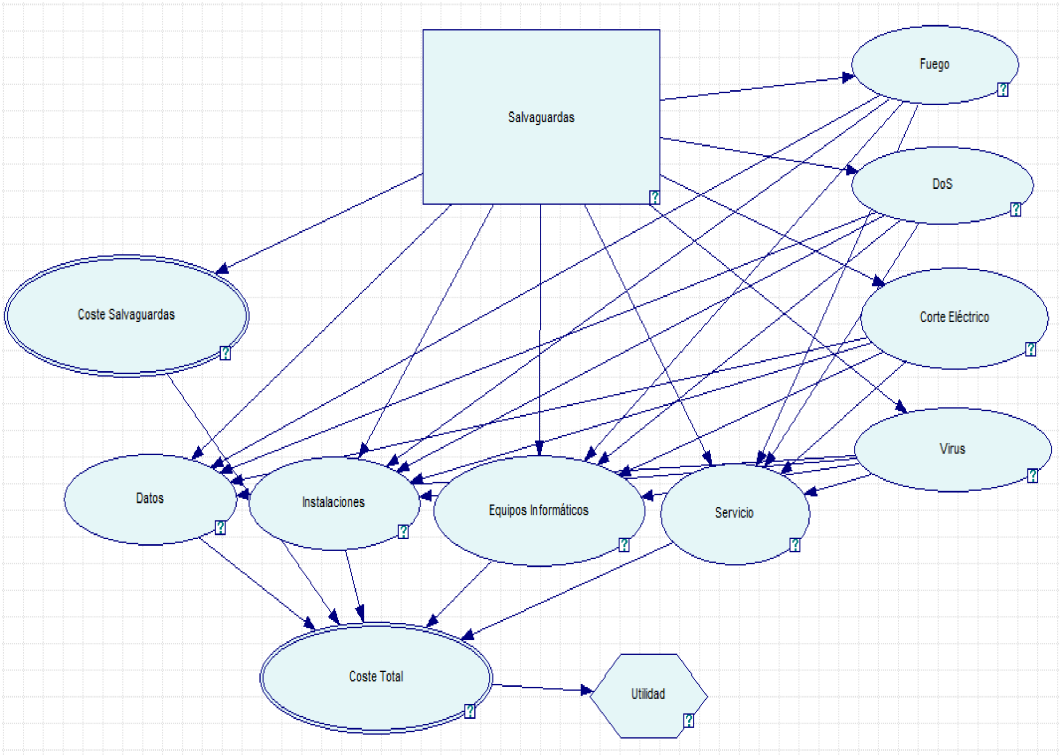


Figura 3.6: Modelo de análisis de riesgos. Diagrama de influencia construido a través de la herramienta GeNIe.

- Amenazas

  1. Fuego: inicio de un fuego en los inmuebles de la institución bajo estudio que pondrá en peligro dichas instalaciones, junto con los sistemas informáticos que en ellas se alberguen, los cuales se verán degradados en cierto modo según el tiempo de exposición y la crudeza del fuego. Es un ejemplo de amenaza natural que puede suceder de forma intencionada o accidental.
  2. Corte Eléctrico: las razones para la caída del suministro normalmente estarán en el fallo de alguno de los elementos que componen el sistema de suministro eléctrico. Este tipo de cortes pueden producirse tanto accidental como inten-

cionadamente. Un corte eléctrico puede tener serias consecuencias para una institución, desde la pérdida de información o servicio en entornos informáticos, hasta consecuencias más graves si tuviéramos en cuenta una institución de tipo sanitaria como sería un hospital.

3. Denegación de servicio o DoS (de las siglas en inglés Denial Of Service): ataque dirigido a los sistemas informáticos de una institución que afectaría directamente a la disponibilidad de dichos sistemas. Es un ejemplo de amenaza informática intencionada. Este tipo de ataque provoca normalmente pérdidas en la conectividad o sobrecarga de los recursos computacionales del sistema de la víctima, lo cual puede llegar a suponer una pérdida de servicio dependiendo del tipo de institución objeto del ataque. Los ataques por Denegación de Servicio han evolucionado en los últimos años en lo que se han venido a llamar ataques distribuídos de denegación de servicio (DDoS de las siglas en inglés Distributed Denial of Service).
4. Virus Informático: software malintencionado que tiene por objeto alterar el normal funcionamiento de los sistemas informáticos. Generalmente los Virus Informáticos pueden afectar de diversas maneras a nuestros sistemas. Podrían, por ejemplo, afectar directamente a los datos almacenados, destruyéndolos, o bien únicamente reducir el rendimiento de los servicios ofrecidos. En cuanto a su propagación existen dos principales vías. En la primera, el usuario, en un momento dado, ejecuta o acepta de forma inadvertida la instalación del virus. En la segunda, el programa malicioso actúa replicándose a través de las redes.

- Activos

  Tendremos en cuenta los que siguen:

1. Instalaciones: Oficinas de la institución bajo estudio que pueden verse afectadas tanto por la amenaza de fuego como por un corte eléctrico. Son un ejemplo de elemento no informático que ha de ser tenido en cuenta, ya que sin él una organización no podría continuar con su operativa, siendo el impacto en este ejemplo un coste.
2. Datos: El almacenamiento de datos y la seguridad de los mismos es uno de los puntos clave dentro de un departamento de TIC, ya que la información es tal vez el más valioso de los activos para una institución. Estos datos están expuestos a las amenazas anteriormente definidas y, por tanto, dada la importancia de los mismos, el análisis de los riesgos derivados de su pérdida se antoja

verdaderamente importante.

3. Equipos informáticos: Por supuesto los equipos informáticos, ya sea un centro de cómputo de una gran organización, como los puestos de trabajo normalmente situados en un edificio de oficinas, suponen un activo realmente importante para una institución. Tanto la amenaza Fuego como la amenaza Corte Eléctrico afectaría a este importante activo de la institución en estudio y podrían incidir, por tanto, de manera importante en los costes de la misma.
4. Servicio: Cualquiera de las amenazas definidas en el apartado anterior podrían afectar al servicio ofrecido por la institución objeto de análisis, tanto sea una institución vinculada directamente con las Tecnologías de la Información, como una institución dedicada a cualquier otro ámbito pero con un departamento TIC.

- Salvaguardas

  - Salvaguardas: De forma general, los responsables del departamento TI en una organización deben decidir qué salvaguardas implementar en sus sistemas con el objetivo de reducir el impacto y la frecuencia de las posibles amenazas. Según la elección de unas u otras soluciones el problema se solventará en uno u otro grado. En el caso de estudio que nos ocupa las salvaguardas a tener en cuenta serán un sistema antiincendios, un sistema UPS (del inglés Uninterrupted Power System), un sistema de Firewall y, por último, la implemenctación de un sistema de Backup. Nuestro estudio no se centra en realizar la mejor elección de estas salvaguardas de entre todas las disponibles en el mercado, sino en realizar un análisis exhaustivo del conjunto de salvaguardas seleccionadas, obteniendo así la combinación óptima de las mismas tratando de reducir al máximo tanto los riesgos presentes en la institución bajo estudio como los costes derivados de los mismos.
  - Coste de salvaguardas: Las salvaguardas elegidas conllevarán un cierto coste, el cual ha de valorarse en función del presupuesto con que se cuente. Dicho coste siempre ha de estar relacionado con la criticidad de los sistemas a defender, ya que, en caso contrario, se estarían desperdiciando recursos de forma innecesaria. Además, tendrían un impacto sobre la probabilidad de aparición y los efectos de las amenazas.

- Coste total

  - Coste total: Teniendo en cuenta todos los elementos anteriores, la aparición de ciertos riesgos y la implantación de ciertas salvaguardas conllevará un coste, que ha de ser asumible por la organización. También se podrían considerar costes menos tangibles, como pudiera ser la imagen corporativa o la pérdida de clientes por un fallo puntual.

- Utilidad

  - Utilidad: Finalmente el análisis de decisiones solventará el problema viendo cuál es la solución óptima. De este modo, los responsables de dirección cuentan con una información muy valiosa para tomar una decisión en consonancia con la situación real y los objetivos perseguidos.

Especificación de los nodos

A continución pasaremos a definir cada uno de los nodos implicados en el modelo anterior y representados en la figura 3.6

Nodo Salvaguardas

Para el nodo inicial de Salvaguardas consideraremos todas las posibles combinaciones de las mismas:

- Ninguna salvaguarda
- Instalar un Antiincendios
- Instalar un UPS
- Instalar un Firewall
- Instalar un Backup
- Instalar Antiincendios y UPS
- Instalar Antiincendios y Firewall
- Instalar Antiincendios y Backup
- Instalar Antiincendios, UPS y Firewall

- Instalar Antiincendios, UPS y Backup
- Instalar Antiincendios, Firewall y Backup
- Instalar Antiincendios, UPS, Backup y Firewall
- Instalar UPS y Firewall
- Instalar UPS y Backup
- Instalar Firewall y Backup
- Instalar UPS, Firewall y Backup

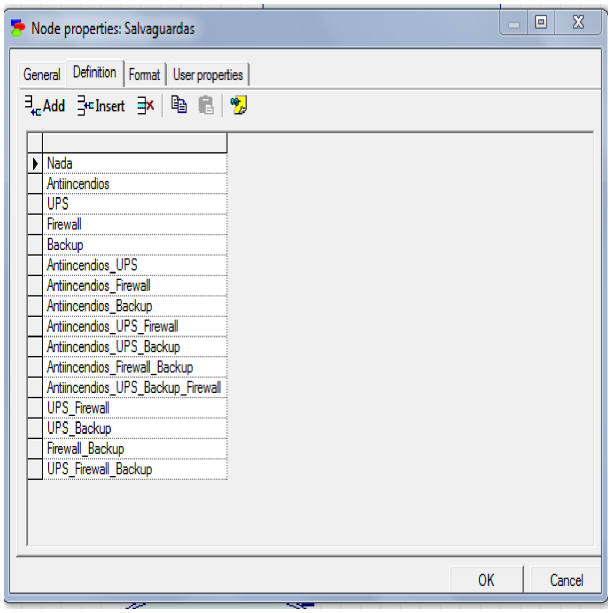


Figura 3.7: Nodo Salvaguardas

Nodo Costes Salvaguardas

Estas salvaguardas conllevan un coste asociado, el cual ha de ser considerado minuciosamente en nuestro estudio, ya que habrá restricciones de presupuesto a cumplir. En este caso se considera que dichos rangos monetarios irían de 0 € , en caso de no tener ninguna salvaguarda, hasta los 7050 €, según la combinación de salvaguardas que se diera, como detallamos a continuación.

- Ninguna salvaguarda: 0 €
- Instalar un Antiincendios: 300 €

- Instalar un UPS: 5000 €
- Instalar un Firewall: 1050 €
- Instalar un Backup: 700 €

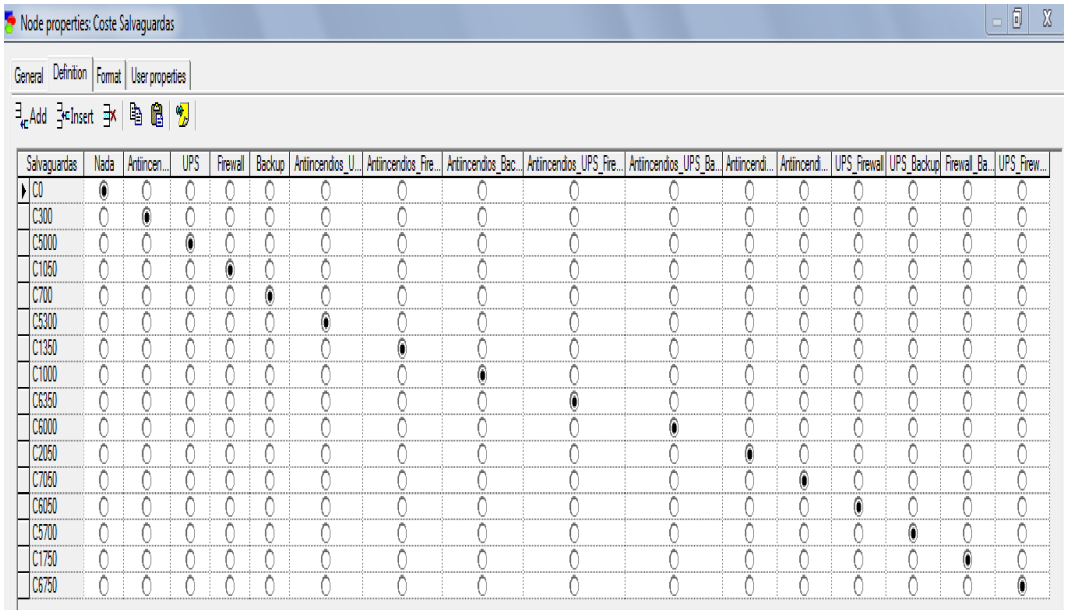


Figura 3.8: Coste de Salvaguardas representado en la herramienta Genie

Nodos de Probabilidad de Salvaguardas

A continuación pasamos a detallar las distintas probabilidades de ocurrencia, en el período de un año, para cada una de las amenazas. Estas probabilidades vendrán condicionadas por las distintas combinaciones de contramedidas que se utilicen. En primer lugar, consideramos las siguientes probabilidades para el nodo Fuego.

- P(fuego | no salvaguardas) = 0,1
- P(fuego | Antiincendios) = 0,05
- P(fuego | UPS) = 0,1
- P(fuego | Firewall) = 0,1
- P(fuego | Backup) = 0,1
- P(fuego | Antiincendios y UPS) = 0,05
- P(fuego | Antiincendios y Firewall) = 0,05

- P(fuego | Antiincendios y Backup) = 0,05
- P(fuego | Antiincendios, UPS y Firewall) = 0,05
- P(fuego | Antiincendios, UPS y Backup) = 0,05
- P(fuego | Antiincendios, Firewall y Backup) = 0,05
- P(fuego | Antiincendios, UPS, Backup y Firewall) = 0,05
- P(fuego | UPS y Firewall) = 0,1
- P(fuego | UPS y Backup) = 0,1
- P(fuego | Firewall y Backup) = 0,1
- P(fuego | UPS, Firewall y Backup) = 0,1

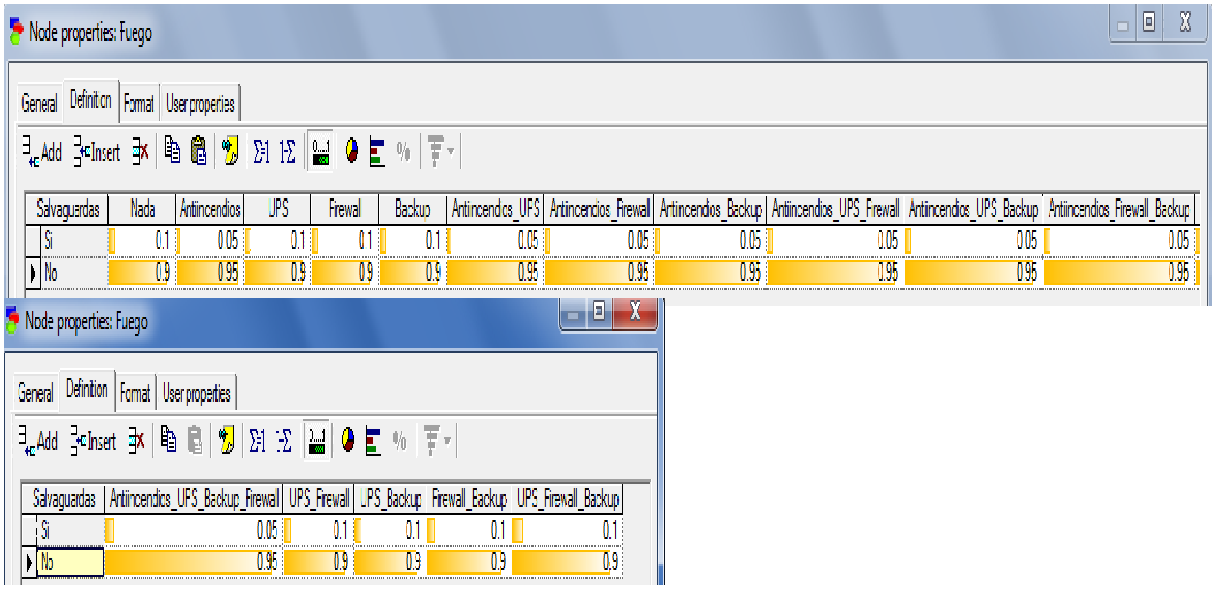


Figura 3.9: P(fuego) representado en la herramienta Genie

En segundo lugar, pasamos a evaluar la amenaza Corte Eléctrico. De la misma manera, para esta amenaza la probabilidad de ocurrencia será diferente según las contramedidas establecidas.

- P(Corte Eléctrico | no salvaguardas) = 0,35
- P(Corte Eléctrico | Antiincendios) = 0,35

- P(Corte Eléctrico | UPS) = 0,1
- P(Corte Eléctrico | Firewall) = 0,35
- P(Corte Eléctrico | Backup) = 0,35
- P(Corte Eléctrico | Antiincendios y UPS) = 0,1
- P(Corte Eléctrico | Antiincendios y Firewall) = 0,35
- P(Corte Eléctrico | Antiincendios y Backup) = 0,35
- P(Corte Eléctrico | Antiincendios, UPS y Firewall) = 0,1
- P(Corte Eléctrico | Antiincendios, UPS y Backup) = 0,1
- P(Corte Eléctrico | Antiincendios, Firewall y Backup) = 0,35
- P(Corte Eléctrico | Antiincendios, UPS, Backup y Firewall) = 0,1
- P(Corte Eléctrico | UPS y Firewall) = 0,1
- P(Corte Eléctrico | UPS y Backup) = 0,1
- P(Corte Eléctrico | Firewall y Backup) = 0,35
- P(Corte Eléctrico | UPS, Firewall y Backup) = 0,1

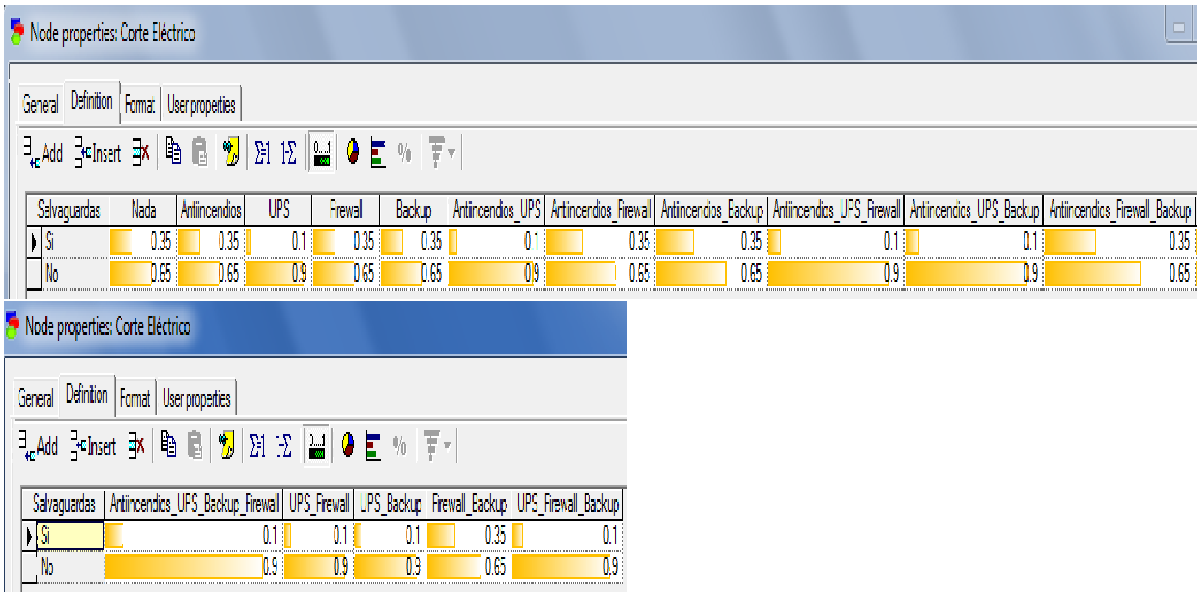


Figura 3.10: P(Corte Eléctrico) representado en la herramienta Genie

En tercer lugar, se considera la amenaza Denegación de Servicio (DoS) que, de nuevo, incidirá en el sistema bajo estudio en función de las salvaguardas que se hayan contemplado.

- P(DoS | no salvaguardas) = 0,3
- P(DoS | Antiincendios) = 0,3
- P(DoS | UPS) = 0,3
- P(DoS | Firewall) = 0,1
- P(DoS | Backup) = 0,3
- P(DoS | Antiincendios y UPS) = 0,3
- P(DoS | Antiincendios y Firewall) = 0,1
- P(DoS | Antiincendios y Backup) = 0,3
- P(DoS | Antiincendios, UPS y Firewall) = 0,1
- P(DoS | Antiincendios, UPS y Backup) = 0,3
- P(DoS | Antiincendios, Firewall y Backup) = 0,1
- P(DoS | Antiincendios, UPS, Backup y Firewall) = 0,1
- P(DoS | UPS y Firewall) = 0,1
- P(DoS | UPS y Backup) = 0,3
- P(DoS | Firewall y Backup) = 0,1
- P(DoS | UPS, Firewall y Backup) = 0,1

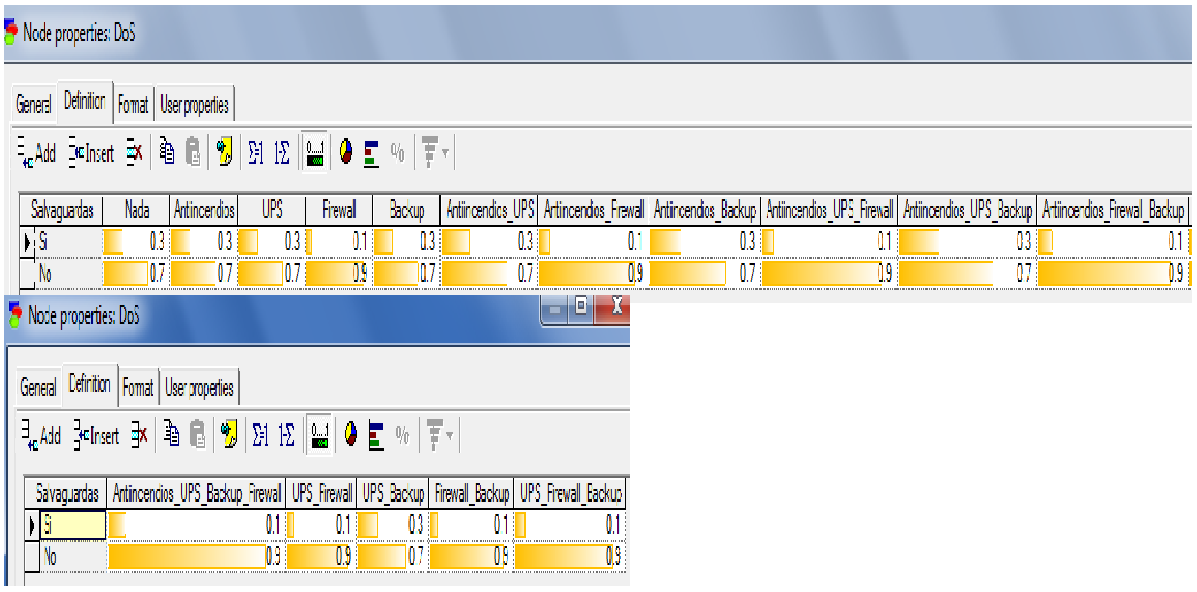


Figura 3.11: P(DoS) representado en la herramienta Genie

Por último, vemos cómo la amenaza Virus también verá variada su probabilidad de aparición en función de las salvaguardas utilizadas. En este punto, debemos aclarar que las probabilidades que se muestran a continuación se refieren a la probabilidad de que un ataque por Virus sea exitoso, no sólo a la probabilidad de que la institución sea objeto de un ataque.

- P(virus | no salvaguardas) = 0,4
- P(virus | Antiincendios) = 0,4
- P(virus | UPS) = 0,4
- P(virus | Firewall) = 0,2
- P(virus | Backup) = 0,4
- P(virus | Antiincendios y UPS) = 0,4
- P(virus | Antiincendios y Firewall) = 0,2
- P(virus | Antiincendios y Backup) = 0,4
- P(virus | Antiincendios, UPS y Firewall) = 0,2
- P(virus | Antiincendios, UPS y Backup) = 0,4

- P(virus | Antiincendios, Firewall y Backup) = 0,2
- P(virus | Antiincendios, UPS, Backup y Firewall) = 0,2
- P(virus | UPS y Firewall) = 0,2
- P(virus | UPS y Backup) = 0,4
- P(virus | Firewall y Backup) = 0,2
- P(virus | UPS, Firewall y Backup) = 0,2

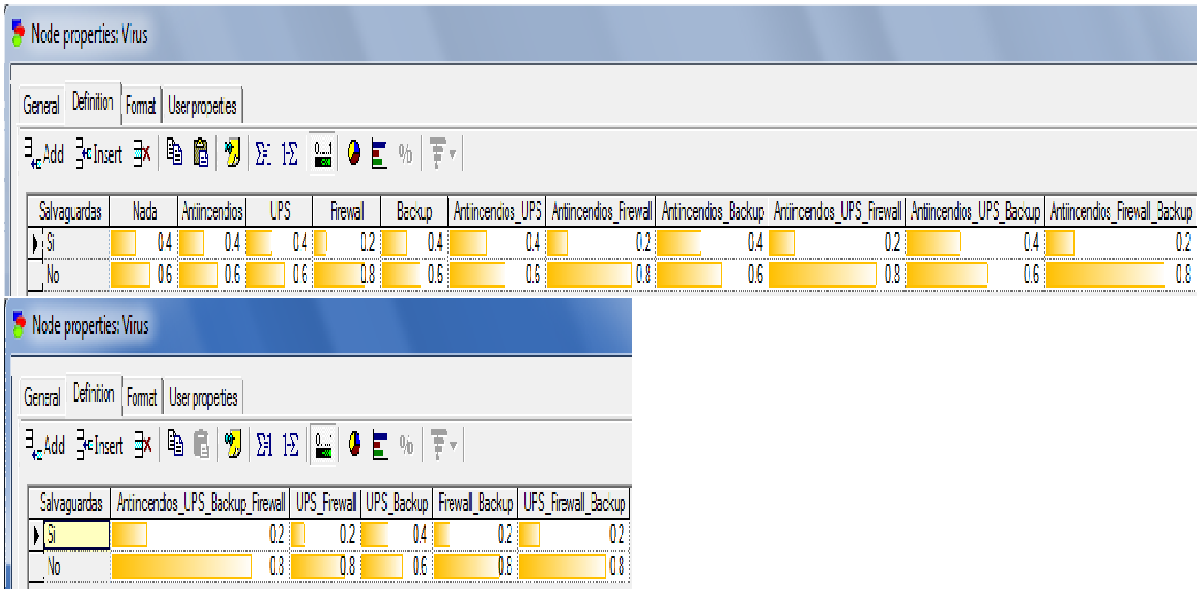


Figura 3.12: P(Virus) representado en la herramienta Genie

Nodos de Probabilidad de Activos afectados

Las amenazas anteriores podrían afectar directamente a los activos de la empresa, lo cual se verá reflejado directamente en forma de costes.

Para empezar, en el caso del activo Instalaciones se verían claramente afectados por la aparición de un fuego. En este caso hemos considerado unos costes de 50.000 €.

- P(coste 50.000 € | no salvaguardas) = 1
- P(coste 50.000 € | Antiincendios) = 0,3
- P(coste 50.000 € | UPS) = 1
- P(coste 50.000 € | Firewall) = 1

- P(coste 50.000€ | Backup) = 1
- P(coste 50.000€ | Antiincendios y UPS) = 0,3
- P(coste 50.000€ | Antiincendios y Firewall) = 0,3
- P(coste 50.000€ | Antiincendios y Backup) = 0,3
- P(coste 50.000€ | Antiincendios, UPS y Firewall) = 0,3
- P(coste 50.000€ | Antiincendios, UPS y Backup) = 0,3
- P(coste 50.000€ | Antiincendios, Firewall y Backup) = 0,3
- P(coste 50.000€ | Antiincendios, UPS, Backup y Firewall) = 0,3
- P(coste 50.000€ | UPS y Firewall) = 1
- P(coste 50.000€ | UPS y Backup) = 1
- P(coste 50.000€ | Firewall y Backup) = 1
- P(coste 50.000€ | UPS, Firewall y Backup) = 1

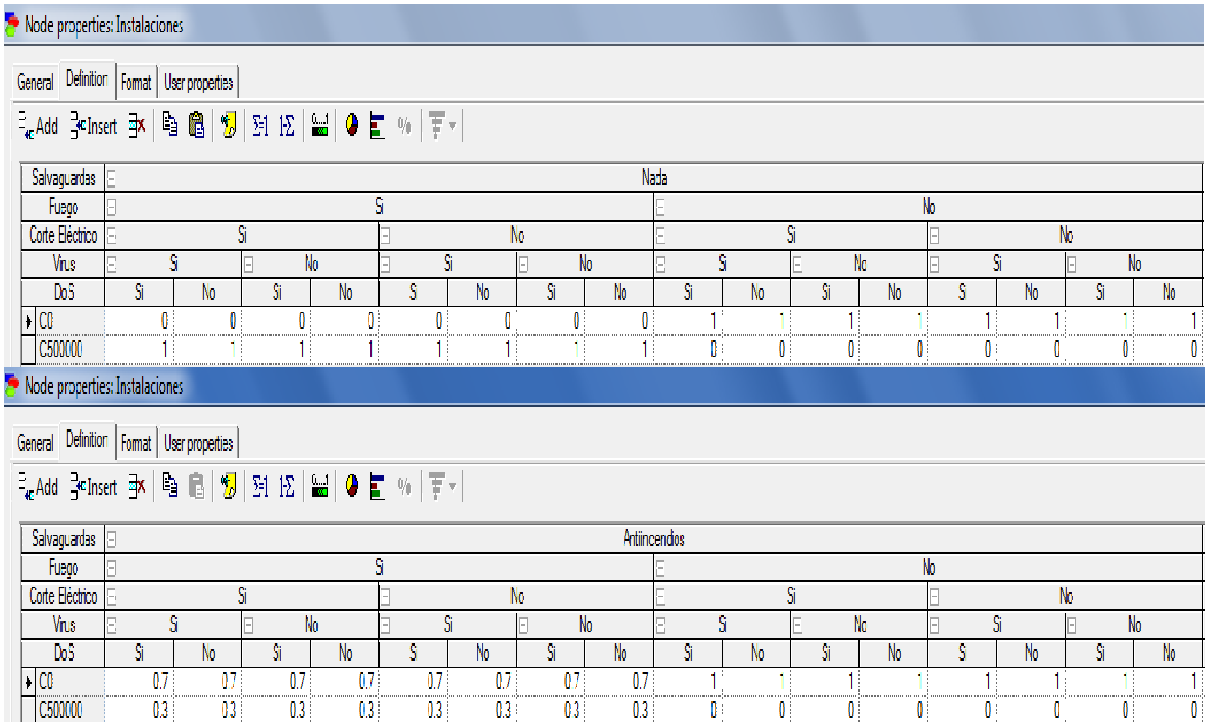


Figura 3.13: Probabilidad de incidencia en el Coste de las Instalaciones representada en la herramienta Genie

A continuación, pasamos a tratar el activo Datos. En esta ocasión las amenazas por las que se vería afectado serán tanto la amenaza Fuego como la amenaza Virus, por lo que habría que contemplar ambas junto a las salvaguardas consideradas. Para este caso hemos estimado unos costes que varían entre 0€, 10.000€ (si le afecta un virus) y 30.000€ (en caso de que se vea afectado por un fuego).

- P(coste 30.000€ | no salvaguardas) = 1
- P(coste 30.000€ | Antiincendios) = 0,05
- P(coste 10.000€ | Antiincendios) = 0,4
- P(coste 30.000€ | UPS) = 1
- P(coste 10.000€ | UPS) = 0,4
- P(coste 30.000€ | Firewall) = 1
- P(coste 10.000€ | Firewall) = 0,2
- P(coste 30.000€ | Backup) = 0,05
- P(coste 10.000€ | Backup) = 0,05
- P(coste 30.000€ | Antiincendios y UPS) = 0,05
- P(coste 10.000€ | Antiincendios y UPS) = 0,4
- P(coste 30.000€ | Antiincendios y Firewall) = 0,05
- P(coste 10.000€ | Antiincendios y Firewall) = 0,2
- P(coste 30.000€ | Antiincendios y Backup) = 0,05
- P(coste 10.000€ | Antiincendios y Backup) = 0,05
- P(coste 30.000€ | Antiincendios, UPS y Firewall) = 0,05
- P(coste 10.000€ | Antiincendios, UPS y Firewall) = 0,2
- P(coste 30.000€ | Antiincendios, UPS y Backup) = 0,05
- P(coste 10.000€ | Antiincendios, UPS y Backup) = 0,05
- P(coste 30.000€ | Antiincendios, Firewall y Backup) = 0,05
- P(coste 10.000€ | Antiincendios, Firewall y Backup) = 0,05

- P(coste 30.000€ | Antiincendios, UPS, Backup y Firewall) = 0,05
- P(coste 10.000€ | Antiincendios, UPS, Backup y Firewall) = 0,05
- P(coste 30.000€ | UPS y Firewall) = 1
- P(coste 10.000€ | UPS y Firewall) = 0,2
- P(coste 30.000€ | UPS y Backup) = 0,05
- P(coste 10.000€ | UPS y Backup) = 0,05
- P(coste 30.000€ | Firewall y Backup) = 0,05
- P(coste 10.000€ | Firewall y Backup) = 0,05
- P(coste 30.000€ | UPS, Firewall y Backup) = 0,05
- P(coste 10.000€ | UPS, Firewall y Backup) = 0,05

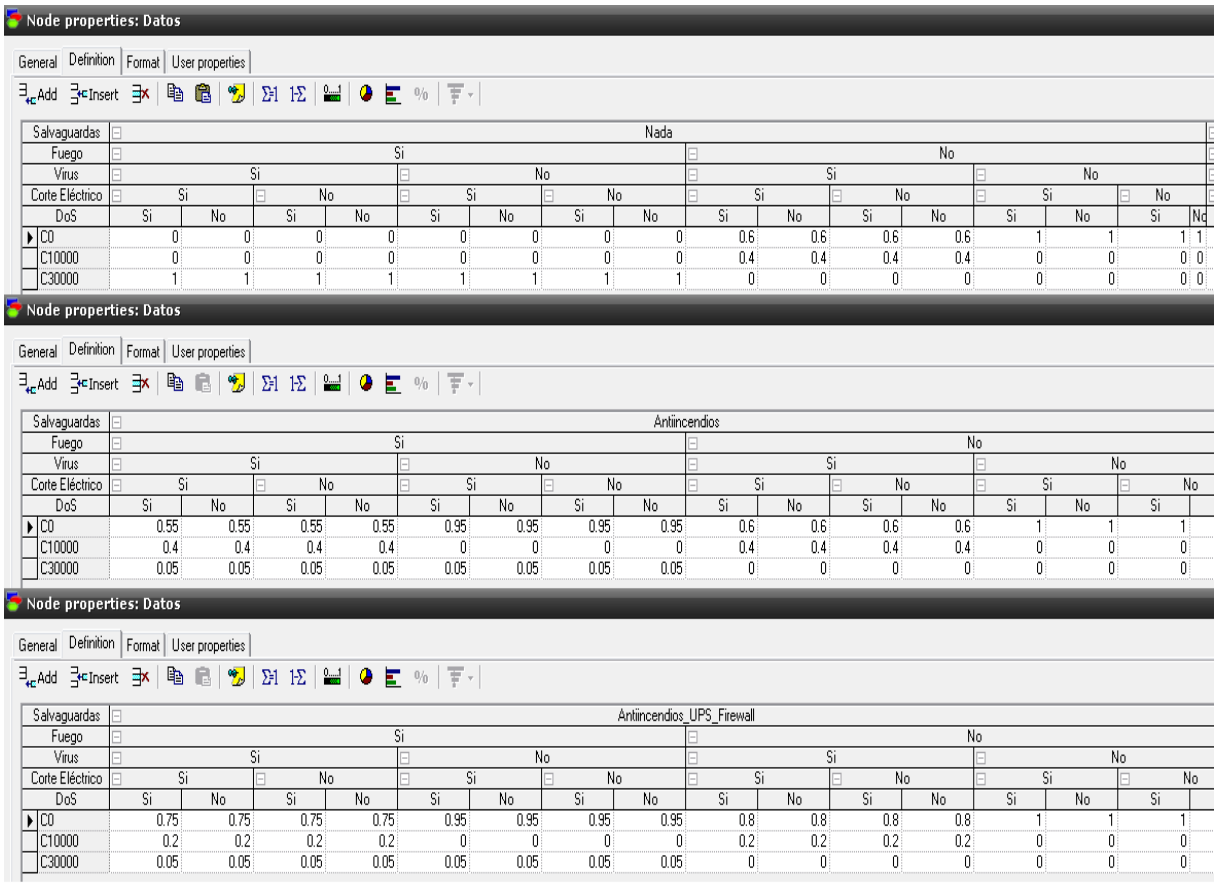


Figura 3.14: Probabilidad de incidencia en el Coste del activo Datos representada en la herramienta Genie

En el caso del activo Equipos Informáticos, se vería comprometido sin ninguna duda por la aparición de un Fuego. El rango de costes asociados a este activo se ha fijado en el rango de los 0 € a los 20.000 €, según la existencia de unas u otras medidas de seguridad.

- P(coste 20.000 € | no salvaguardas) = 1
- P(coste 20.000 € | Antiincendios) = 0,3
- P(coste 20.000 € | UPS) = 1
- P(coste 20.000 € | Firewall) = 1
- P(coste 20.000 € | Backup) = 1
- P(coste 20.000 € | Antiincendios y UPS) = 0,3
- P(coste 20.000 € | Antiincendios y Firewall) = 0,3
- P(coste 20.000 € | Antiincendios y Backup) = 0,3
- P(coste 20.000 € | Antiincendios, UPS y Firewall) = 0,3
- P(coste 20.000 € | Antiincendios, UPS y Backup) = 0,3
- P(coste 20.000 € | Antiincendios, Firewall y Backup) = 0,3
- P(coste 20.000 € | Antiincendios, UPS, Backup y Firewall) = 0,3
- P(coste 20.000 € | UPS y Firewall) = 1
- P(coste 20.000 € | UPS y Backup) = 1
- P(coste 20.000 € | Firewall y Backup) = 1
- P(coste 20.000 € | UPS, Firewall y Backup) = 1

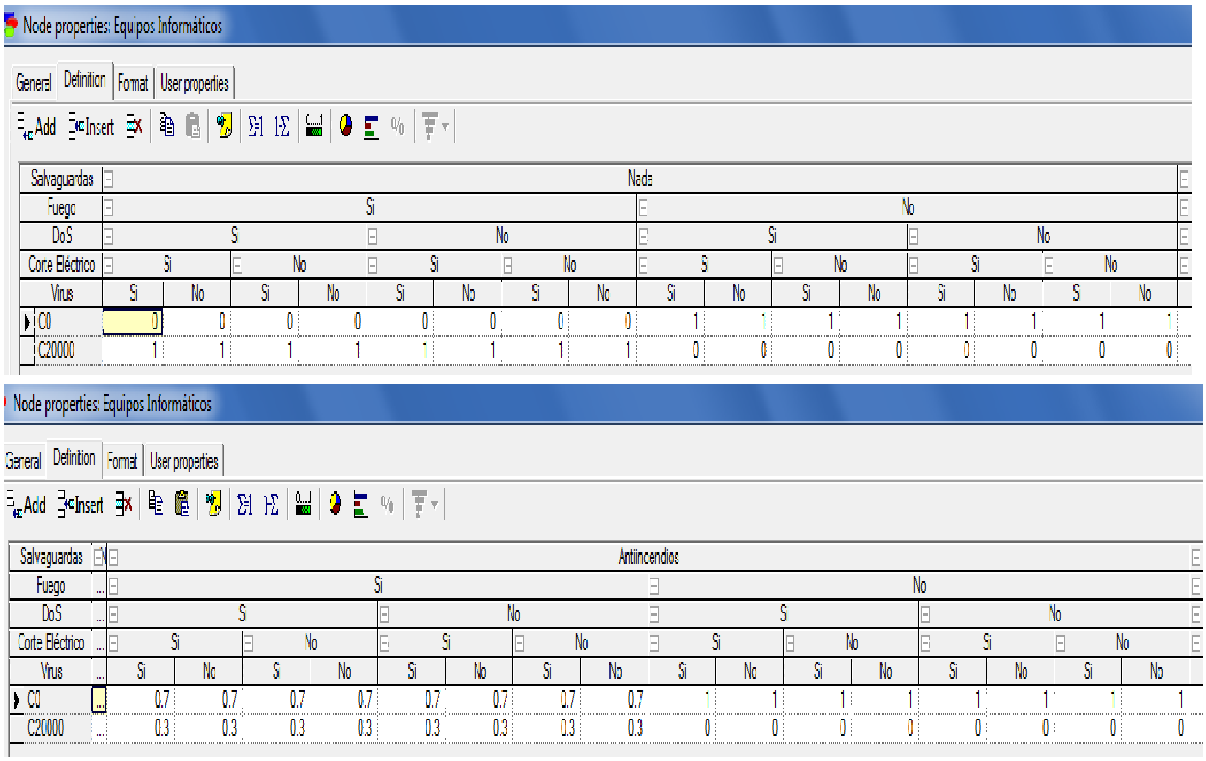


Figura 3.15: Representación de la probabilidad de incidencia en el Coste del Equipos Informáticos

Por último, pasamos a valorar el activo Servicio. Este Servicio ofrecido por una institución dependiente, al menos en parte, de una infraestructura TI, podría verse interrumpido por todas y cada una de las amenazas que estamos teniendo en cuenta en la realización de este estudio. Hemos considerados que los Costes asociados a la interrupción del Servicio se situarán entre los 0€ y los 15.000€, según las distintas combinaciones posibles de amenazas y salvaguardas. Parte de esas combinaciones se pueden apreciar en la figura 3.16.

- P(coste 15.000€ | no salvaguardas) = 1
- P(coste 15.000€ | Antiincendios) = 1
- P(coste 15.000€ | UPS) = 1
- P(coste 15.000€ | Firewall) = 1
- P(coste 15.000€ | Backup) = 1
- P(coste 15.000€ | Antiincendios y UPS) = 0,95
- P(coste 15.000€ | Antiincendios y Firewall) = 0,9

- P(coste 15.000€ | Antiincendios y Backup) = 1
- P(coste 15.000€ | Antiincendios, UPS y Firewall) = 0,45
- P(coste 15.000€ | Antiincendios, UPS y Backup) = 0,85
- P(coste 15.000€ | Antiincendios, Firewall y Backup) = 0,9
- P(coste 15.000€ | Antiincendios, UPS, Backup y Firewall) = 0,45
- P(coste 15.000€ | UPS y Firewall) = 1
- P(coste 15.000€ | UPS y Backup) = 1
- P(coste 15.000€ | Firewall y Backup) = 1
- P(coste 15.000€ | UPS, Firewall y Backup) = 1

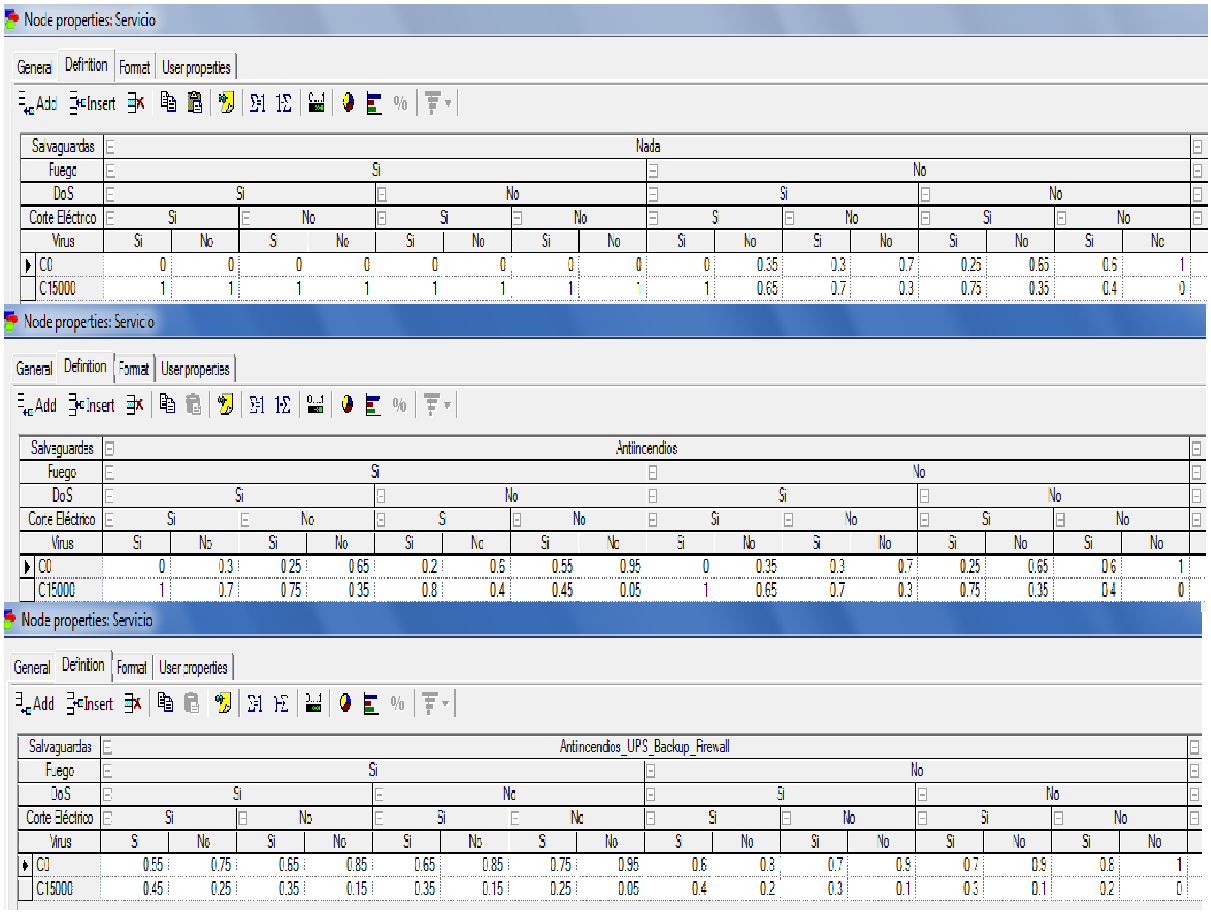


Figura 3.16: Representación de la probabilidad de los Costes asociados la interrupción del Servicio

Nodo Coste Total

Con todos estos elementos, podemos trabajar sobre el Coste Total del problema planteado, teniendo en cuenta los anteriores costes definidos, las amenazas descritas y la existencia, o no, de ciertas salvaguardas. En este punto, se puede apreciar la potencia y precisión de este sistema de toma de decisiones, ya que de ninguna otra forma hubiera sido posible detallar de forma tan granular este problema de seguridad. Obtenemos por tanto un análisis de riesgos muy detallado, capaz de ajustarse a la realidad vivida en cualquier tipo de organización actual.

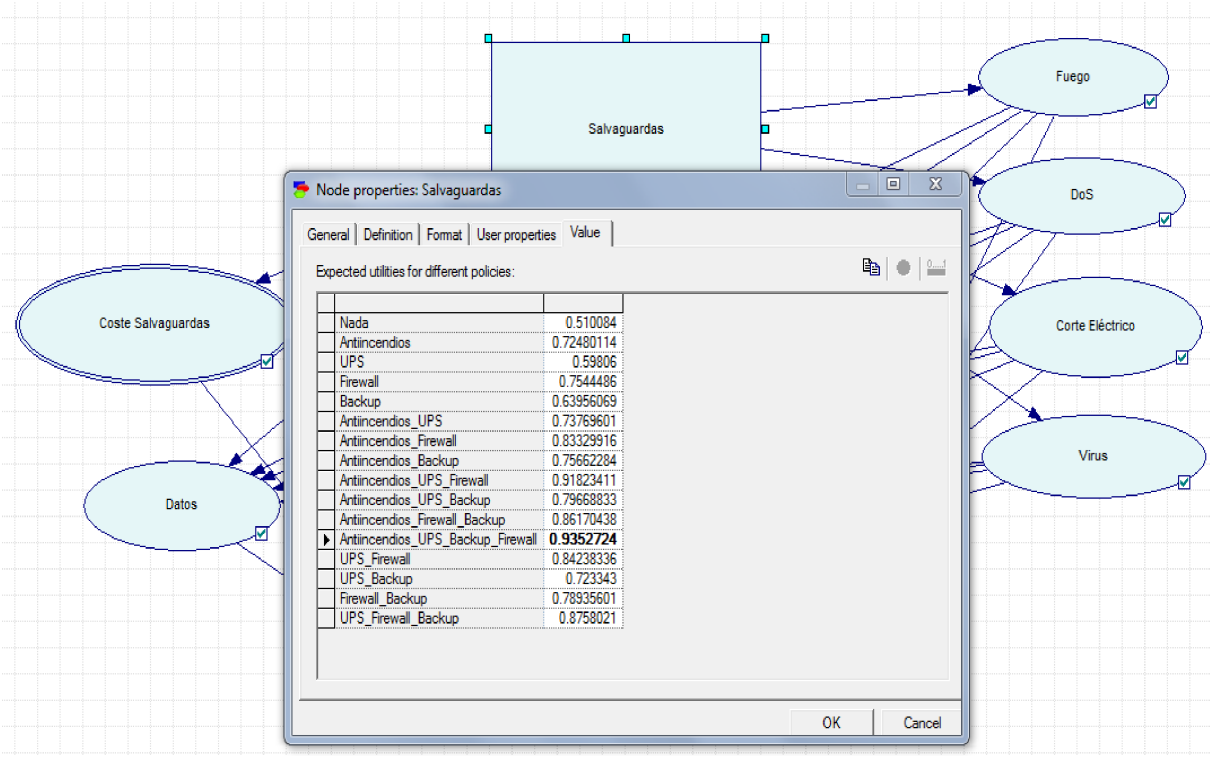


Figura 3.17: Coste Total

Nodo Utilidad

Por último, con todo el problema planteado calcularemos la utilidad esperada de cada una de las decisiones tomadas a lo largo del árbol de decisión. En este caso, daremos una utilidad menor cuanto mayor sea el coste asociado a dichas decisiones. Mientras, la utilidad será mayor según mejore la efectividad de la combinación de salvaguardas seleccionadas con respecto a la reducción de los costes derivados de las amenazas. Parte de esta distribución de utilidades para cada posible coste puede apreciarse en la figura 3.18. De esta manera se plantea un problema de optimización con la finalidad de conseguir unas medidas de seguridad robustas con un coste limitado a un cierto presupuesto, el cual marcará la decisión final. Una herramienta, por tanto, de gran valor para los responsables

de tomar este tipo de decisiones.

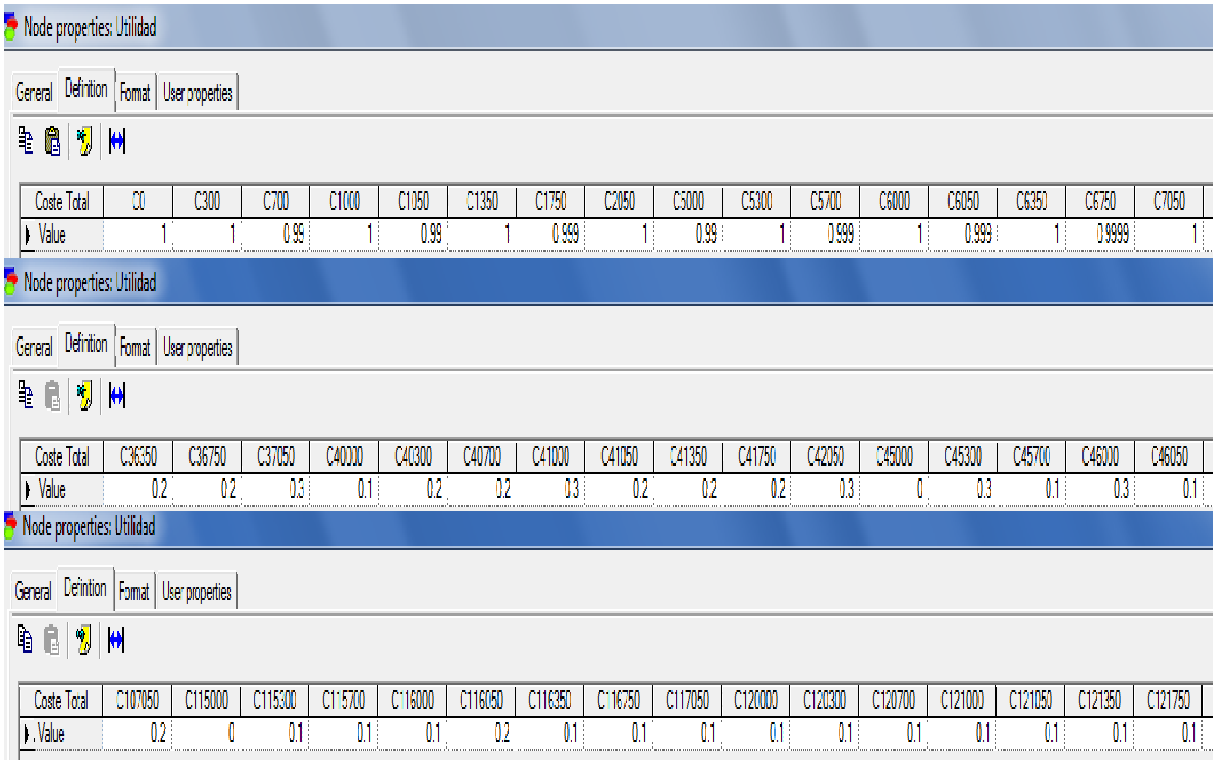


Figura 3.18: Utilidad

Resolución del problema

Finalmente, resolveríamos el problema obteniendo las decisiones óptimas a considerar en cada uno de los pasos dados. En cuanto a la elección de las salvaguardas, como se ve en la imagen que sigue, lo mejor en este caso sería claramente implantar todas las salvaguardas disponibles, es decir, un Firewall, un sistema Antiincendio, un sistema UPS y un sitema de Backup, obteniendo de esta manera una utilidad de 0.9352724 sobre 1. Para poder alcanzar esta utilidad máxima, asumimos que el presupuesto del que dispone la institución bajo estudio es capaz de cubrir la inversión necesaria para la implantación de todas las salvaguardas propuestas. De no ser así, optaríamos como solución por la combinación de salvaguardas con mejor utilidad cuyo coste se ajustase al presupuesto disponible. Aunque la implementación de todas estas salvaguardas suponga un cierto coste económico, su empleo haría que bajasen sustancialmente los costes derivados de las amenazas que se han visto en el diagrama de influencia presentado, con lo que su aplicación resultaría rentable en el sistema bajo estudio.

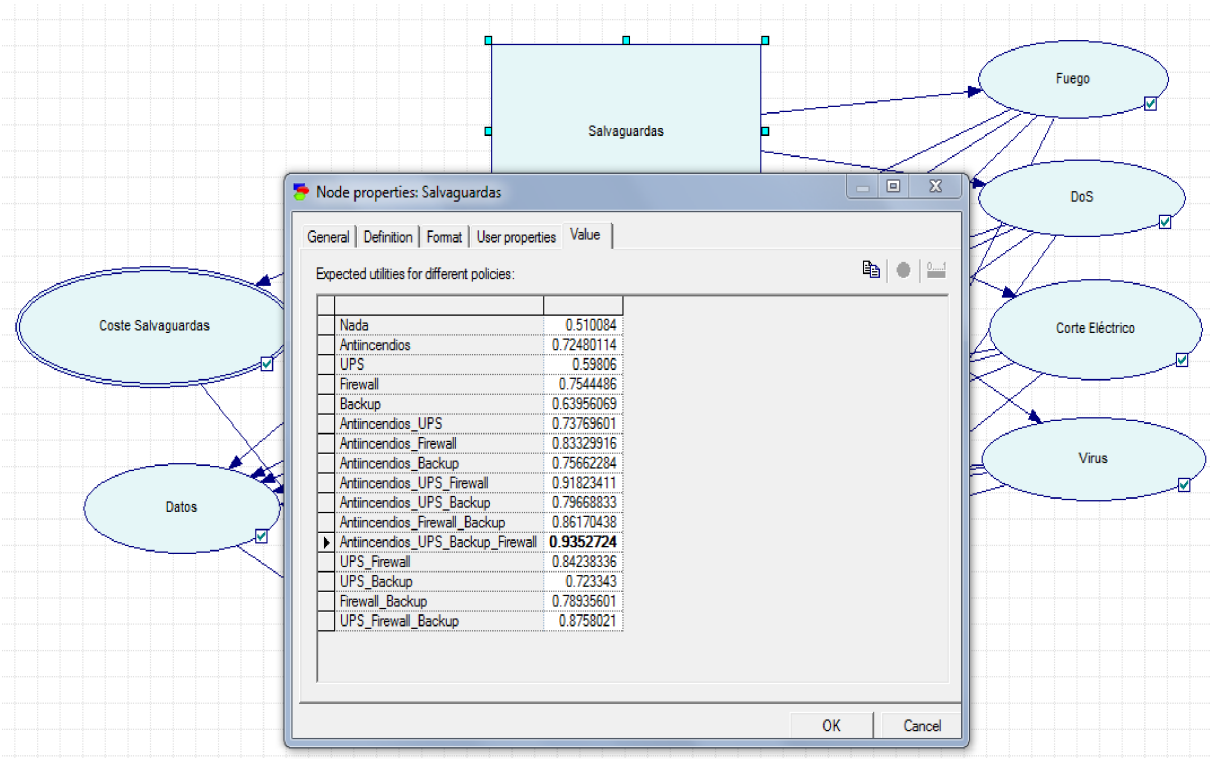
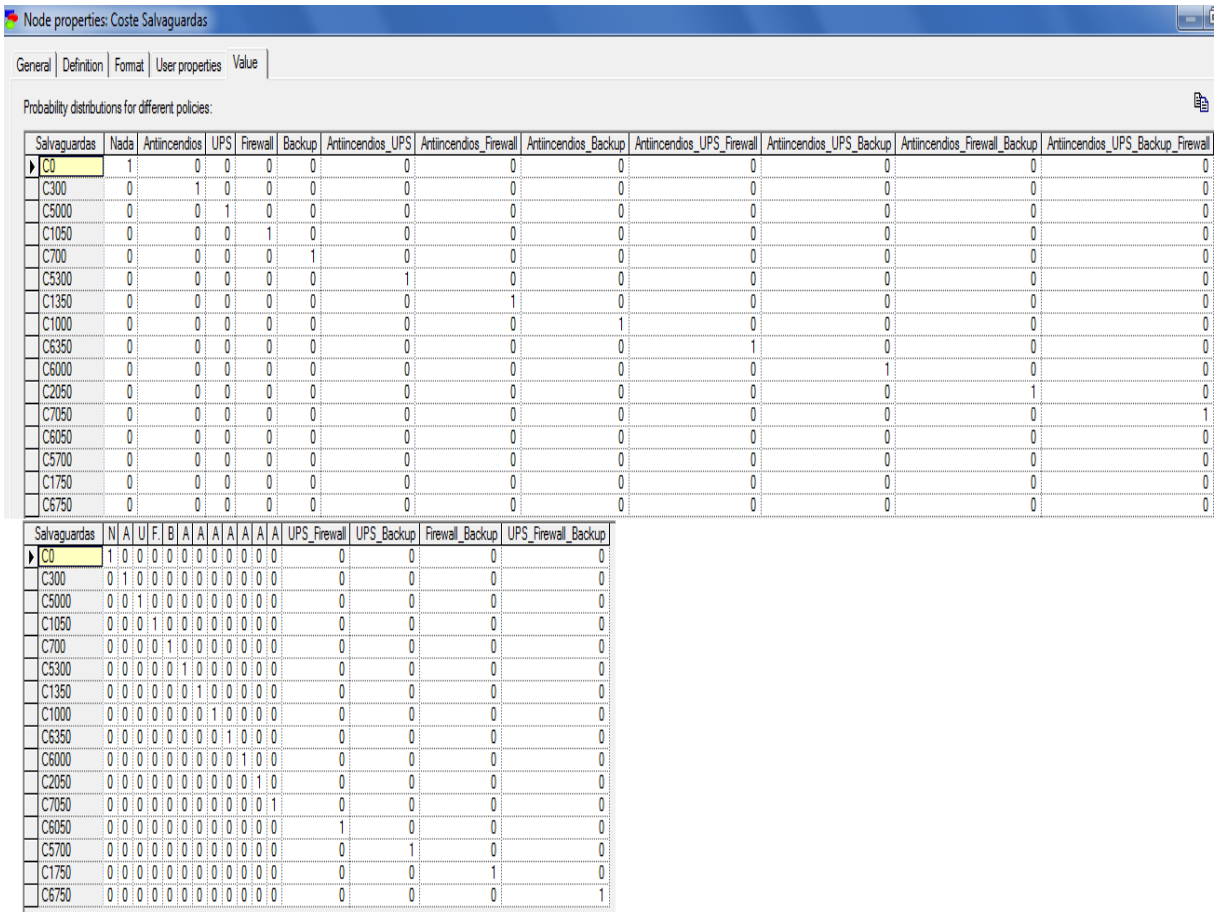


Figura 3.19: Utilidad esperada Savaguardas

En la figura 3.20 se observan cuáles serían esos costes referentes a las distintas combinaciones de salvaguardas que se podrían implantar.



Salvaguardas	Nada	Antiincendios	UPS	Firewall	Backup	Antiincendios_UPS	Antiincendios_Firewall	Antiincendios_Backup	Antiincendios_UPS_Firewall	Antiincendios_UPS_Backup	Antiincendios_Firewall_Backup	Antiincendios_UPS_Backup_Firewall
C0	1	0	0	0	0	0	0	0	0	0	0	0
C300	0	1	0	0	0	0	0	0	0	0	0	0
C5000	0	0	1	0	0	0	0	0	0	0	0	0
C1050	0	0	0	1	0	0	0	0	0	0	0	0
C700	0	0	0	0	1	0	0	0	0	0	0	0
C5300	0	0	0	0	0	1	0	0	0	0	0	0
C1350	0	0	0	0	0	0	1	0	0	0	0	0
C1000	0	0	0	0	0	0	0	1	0	0	0	0
C6350	0	0	0	0	0	0	0	0	1	0	0	0
C6000	0	0	0	0	0	0	0	0	0	1	0	0
C2050	0	0	0	0	0	0	0	0	0	0	1	0
C7050	0	0	0	0	0	0	0	0	0	0	0	1
C6050	0	0	0	0	0	0	0	0	0	0	0	0
C5700	0	0	0	0	0	0	0	0	0	0	0	0
C1750	0	0	0	0	0	0	0	0	0	0	0	0
C6750	0	0	0	0	0	0	0	0	0	0	0	0

Salvaguardas	N	A	U	F	B	A	A	A	A	A	A	UPS_Firewall	UPS_Backup	Firewall_Backup	UPS_Firewall_Backup
C0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C300	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
C5000	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
C1050	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
C700	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
C5300	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
C1350	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
C1000	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
C6350	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
C6000	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
C2050	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
C7050	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
C6050	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
C5700	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
C1750	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
C6750	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Figura 3.20: Costes por Salvaguardas

En la figura 3.21 se muestran las probabilidades sobre los costes que pueden sufrir las instalaciones de la institución bajo estudio. Se puede observar que el mejor margen de seguridad se obtendría siempre y cuando se utilice como contramedida un sistema antiincendios, ya que sería la amenaza fuego el principal elemento de agresión a considerar en este caso.

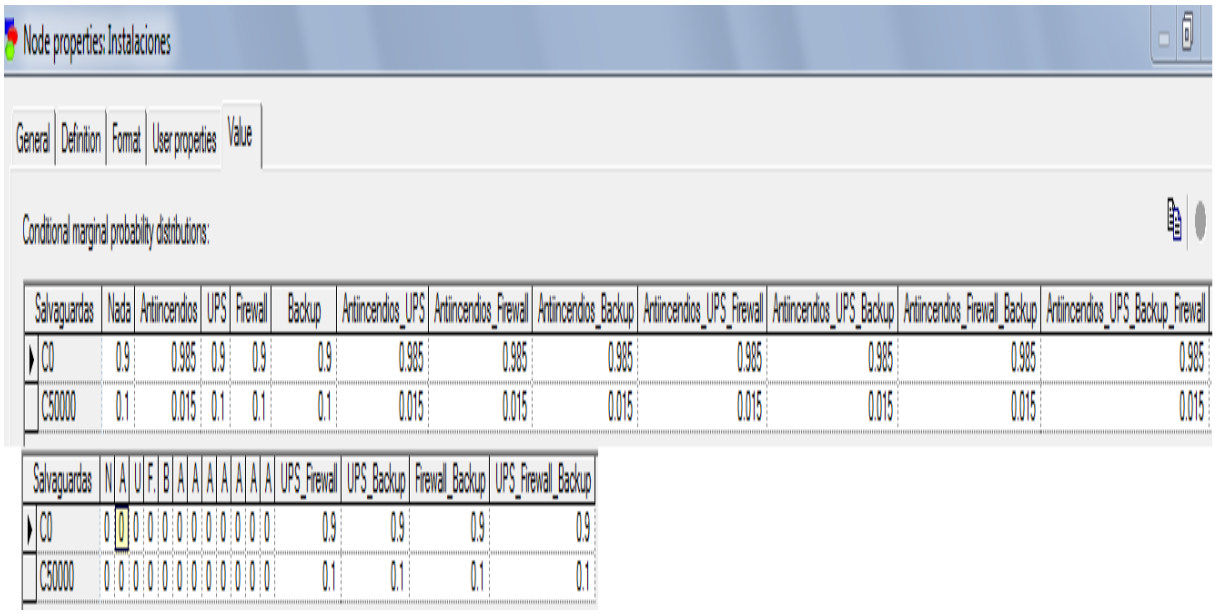
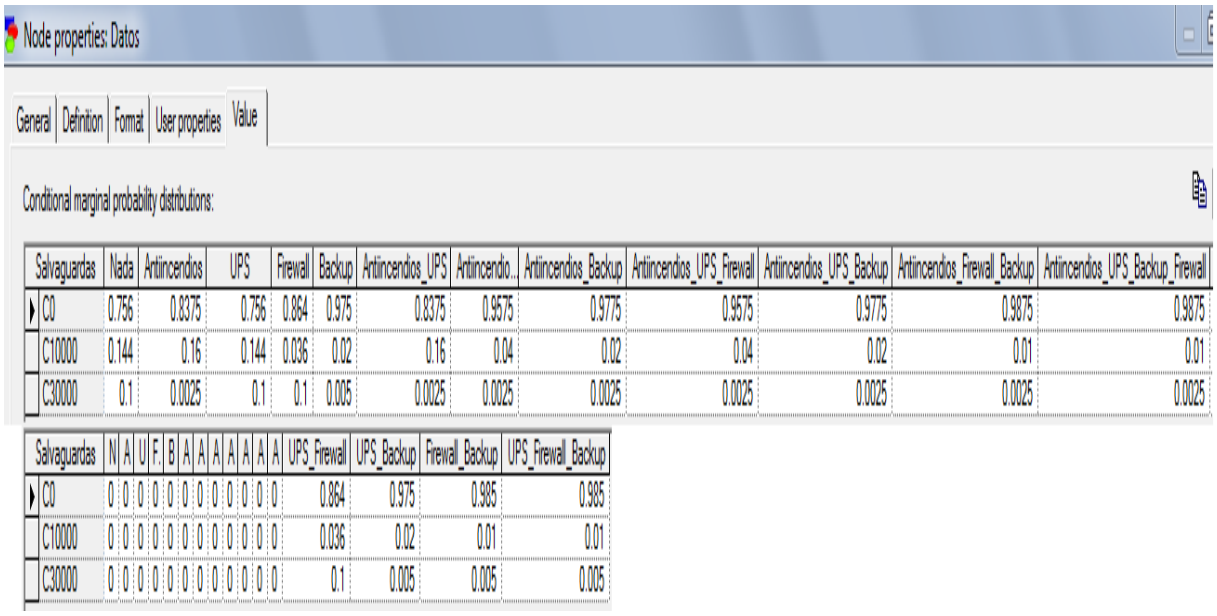


Figura 3.21: Probabilidad de sufrir ciertos costes en el activo Instalaciones según la combinación de Salvaguardas utilizada

En la figura 3.22 veríamos el mismo caso pero en relación con el activo Datos. En este caso tanto la amenaza Fuego como la amenaza Virus incidirían en el mismo, por lo que de tener implantadas las salvaguardas firewall y sistema antiindencios se reduciría considerablemente la probabilidad de tener unos costes elevados por la incidencia de dichas amenazas. Pero, en este caso, la contramedida más eficaz sería la implantación de un sistema de Backup, lo que, combinado con las dos anteriores salvaguardas, nos deja una probabilidad de 0.9875 de que los costes derivados de las amenazas tenidas en cuenta sean nulos.

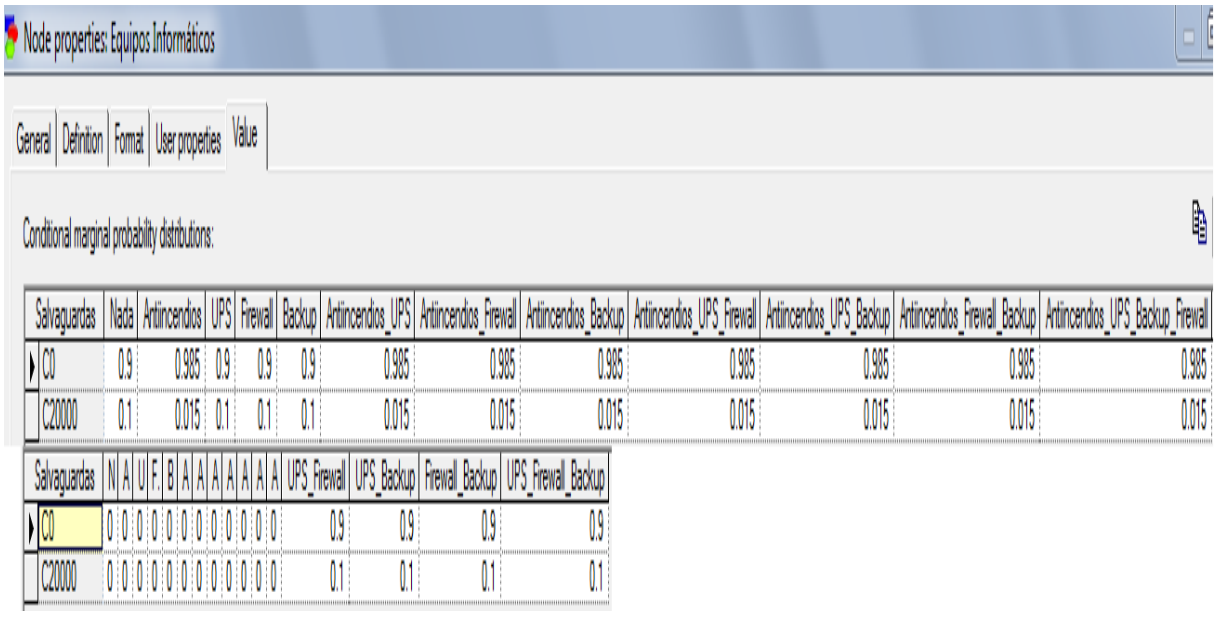


Salvaguardas	Nada	Antiincendios	UPS	Firewall	Backup	Antiincendios_UPS	Antiincendio...	Antiincendios_Backup	Antiincendios_UPS_Firewall	Antiincendios_UPS_Backup	Antiincendios_Firewall_Backup	Antiincendios_UPS_Backup_Firewall
C0	0.756	0.8375	0.756	0.864	0.975	0.8375	0.9575	0.9775	0.9575	0.9775	0.9875	0.9875
C10000	0.144	0.16	0.144	0.036	0.02	0.16	0.04	0.02	0.04	0.02	0.01	0.01
C30000	0.1	0.0025	0.1	0.1	0.005	0.0025	0.0025	0.0025	0.0025	0.0025	0.0025	0.0025

Salvaguardas	N	A	U	F	B	A	A	A	A	A	A	UPS_Firewall	UPS_Backup	Firewall_Backup	UPS_Firewall_Backup
C0	0	0	0	0	0	0	0	0	0	0	0	0.864	0.975	0.985	0.985
C10000	0	0	0	0	0	0	0	0	0	0	0	0.036	0.02	0.01	0.01
C30000	0	0	0	0	0	0	0	0	0	0	0	0.1	0.005	0.005	0.005

Figura 3.22: Probabilidad de sufrir ciertos costes en el activo Datos según la combinación de Salvaguardas utilizada

La figura 3.23 hace referencia a la distribución de probabilidades para los costes asociados al nodo Equipos Informáticos. De nuevo en este caso la contramedida más eficaz será el sistema Antiincendios.



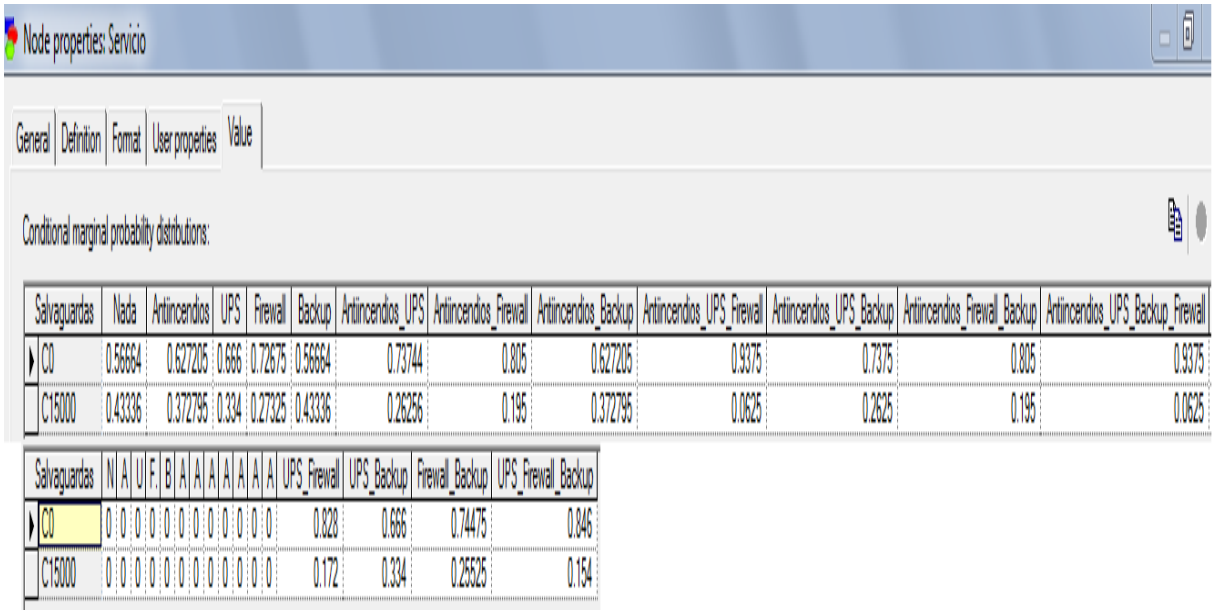
Salvaguardas	Nada	Antiincendios	UPS	Firewall	Backup	Antiincendios_UPS	Antiincendios_Firewall	Antiincendios_Backup	Antiincendios_UPS_Firewall	Antiincendios_UPS_Backup	Antiincendios_Firewall_Backup	Antiincendios_UPS_Backup_Firewall
C0	0.9	0.985	0.9	0.9	0.9	0.985	0.985	0.985	0.985	0.985	0.985	0.985
C20000	0.1	0.015	0.1	0.1	0.1	0.015	0.015	0.015	0.015	0.015	0.015	0.015

Salvaguardas	N	A	U	F	B	A	A	A	A	A	A	UPS_Firewall	UPS_Backup	Firewall_Backup	UPS_Firewall_Backup
C0	0	0	0	0	0	0	0	0	0	0	0	0.9	0.9	0.9	0.9
C20000	0	0	0	0	0	0	0	0	0	0	0	0.1	0.1	0.1	0.1

Figura 3.23: Probabilidad de sufrir ciertos costes en el activo Equipos Informáticos según la combinación de Salvaguardas utilizada

Por último, en la figura 3.24 analizamos el caso para el nodo Servicio. En esta ocasión todan las salvaguardas utilizadas muestran su utilidad en mayor o menor medida, de lo que

se desprende que la mayor probabilidad de anular completamente los costes derivados de las amenazas que nos acechan sería la combinación de todas las salvaguardas disponibles.

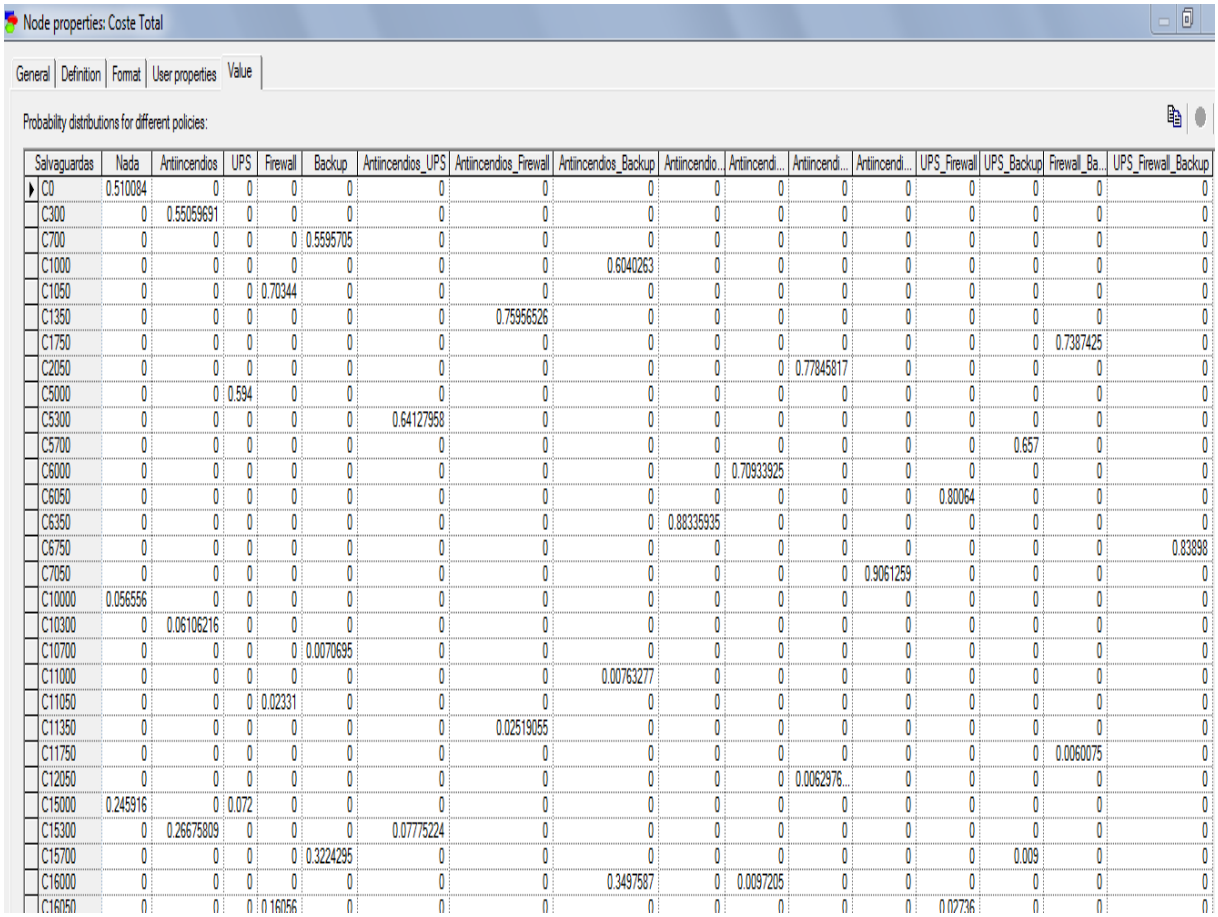


Salvaguardas	Nada	Antiincendios	UPS	Firewall	Backup	Antiincendios_UPS	Antiincendios_Firewall	Antiincendios_Backup	Antiincendios_UPS_Firewall	Antiincendios_UPS_Backup	Antiincendios_Firewall_Backup	Antiincendios_UPS_Backup_Firewall
C0	0.56664	0.627205	0.666	0.72675	0.56664	0.73744	0.805	0.627205	0.9375	0.7375	0.805	0.9375
C15000	0.43336	0.372795	0.334	0.27325	0.43336	0.26256	0.195	0.372795	0.0625	0.2625	0.195	0.0625

Salvaguardas	N	A	U	F	B	A	A	A	A	A	A	UPS_Firewall	UPS_Backup	Firewall_Backup	UPS_Firewall_Backup
C0	0	0	0	0	0	0	0	0	0	0	0	0.828	0.666	0.74475	0.846
C15000	0	0	0	0	0	0	0	0	0	0	0	0.172	0.334	0.25525	0.154

Figura 3.24: Probabilidad de sufrir ciertos costes en el activo Servicio según la combinación de Salvaguardas utilizada

En la figura 3.25 vemos las probabilidades referentes a los costes globales, donde se contemplan tanto las cantidades relativas a las salvaguardas como a las derivadas de la incidencia de alguna de las amenazas sobre los activos considerados.


Node properties: Coste Total

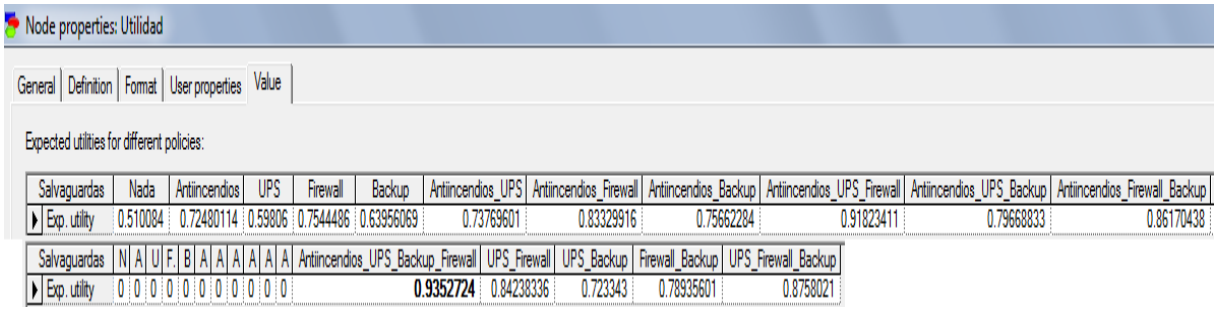
General | Definition | Format | User properties | Value

Probability distributions for different policies:

Salvaguardas	Nada	Antiincendios	UPS	Firewall	Backup	Antiincendios_UPS	Antiincendios_Firewall	Antiincendios_Backup	Antiincendio...	Antiincendi...	Antiincendi...	Antiincendi...	UPS_Firewall	UPS_Backup	Firewall_Ba...	UPS_Firewall_Backup
C0	0.510084	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C300	0	0.55059691	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C700	0	0	0	0	0.5595705	0	0	0	0	0	0	0	0	0	0	0
C1000	0	0	0	0	0	0	0	0.6040263	0	0	0	0	0	0	0	0
C1050	0	0	0	0.70344	0	0	0	0	0	0	0	0	0	0	0	0
C1350	0	0	0	0	0	0	0.75956526	0	0	0	0	0	0	0	0	0
C1750	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.7387425	0
C2050	0	0	0	0	0	0	0	0	0	0	0.77845817	0	0	0	0	0
C5000	0	0	0.594	0	0	0	0	0	0	0	0	0	0	0	0	0
C5300	0	0	0	0	0	0.64127958	0	0	0	0	0	0	0	0	0	0
C5700	0	0	0	0	0	0	0	0	0	0	0	0	0	0.657	0	0
C6000	0	0	0	0	0	0	0	0	0	0.70933925	0	0	0	0	0	0
C6050	0	0	0	0	0	0	0	0	0	0	0	0	0.80064	0	0	0
C6350	0	0	0	0	0	0	0	0	0.88335935	0	0	0	0	0	0	0
C6750	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.83898
C7050	0	0	0	0	0	0	0	0	0	0	0	0.9061259	0	0	0	0
C10000	0.056556	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C10300	0	0.06106216	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C10700	0	0	0	0	0.0070695	0	0	0	0	0	0	0	0	0	0	0
C11000	0	0	0	0	0	0	0	0.00763277	0	0	0	0	0	0	0	0
C11050	0	0	0	0.02331	0	0	0	0	0	0	0	0	0	0	0	0
C11350	0	0	0	0	0	0	0.02519055	0	0	0	0	0	0	0	0	0
C11750	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.0060075	0
C12050	0	0	0	0	0	0	0	0	0	0	0.0062976...	0	0	0	0	0
C15000	0.245916	0	0.072	0	0	0	0	0	0	0	0	0	0	0	0	0
C15300	0	0.26675809	0	0	0	0.07775224	0	0	0	0	0	0	0	0	0	0
C15700	0	0	0	0	0.3224295	0	0	0	0	0	0	0	0	0.009	0	0
C16000	0	0	0	0	0	0	0	0.3497587	0	0.0097205	0	0	0	0	0	0
C16050	0	0	0	0.16056	0	0	0	0	0	0	0	0	0.02736	0	0	0

Figura 3.25: Detalle de la probabilidad obtenida para cada uno de los posibles costes definidos en el nodo Coste Total

Para finalizar, en la figura 3.26 se ven finalmente las utilidades esperadas. Podemos apreciar que la utilidad más alta es la relativa al empleo de todas las salvaguardas disponibles, siendo por tanto ésta la decisión más óptima.


Node properties: Utilidad

General | Definition | Format | User properties | Value

Expected utilities for different policies:

Salvaguardas	Nada	Antiincendios	UPS	Firewall	Backup	Antiincendios_UPS	Antiincendios_Firewall	Antiincendios_Backup	Antiincendios_UPS_Firewall	Antiincendios_UPS_Backup	Antiincendios_Firewall_Backup
Exp. utility	0.510084	0.72480114	0.59806	0.7544486	0.63956069	0.73769601	0.83329916	0.75662284	0.91823411	0.79668833	0.86170438

Salvaguardas	N	A	U	F.	B	A	A	A	A	A	A	Antiincendios_UPS_Backup_Firewall	UPS_Firewall	UPS_Backup	Firewall_Backup	UPS_Firewall_Backup
Exp. utility	0	0	0	0	0	0	0	0	0	0	0	**0.9352724**	0.84238336	0.723343	0.78935601	0.8758021

Figura 3.26: Distribución de probabilidad del nodo Utilidad

El modelo que acabamos de presentar describe el problema del análisis de riesgos desde

un punto de vista muy general. En el próximo capítulo trataremos de incidir en él de una manera más rigurosa, identificando fuentes de información disponibles públicamente que nos ayuden a construir las distribuciones involucradas.

Capítulo 4

Fuentes de datos para un Modelo Continuo

En este capítulo tratamos de dar un enfoque real al problema planteado en el capítulo anterior. Nuestro objetivo será obtener datos reales para cada una de las amenazas en estudio. El escenario planteado consitirá en la gestión de riesgos, para un año, de una organización que posea cierta infraestructura TI como, por ejemplo, un Centro de Procesamiento de Datos (CPD).

4.1. Amenazas

En los próximos apartados tratamos individualmente cada amenaza, centrando nuestro estudio en los datos relativos a probabilidad, duración y coste de cada una de ellas.

Fuegos

Para la amenaza Fuego, nos basaremos en los datos recogidos entre varios estudios realizados en diferentes partes del mundo, como el *World Fire Statistics Centre* financiado por The Geneva Association (World Fire Statistics, 2010), en el que se recogen datos estadísticos anuales de costes, daños, número y tiempo de las intervenciones, pérdidas humanas y materiales, etc; en distintos países.

Para la extrapolación al caso particular que queremos representar, por cercanía a un modelo español y por reducir los datos con respecto a valores a nivel mundial, nos centraremos en el informe realizado por el cuerpo de bomberos de Vitoria (2009). A partir de él, hemos obtenido los datos de intervenciones realizadas sobre edificios industriales dentro del total de edificios de la ciudad desde 1989 hasta 2009. Centrándonos en los datos más actuales (2005-2009) se localizaron el número de edificios industriales (Sistema de Indicador Urbano, 2009) y las intervenciones realizadas (Figura 4.1).

Año	Fuegos Totales	Edificios Ind.	F.Industria 3%	Exponential Smoothing	
2005	1.062	1.220	31,86	α =	0,5
2006	966	1.266	28,98	Edificios Ind.	Previsión
2007	991	1.320	29,73	1.220	-
2008	964	1.347	28	1.266	1.220
2009	904	-	28	1.320	1243
Exponential Smoothing:		1314,25		1.347	1281,5
				-	1314,25

Figura 4.1: Información Cuerpo de Bomberos del Ayto. de Vitoria

En la figura se detallan los fuegos ocurridos en toda la ciudad desde 2005 hasta 2009 y los fuegos que sólo afectaron a edificios industriales. Existía un problema con respecto a 2009, puesto que aún no estaba registrado el número exacto de edificios industriales. Para hallarlo, basándonos en los datos disponibles de los anteriores años, se ha realizado una aproximación por medio de la técnica de alisado exponencial (Exponential Smoothing, 2011), obteniendo el dato de 1314,25 edificios industriales para 2009. Esta técnica se usa normalmente en series temporales de datos para generar una estimación de la siguiente observación a través de una *suavización* de las observaciones anteriores.

A partir de estos datos, estimamos la probabilidad de que **en un año, en un edificio industrial se produzca un incendio**. Para ello, usaremos la distribución a priori:

$$\beta(1,1)$$

Teniendo en cuenta las observaciones de las que disponemos para un año (2008), tenemos la siguiente distribución a posteriori:

$$\beta(1+x, 1+n-x) -> \beta(1+28, 1+1347-28)$$

donde x será los fuegos que sólo afectaron a edificios industriales y n será el total de fuegos producidos en la ciudad de Vitoria. Por último, con los datos disponibles obtendríamos una distribución a posteriori basada en dos años (2008 y 2009) como sigue:

$$\beta(1+x_1+x_2, 1+(n_1-x_1)+(n_2-x_2)) -> \beta(1+28+28, 1+(1347-28)+(1314,25-28))$$

Resumimos esta distribución usando la media:

$$\widehat{p} = \frac{1+x_1+x_2}{2+n_1+n_2} = \mathbf{0,02140242},$$

que será nuestra estimación de la probabilidad de que en un año, en un edificio industrial se produzca un incendio.

Una vez llegado a nuestro objetivo, concluimos que el número de fuegos por año sigue una distribucion de Poisson $e^{-\lambda}\frac{\lambda^k}{k!}$ donde λ se deduce de la probabilidad de que haya cero fuegos:

$$p(0) = 1 - \widehat{p} = 0,9786 = e^{-\lambda}\frac{\lambda^0}{0!} = e^{-\lambda}$$

Despejando λ, tenemos $\lambda \simeq 0,021$. La distribución del número de fuegos sería entonces:

$$\text{P(k fuegos en un año)}= e^{-0,021}(\frac{0,021^k}{k!})$$

Fuego	
k	$Probabilidad$
0	$0,9786$
1	$0,0214$
2	$0,000457942$
3	$4,95E-06$
4	$3,57E-08$
5	$1,93E-10$
...	...

Tabla 4.1: Tabla de probabilidad para la amenaza Fuego

Una vez estimada la probabilidad de ocurrencia de la amenaza Fuego, nos centraremos en la duración de los mismos. Este dato nos proporcionará una información que influye directamente sobre los costes derivados de la gestión de la seguridad. Para el estudio de la duración de un fuego, volvemos a recurrir a los informes anteriormente mencionados. A partir de ellos, obtenemos los datos que se pueden ver en la figura 4.2.

TIEMPO	ACTUACIONES
SIN INTERVENCION	6
<15'	270
15'-30'	855
30'-1H.	1197
1H.-2H-	576
2H.-3H.	194
3H-6H.	117
6H.-10H.	25
>10H.	11
TOTAL	3.251

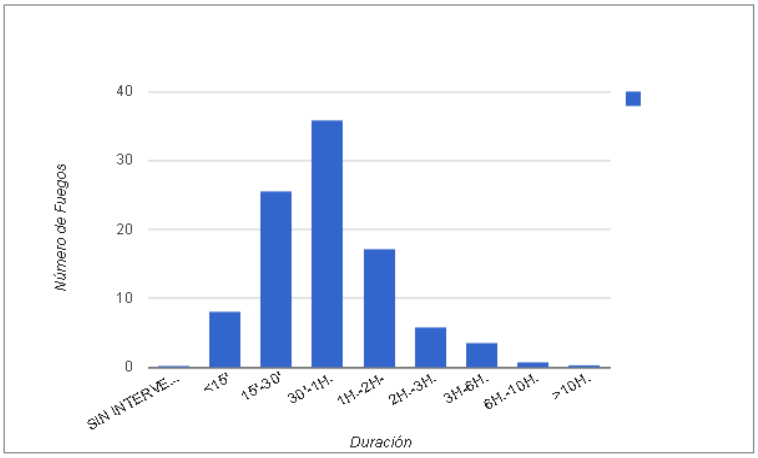


Figura 4.2: Histograma Fuegos

En la primera tabla se observa el número total de las intervenciones que realizó el cuerpo de bomberos del Ayuntamiento de Vitoria. A partir de estos datos, generamos el histograma mostrado, donde queda claramente reflejado que la mayoría de los fuegos producidos tienen una duración aproximada de entre 30 minutos y una hora. Consideraremos que la duración vendrá modelizada mediante una distribución Gamma(k,θ).

$$g(k,\theta) = \frac{x^{k-1}exp(-\frac{x}{\theta})}{\Gamma(k)\theta^k}$$

Aplicando el método de momentos tenemos, para la media

$$k\theta = m$$

y la varianza es

$$k\theta^2 = \sigma^2$$

de ahí se deduce $\theta = \frac{\sigma^2}{m}$ y $k = \frac{m^2}{\sigma^2}$. A partir de los valores empíricos m = 78 y $\sigma^2 =$ 7127,273, resolvemos las anteriores ecuaciones

$$\text{k} = 0{,}0536224$$
$$\theta = 91,3753$$

A continuación, pasamos a estudiar la influencia directa que se deriva de la duración de un incendio con respecto a los costes. Consideramos que la duración de un fuego guarda una relación directa con el porcentaje de destrucción del edificio afectado, cuanto más se prolongue el fuego, mayor será la incidencia sobre los activos de la empresa. Dado que no disponemos de información exacta acerca del tiempo a partir del cual la destrucción de un edificio sería fatal, hemos fijado dicho umbral en 2 horas. Teniendo en cuenta esta estimación, en la figura 4.3 podemos observar una representación gráfica de la evolución de la destrucción provocada por un incendio.

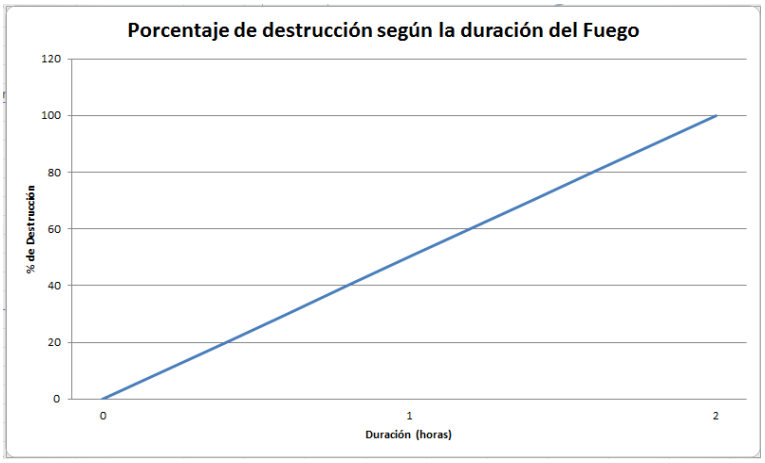


Figura 4.3: Evolución de la destrucción causada por Fuego en función del tiempo

Una vez halladas las probabilidades y los tiempos respecto de la amenaza Fuego, pasamos a analizar los costes derivados de la misma. Para ello, volvemos a recurrir a los informes realizados por la Geneva Association para 2010. En estos informes se encuentra detallado el gasto en protección antiincendios de un gran número de países en porcentaje de su PIB (Figura 4.4)

Cost of Fire Protection to Buildings

Average percentage of GDP (2005-07)

Country	%
Japan	0.14
Slovenia	0.16 (2002-04)
France	0.18
Czech Republic	0.19
Sweden	0.19
U.K.	0.22
New Zealand	0.24
Denmark	0.26
Belgium	0.29 (1998-2000)
Switzerland	0.29 (1989)
Netherlands	0.30
Singapore	0.31
Canada	0.32
Italy	0.35
Norway	0.36 (2003-05)
Australia	0.37 (2005)
USA	0.39
Hungary	0.42 (1987-88)

Figura 4.4: Porcentaje medio de gasto del PIB por países

Para obtener los costes del daño producido por los incendios, nos basaremos en el informe realizado por la CTIF (International Association of Fire and Rescue Service, 2008) donde se detalla, también para un buen número de países, una evaluación de los costes derivados de los incendios en porcentaje al PIB de cada una de las naciones (Figura 4.5)

Economic-statistical evaluation of "costs" of fire (average for 2002-2004 years)

Экономико-статистические оценки «стоимости» пожаров (средние за 2002-2004 гг.)

Wirtschaftlich-statistische Einschaetzung der "Kosten" der Braende (Mittl. fuer 2002-2004)

N	Country	Cost in portion of GDP (%)					$\sum_{i=1}^{5} C_i$	Expenditure / Losses (C3 + C4 + C5)/ (C1+C2)
		Direct losses	Indirect losses	Cost of fire service	Fire protection in buildings	Fire insurance		
		C_1	C_2	C_3	C_4	C_5		
	Страна	Стоимость в долях ВНП (%)					$\sum_{i=1}^{5} C_i$	Затраты/ Потери (C3 + C4 + C5)/ (C1+C2)
		Прямой ущерб	Косвен. ущерб	Содержание пожарной охраны	ППЗ зданий	Страхование		
		C_1	C_2	C_3	C_4	C_5		
	Staat	Kosten in BSP-Anteilen (%)					$\sum_{i=1}^{5} C_i$	Ausgaben / Verluste (C3 + C4 + C5)/ (C1+C2)
		Direkter Schaden	Indirekter Schaden	Unterhalt Feuerwehren	VB in Gebaeuden	Feuerversicherung		
		C_1	C_2	C_3	C_4	C_5		
1	Czechia	0,10	-	-	0,18	-	-	-
2	Denmark	0,20	-	0,08	0,52	0,06	0,87*	3,2
3	Finland	0,15	0,008	0,22	-	0,03	0,66*	3,1
4	France	0,19	0,013	-	0,16	0,08	0,60*	2,0
5	Germany	0,16	0,012	-	-	0,06	-	-
6	Italy	0,18	-	-	0,34	0,04	-	-
7	Japan	0,10	0,021	0,34	0,15	0,09	0,70	4,8
8	New Zealand	0,11	0,007	0,15	0,18	0,08	0,53	3,5
9	Norway	0,25	0,002	0,11	0,36	0,11	0,83	2,3
10	Poland	0,07	-	0,18	-	-	-	-
11	Singapore	0,07	-	0,04	0,27	0,03	0,42*	4,3
12	Slovenia	0,07		0,05	0,18	0,06	0,31*	3,1
13	Sweden	0,17	0,005	0,15	0,16	0,05	0,54	2,1
14	UK	0,13	0,009	0,21	0,21	0,09	0,65	3,7
15	USA	0,10	0,007	0,25	0,35	0,13	0,84	6,8
Avrg./Сред./Mittl.		**0,14**	**0,009**	**0,16**	**0,25**	**0,07**	**0,63**	**3,2**

* - Estimation under average meaning Ci / Оценка при среднем значении Ci /

Data for this table are taken from the annual report of World Fire Statistics Center

http://www.genevaassociation.org/Affiliated_Organizations/WFSC.aspx

Figura 4.5: Coste derivados de los fuegos en % del PIB por países

La tabla anterior recoge datos para el Coste del Servicio antiincendios (C3) y para el coste en contratación de Seguros antiincendios (C5), que no tendremos en cuenta en nuestro estudio. Nos centraremos en las pérdidas directas (C1) e indirectas (C2) causadas por fuego, así como en los costes asociados a la protección antiincendios en edificios (C4). Estos últimos datos son los que están realmente relacionados, tanto con la prevención como con las pérdidas producidas por la amenaza Fuego. Después de estudiarlos en detalle, hemos decidido excluir los valores correspondientes a Noruega, ya que se trata de un caso aislado. A pesar de ser una de las naciones con mayor inversión en protección antiincendios presenta las mayores pérdidas directas.

Procedemos por tanto a cruzar los valores (C4,(C1+C2)) para representarlos en forma de gráfica.

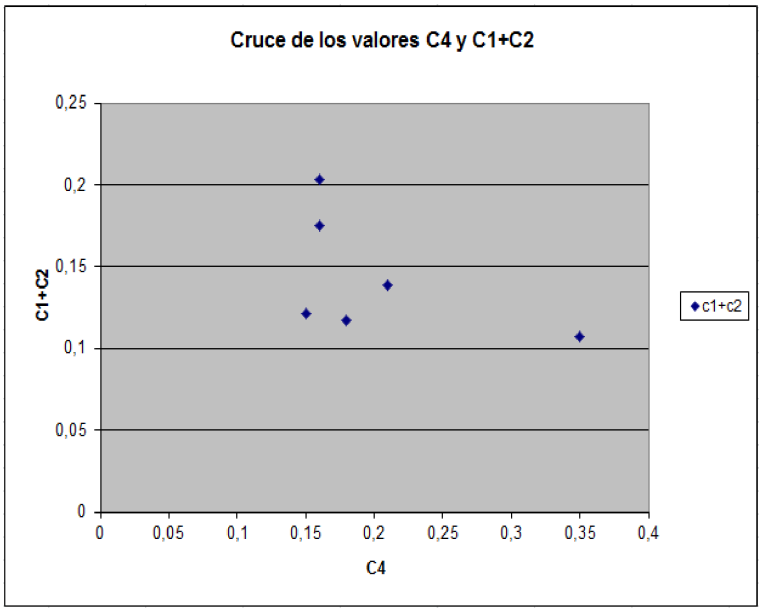


Figura 4.6: Cruce de los valores de C4 frente a C1+C2

En la figura 4.7 observamos que se consigue un ajuste razonable obteniendo la fórmula $y=a+bx$, donde x será nuestra variable de inversión en seguridad e y será el gasto total ocasionado. Por tanto, si decidimos invertir x en seguridad esperamos alcanzar un coste total de $a+bx$ para la amenaza Fuego. Si invertimos 0, tenemos a, que sería el coste de las pérdidas totales frente a un fuego sin ningún tipo de salvaguarda.

A través de la fórmula de regresión **lm(C1+C2 ~ C4)** estimamos los valores

$$a = 0{,}1964$$
$$b = -0{,}2617$$

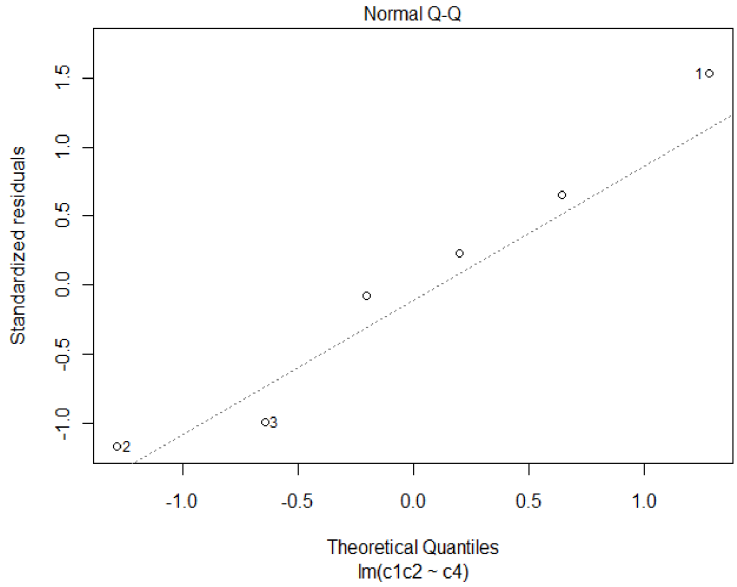


Figura 4.7: Gráfica representativa de la relación entre la inversión en la prevención de incendios y los costes derivados de las pérdidas que producen.

Con lo detallado anteriormente, tenemos todos los datos relativos a la probabilidad, duración y coste para la amenaza Fuego.

Cortes Eléctricos

A continuación consideramos la amenaza Corte Eléctrico. Para ello tenemos antes que familiarizarnos con los diferentes conceptos de medida que trataremos (CAIDI, SAIDI, SAIFI). No existe un método oficial para cálcular los índices de médida en cuanto a cortes eléctricos. El único requerimiento que se está utilizando actualmente es usar las mismas normas de medida cada año para poder compararlos entre sí. Esta información se publica periódicamente en una serie de informes, los cuales recopilan los datos reales obtenidos en diferentes categorías según el tipo de incidencia. De todas estas categorías se excluyen los datos relativos a cortes eléctricos causados por fenómenos naturales como terremotos, tormentas violentas o cualquier otro desastre ante el cual un sistema eléctrico es imposible que resista. También se excluyen los datos referentes a cortes planificados.

Los tipos de medida utilizados en este tipo de informes, y en los que nos hemos basado en este estudio son:

SAIFI (System Average Interruption Frecuency Index): Medida de interrupciones por cliente al año.

$$SAIFI = \frac{(Total\ de\ Interrupciones\ por\ cliente)}{(Total\ de\ clientes)}$$

SAIDI (System Average Interruption Duration Index): Medida del tiempo de la interrupción por cliente, si todos los clientes la han sufrido al mismo tiempo (horas por año).

$$SAIDI = \frac{(Suma\ de\ la\ duracion\ de\ todas\ las\ interrupciones)}{(Total\ de\ clientes)}$$

CAIDI (Customer Average Interruption Duration Index): Media de la duración de las interrupciones por cliente (horas por interrupción).

$$CAIDI = \frac{(Suma\ de\ las\ duraciones\ de\ todas\ las\ interrupciones)}{(Total\ de\ interrupciones)} = \frac{SAIDI}{SAIFI}$$

A continuación, se mostrarán unos gráficos dónde se podrá observar más en detalle cada uno de estos índices. En la figura 4.8 queda representado los índices SAIDI, SAIFI y CAIDI en el condado de *Los Álamos, Estados Unidos* (2010 SAIDI Report, 2010) durante los 12 meses previos a Julio de 2010.

Twelve Month History	JULY 2010	
Total # Accounts	8850	
Total # Interruptions	63	
Sum Customer Interruption Durations	17038:49:00	hours:min:sec
# Customers Interrupted	12321	
SAIFI(APPA AVG. = 1.0)	1.39	int./cust.
SAIDI (APPA AVG. = 1:00)	1:55	hours:min
CAIDI	1:22	hours:min/INT
ASAI	99.9991%	% available

Figura 4.8: Distribución de Cortes Electricos en el condado de Los Álamos (Julio 2009 - Julio 2010)

En la próxima gráfica observamos un histórico de los valores del índice SAIDI para cada mes desde Noviembre del año 2005, viendo así la evolución del mismo en los últimos años.

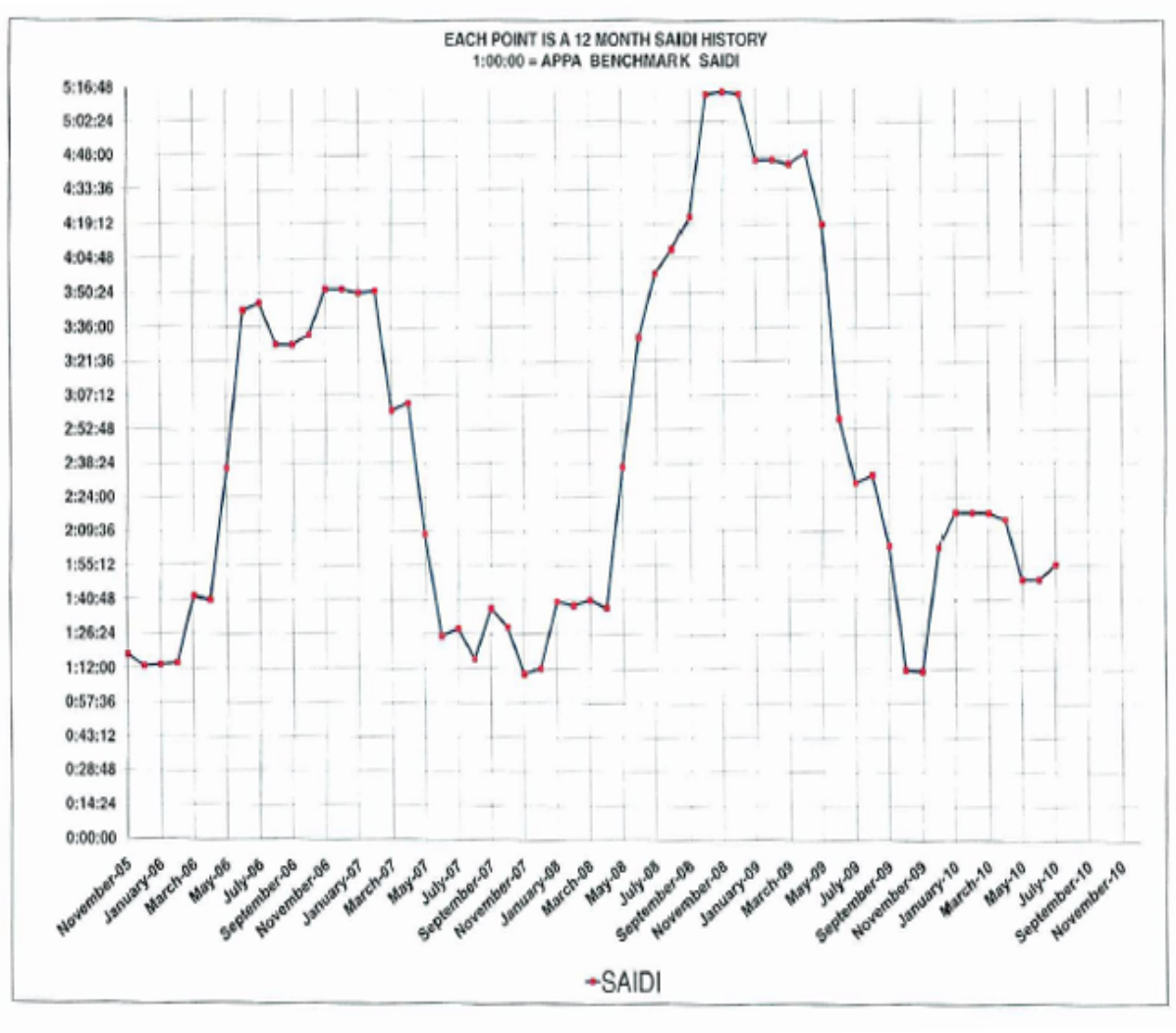


Figura 4.9: Evolución del índice SAIDI

Los índices representados en la figura 4.9 se han obtenido a partir del siguiente informe que refleja todas las incidencias por Corte Eléctrico en el condado de Los Álamos durante los 12 meses previos a Julio de 2010, incluyendo este último.

Date	Call Rcd.	Circuit	Cause	Start Time	End Time	Duration	Customers Affected (Meters)	Combined Customer Outage Durations	Total Outage H:M:S	Running SAIDI
8/2/2009	Utilities	14	HUMAN	14:25	14:28	0:03	800	40:00:00	40:00:00	0:00:16
8/2/2009	Utilities	14	HUMAN	14:25	19:25	5:00	210	1050:00:00	1090:00:00	0:07:23
8/3/2009	Utilities	14	URD Failure	10:30	17:00	6:30	140	910:00:00	2000:00:00	0:13:34
8/24/2009	Utilities	14	URD Failure	14:30	15:30	1:00	13	13:00:00	2013:00:00	0:13:39
8/24/2009	Utilities	14	URD Failure	14:30	17:30	3:00	10	30:00:00	2043:00:00	0:13:51
8/29/2009	Utilities	13	Unknown	14:00	15:50	1:50	10	18:20:00	2061:20:00	0:13:59
8/29/2009	Utilities	16	Weather	16:25	16:45	0:20	15	5:00:00	2066:20:00	0:14:01
8/31/2009	Utilities	14	URD Failure	15:00	17:30	2:30	1	2:30:00	2068:50:00	0:14:02
9/6/2009	LAPD	WR1	Weather	18:00	22:30	4:30	1	4:30:00	2073:20:00	0:14:03
9/6/2009	LAPD	15	Weather	18:30	19:30	1:00	5	5:00:00	2078:20:00	0:14:05
9/6/2009	LAPD	16	Weather	19:30	21:00	1:30	10	15:00:00	2093:20:00	0:14:12
9/7/2009	LAPD	15	Weather	7:00	7:30	0:30	8	4:00:00	2097:20:00	0:14:13
9/7/2009	LAPD	15	Weather	8:00	9:30	1:30	2	3:00:00	2100:20:00	0:14:14
9/7/2009	LAPD	16	Weather	15:30	16:15	0:45	1	0:45:00	2101:05:00	0:14:15
9/14/2009	Utilities	16	Weather	15:08	15:35	0:27	1700	765:00:00	2866:05:00	0:19:26
9/17/2009	Dispatch	WR2	Weather	18:51	20:00	1:09	1	1:09:00	2867:14:00	0:19:26
9/22/2009	Utilities	14	URD Failure	16:45	18:30	1:45	4	7:00:00	2874:14:00	0:19:29
9/22/2009	Utilities	14	URD Failure	16:45	19:01	2:16	4	9:04:00	2883:18:00	0:19:33
9/30/2009	Dispatch	13	Tree	17:50	21:12	3:22	5	16:50:00	2900:08:00	0:19:40
10/2/2009	Dispatch	14	URD Failure	15:30	18:30	3:00	3	9:00:00	2909:08:00	0:19:43
10/3/2009	LAPD	EA4	OH Failure	13:12	14:53	1:41	2	3:22:00	2912:30:00	0:19:45
10/20/2009	Dispatch	15	Weather	20:31	20:40	0:09	1498	224:42:00	3137:12:00	0:21:16
10/20/2009	Dispatch	WR1	OH Failure	19:10	20:17	1:07	1	1:07:00	3138:19:00	0:21:17
11/4/2009	Utilities	14	URD Failure	14:19	14:24	0:05	549	45:45:00	3184:04:00	0:21:35
11/12/2009	Utilities	14	URD Failure	10:00	14:30	4:30	2	9:00:00	3193:04:00	0:21:39
11/26/2009	Dispatch	14	Animal	2:47	7:20	4:33	5	22:45:00	3215:49:00	0:21:48
12/8/2009	Dispatch	16	Weather	5:07	8:00	2:53	1050	3027:30:00	6243:19:00	0:42:20
12/8/2009	Dispatch	16	Weather	5:07	8:30	3:23	679	2297:17:00	8540:36:00	0:57:54
12/8/2009	Dispatch	Royal Crest	Weather	4:30	9:30	5:00	175	875:00:00	9415:36:00	1:03:50
12/8/2009	Dispatch	13	Weather	8:00	10:00	2:00	10	20:00:00	9435:36:00	1:03:50
12/8/2009	Dispatch	14	Weather	2:30	3:30	1:00	8	8:00:00	9443:36:00	1:04:01
12/9/2009	Dispatch	16	OH Failure	1:00	3:15	2:15	5	11:15:00	9454:51:00	1:04:06
12/9/2009	Dispatch	15	OH Failure	1:00	3:15	2:15	5	11:15:00	9466:06:00	1:04:11
12/11/2009	Utilities	16	Animal	9:41	10:14	0:33	679	373:27:00	9839:33:00	1:06:43
12/11/2009	Utilities	16	Animal	9:41	11:00	1:19	1050	1382:30:00	11222:03:00	1:16:05

Date	Call Rcd.	Circuit	Cause	Start Time	End Time	Duration	Customers Affected (Meters)	Combined Customer Outage Durations	Total Outage H:M:S	Running SAIDI
1/9/2010	Dispatch	13	URD Failure	2:27	4:30	2:03	950	1947:30:00	13169:33:00	1:29:17
1/9/2010	Dispatch	14	URD Failure	2:38	2:43	0:05	550	45:50:00	13215:23:00	1:29:36
2/4/2010	Dispatch	13	Weather	9:28	9:45	0:17	8	2:16:00	13217:39:00	1:29:37
2/25/2010	Dispatch	WR1	URD Failure	19:00	21:20	2:20	2	4:40:00	13222:19:00	1:29:39
2/27/2010	Dispatch	16	URD Failure	15:30	16:35	1:05	2	2:10:00	13224:29:00	1:29:39
3/16/2010	Dispatch	16	Unknown	17:00	21:30	4:30	4	18:00:00	13242:29:00	1:29:47
3/18/2010	Dispatch	15	HUMAN	15:30	17:00	1:30	4	6:00:00	13248:29:00	1:29:49
3/22/2010	Dispatch	15	Unknown	12:00	14:00	2:00	6	12:00:00	13260:29:00	1:29:54
4/22/2010	Dispatch	18	LANL LINE	5:30	6:20	0:50	25	20:50:00	13281:19:00	1:30:03
4/22/2010	Dispatch	14	URD Failure	11:30	14:00	2:30	51	127:30:00	13408:49:00	1:30:54
4/22/2010	Dispatch	14	URD Failure	11:30	15:45	4:15	31	131:45:00	13540:34:00	1:31:48
5/8/2010	Dispatch	16	URD Failure	2:00	6:30	4:30	45	202:30:00	13743:04:00	1:33:10
5/9/2010	Dispatch	14	URD Failure	14:00	17:30	3:30	42	147:00:00	13890:04:00	1:34:10
5/9/2010	Dispatch	14	URD Failure	8:30	17:30	9:00	34	306:00:00	14196:04:00	1:36:15
6/2/2010	Dispatch	16	URD Failure	2:00	3:10	1:10	8	9:20:00	14205:24:00	1:36:18
6/2/2010	Dispatch	16	URD Failure	2:00	3:30	1:30	48	72:00:00	14277:24:00	1:36:48
6/15/2010	Utilities	WR2	URD Failure	8:35	9:55	1:20	17	22:40:00	14300:04:00	1:36:57
6/27/2010	Dispatch	15	OH Failure	11:30	17:25	5:55	10	59:10:00	14359:14:00	1:37:21
7/4/2010	Dispatch	14	URD Failure	6:00	10:30	4:30	4	18:00:00	14377:14:00	1:37:28
7/3/2010	Dispatch	16	Weather	16:00	21:30	5:30	5	27:30:00	14404:44:00	1:37:40
7/8/2010	Dispatch	WR2	URD Failure	4:00	8:30	4:30	20	90:00:00	14494:44:00	1:38:16
7/15/2010	Dispatch	WR2	URD Failure	5:00	6:30	1:30	20	30:00:00	14524:44:00	1:38:28
7/16/2010	Dispatch	16	URD Failure	14:00	17:00	3:00	115	345:00:00	14869:44:00	1:40:49
7/16/2010	Dispatch	16	URD Failure	19:00	21:00	2:00	8	16:00:00	14885:44:00	1:40:55
7/21/2010	Dispatch	13	Weather	21:30	22:30	1:00	16	16:00:00	14901:44:00	1:41:02
7/22/2010	Dispatch	13	Weather	5:45	9:00	3:15	40	130:00:00	15031:44:00	1:41:55
7/22/2010	Dispatch	13	Weather	20:00	21:00	1:00	1480	1480:00:00	16511:44:00	1:51:57
7/30/2010	Dispatch	16	URD Failure	16:55	21:30	4:35	115	527:05:00	17038:49:00	1:55:31

Figura 4.10: Datos de incidencias por Corte Eléctrico en el condado de Los Álamos, Estados Unidos.

Basándonos en los datos mostrados en la tabla anterior, y en los datos recogidos en los mismos informes de Marzo, Abril, Mayo y Junio de 2010, procedemos, al igual que hicimos con la amenaza Fuego, a estimar la **probabilidad de ocurrencia de un Corte Eléctrico en un año.**

Partimos de una distribución a priori:

$$\beta(1,1)$$

Teniendo en cuenta las observaciones de las que disponemos para el mes de Marzo de 2010, tenemos la siguiente distribución a posteriori:

$$\beta(1+x, 1+n-x) -> \beta(1+64, 1+8850-64)$$

donde x representa el número de cortes eléctricos sufridos y n el número de clientes existentes.

Añadiendo a estos datos los recogidos para los meses posteriores del mismo año, obtenemos las siguientes distribuciones a posteriori:

- Abril

$$\beta(1+x_1+x_2, 1+(n_1-x_1)+(n_2-x_2)) -> \beta(1+64+60, 1+(8850-64)+(8850-60))$$

- Mayo

$$\beta(1+x_1+x_2+x_3, 1+(n_1-x_1)+(n_2-x_2)+(n_3-x_3)) ->$$
$$\beta(1+64+60+58, 1+(8850-64)+(8850-60)+(8850-58))$$

- Junio

$$\beta(1+x_1+x_2+x_3+x_4, 1+(n_1-x_1)+(n_2-x_2)+(n_3-x_3)+(n_4-x_4)) ->$$
$$\beta(1+64+60+58+58, 1+(8850-64)+(8850-60)+(8850-58)+(8850-58))$$

- Julio

$$\beta(1+x_1+x_2+x_3+x_4+x_5, 1+(n_1-x_1)+(n_2-x_2)+(n_3-x_3)+(n_4-x_4)+(n_5-x_5)) ->$$
$$\beta(1+64+60+58+58+63, 1+(8850-64)+(8850-60)+(8850-58)+(8850-58)+(8850-63))$$

Resumimos esta última distribución usando la siguiente estimación de probabilidad de un corte eléctrico en un año, en el Condado de Los Álamos.

$$\widehat{p} = \frac{1+x_1+x_2+x_3+x_4+x_5}{2+n_1+n_2+n_3+n_4+n_5} = \mathbf{0,006869746},$$

De la misma manera que ocurría con la amenaza Fuego, concluimos que el número de Cortes Eléctricos por año sigue una distribucion de Poisson $e^{-\lambda}\frac{\lambda^k}{k!}$ donde λ se deduce de la probabilidad de que haya cero Cortes Eléctricos:

$$p(0) = 1 - \widehat{p} = 0,9931303 = e^{-\lambda}\frac{\lambda^0}{0!} = e^{-\lambda}$$

Así, despejando, obtenemos $\widehat{\lambda} \simeq 0{,}006$. La probabilidad de k cortes eléctricos sería entonces:

$$\text{P(k cortes eléctricos)} = e^{-0,006}(\frac{0,006^k}{k!})$$

Corte Eléctrico	
k	*Probabilidad*
0	$0,9931$
1	$0,0069$
2	$4,72E-05$
3	$1,63E-07$
4	$3,74E-10$
5	$6,44E-13$
...	...

Tabla 4.2: Tabla de probabilidad para la amenaza Corte Eléctrico

A continuación pasamos a evaluar lo referente a la duración de los Cortes Eléctricos. Esta estimación nos servirá de base para el cálculo de los costes derivados de la prevención de los Cortes Eléctricos. Para realizar este estudio, volvemos a recurrir a los datos reflejados en la tabla 4.10, obteniendo el siguiente histograma.

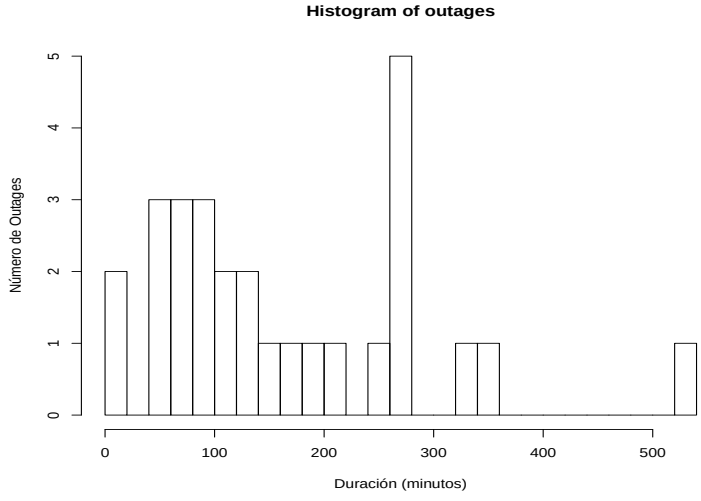


Figura 4.11: Histograma Cortes Eléctricos

En el histograma anterior podemos observar que la mayoría de Cortes Eléctricos tienen una duración menor a cinco horas. A partir de estos datos, modelizamos mediante la distribución Gamma(k,θ). Por tanto, de igual manera que hemos realizado anteriormente con la amenaza Fuegos, estimamos por medio del Método de Momentos la distribución de la duración de un Corte Eléctrico.

La media de Gamma (k,θ) es:

$$k\theta = m$$

La varianza es:

$$k\theta^2 = \sigma^2$$

de donde obtenemos $\theta = \frac{\sigma^2}{m}$ y $k = \frac{m^2}{\sigma^2}$, resultando los siguientes valores

$$\text{k} = 1{,}926359$$
$$\theta = 88,06397$$

para m = 169,6429 y σ^2 = 14939,42

A continuación pasamos a evaluar los costes derivados de la posible ocurrencia de un corte eléctrico. Para realizar este cálculo vamos a utilizar como referencia un estudio realizado por la Universidad de Berkeley (A Simple Way to Estimate the Cost of Downtime, 2002). Dicho estudio analiza de manera detallada las pérdidas que sufrirían distintos tipos de entidades a causa de una interrupción del servicio. De las distintas instituciones objeto del estudio, hemos decidido centrarnos en la empresa Amazon.com, actualizando los datos financieros del año 2002 a los obtenidos en el año 2010, ya que Amazon.com ofrece estos datos de manera pública (Annual Report, 2010).

Partimos de que la empresa Amazon.com es un negocio *on-line*, por lo que presta servicio las 24 horas del día (24x7). Además, el informe también cosidera que la jornada laboral es de 50 horas semanales (10x5).

Datos disponibles:

- Ingresos Netos Anuales: 34.204.000.000 $
- Ingresos Netos/hora: 34.204.000.000 / 24x7x52 = 3.915.293 $

El estudio realizado por Berkeley supone que la parada del servicio afectaría al 90 % de los ingresos: 3.915.293 x 0,9 = **3.523.764 $**, que sería la estimación de la pérdida de ingresos por hora de interrupción de servicio.

Los resultados ofrecidos por Amazon.com no tienen en cuenta los salarios de los empleados, por lo que pasamos a analizarlos a continuación.

- Número de empleados: 33.700
- Salario medio anual: 85.000 $
- Costes anuales en salarios: 85.000 x 33.700 = 2.864.500.000 $
- Costes por semana en salarios: 2.864.500.000 / 52 = 55.086.538 $
- Costes por hora en salarios: 55.086.538 / 50 = 1.101.730 $
- El estudio supone que la parada del servicio afectaría a un 80 % de los empleados: 1.101.730 x 0,8 = 881.384 $

Costes derivados de la no productividad de los empleados afectados por la interrupción del servicio: **881.384 $**

Para concluir, sumamos las pérdidas en ingresos más los costes en salarios obteniendo la cifra total de los **costes por hora de servicio interrumpido, 4.405.148 $.**

Así pues, hemos recogido todos los datos que se refieren a la probabilidad, duración y coste para la amenaza Corte Eléctrico.

Ataques por Virus Informáticos

A continuación trataremos la amenaza Virus Informáticos. Toda la información utilizada en esta sección proviene del grupo Shadowserver Foundation, un grupo regulador de profesionales en seguridad que ofrece un servicio voluntario reuniendo, dando seguimiento y reportando malware, ataques y fraude electrónico. Su misión principal es la mejora de la seguridad en Internet aumentando la concienciación ante la presencia de servicios comprometidos, atacantes maliciosos y la expansión del malware.

La fundación realiza un informe estadístico con las intercepciones efectuadas por un número bastante amplio de los actuales antivirus presentes en el mercado. Tiene un registro de estadísticas que va desde el diario hasta el anual, pasando por varias franjas temporales. Nosotros nos basaremos, en un primer paso, en el informe semanal, el cual ofrece un conjunto de datos amplio y actual que nos será de gran utilidad a la hora de realizar nuestro estudio.

Como primer ejemplo, seleccionaremos el antivirus con mejor resultado en los citados informes semanales. Esto, a priori, sería lo ideal, pero se tiene que tener en cuenta el presupuesto del que disponemos y el precio que tiene contratar ese antivirus. Por tanto, asumiendo que la empresa que provee el mejor antivirus, será también la más cara, para el siguiente paso (datos anuales) estudiaremos los datos de un antivirus "de mitad de tabla"suponiendo que tenemos un presupuesto ajustado que no nos permite seleccionar siempre el mejor.

Así pues, al igual que hemos realizado para el resto de amenazas, a partir de los datos reflejados en el informe, hallaremos la probabilidad de que **en un año, la institución bajo estudio se vea afectada por un ataque de virus**. Una vez más, usaremos la distribución a priori:

$$\beta(1,1)$$

Basándonos en el informe semanal, se tiene registrado que en la semana 0 tenemos la siguiente distribución a posteriori:

$$\beta(1+x, 1+n-x) -> \beta(1+55, 1+303100-55)$$

donde x representa el número de virus no detectados por el antivirus y n el número total de virus en activo esa semana.

Una vez registrados los datos para la semana anterior, obtendríamos una distribución a posteriori para dos semanas como sigue:

$$\beta(1+x_1+x_2, 1+(n_1-x_1)+(n_2-x_2)) -> \beta(1+55+53, 1+(303100-55)+(230500-53)),$$

que resumimos usando

$$\widehat{p} = \frac{1+x_1+x_2}{2+n_1+n_2} \simeq \mathbf{0,0002},$$

que es la probabilidad de que en un año, un ataque de virus tenga éxito infectando el sistema.

Como hemos explicado anteriormente, estos datos reflejan los resultados del mejor antivirus en las dos semanas últimas semanas. Si contamos con que nuestro presupuesto no es capaz de alcanzar el precio de este antivirus, pero estamos dispuestos a invertir lo suficiente en uno que sea capaz de responder de manera eficaz ante los posibles ataques, recurrimos a las estadísticas anuales que ofrece el grupo ShadowServer (figura 4.12) para las principales compañías Antivirus a nivel mundial y elegimos la empresa que provee el antivirus que está posicionado en la mitad de la tabla, es decir, AVG7 con un 78,66 % de virus detectados.

vendor	detected	total	percent
AntiVir	24,308,342	26,598,228	91.39%
DrWeb	23,041,081	26,598,228	86.63%
Kaspersky	22,886,179	26,598,228	86.04%
F-Secure	22,794,938	26,598,228	85.70%
VirusBuster	22,608,641	26,598,228	85.00%
VBA32	22,044,005	26,598,228	82.88%
Sophos	22,027,039	26,598,228	82.81%
Clam	21,120,442	26,598,228	79.41%
AVG7	20,920,036	26,597,128	78.66%
QuickHeal	20,869,573	26,598,228	78.46%
NOD32	20,706,093	26,598,228	77.85%
Ikarus	20,700,631	26,598,228	77.83%
Avast-Commercial	20,439,249	26,598,028	76.84%
TrendMicro	19,584,155	26,598,228	73.63%
F-Prot6	17,290,652	26,598,228	65.01%
McAfee	16,051,884	26,598,228	60.35%
Panda	15,440,382	26,598,228	58.05%
Vexira	12,766,179	26,598,228	48.00%
BitDefender	11,889,510	26,598,228	44.70%

Figura 4.12: Estadísticas anuales de infección por Virus

Teniendo en cuenta nuestra elección, a partir de los datos mostrados en la tabla anterior, obtenemos que **la probabilidad de éxito de un ataque por Virus en un año** sería:

$$\widehat{p} = 1 - p(0) = 1 - 0,7866 = \mathbf{0,2134}$$

Estudiando y comparando los resultados obtenidos según las estadísticas semanales y anuales, se llega a la conclusión de que los datos semanales no sólo son demasiado optimistas sino que, quizás, se quedan lejos de representar fielmente la actividad de los virus en un año completo. Es por esto, que nos quedamos con la probabilidad obtenida a partir del informe anual.

Por tanto, una vez tomada esta decisión, concluimos que el número de infecciones por año sigue una distribucion de Poisson $e^{-\lambda}\frac{\lambda^k}{k!}$ donde λ se deduce de la probabilidad de que haya cero infecciones:

$$p(0) = 1 - \widehat{p} = 0,7866 = e^{-\lambda}\frac{\lambda^0}{0!} = e^{-\lambda}$$

con lo que despejamos $\lambda \simeq 0,24$ y, a partir de él, podemos completar la tabla de probabilidades para Virus.

La distribución de Poisson correspondiente quedaría de la siguiente manera:

$$\text{P(k ataques)} \simeq e^{-0,24}(\frac{0,24^k}{k!})$$

Virus	
k	*Probabilidad*
0	$0,7866$
1	$0,2134$
2	$0,04532153$
3	$0,00543939$
4	$0,00043522$
5	$2,61E-05$
...	...

Tabla 4.3: Tabla de probabilidad para la amenaza Virus

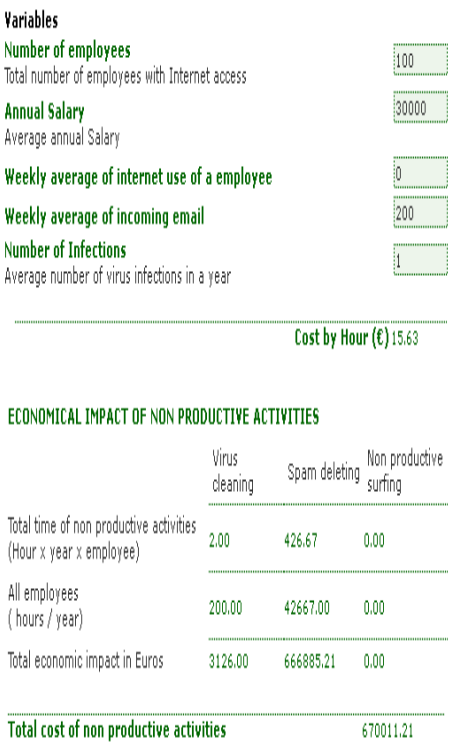
Con respecto a la duración de una caída de servicio debida al ataque de un virus informático sin ningún tipo de defensa, la asociación ICSA labs (de las siglas en inglés Intenational Computer Security Association) recoge que el 36 % de las 300 organizaciones bajo estudio (*ICSA Labs Sixth Annual Computer Virus Prevalence Survey*, 2000), reportaron que sus servidores sufrieron una caída de una hora o menos, con una mediana de tiempo de caída de 21 horas. Sólo unas pocas experimentaron un mayor tiempo de recuperación superando las 1.000 horas, y más del 80 % de estas organizaciones reportaron que las consecuencias del ataque requieron 20 personas/dia o menos para la recuperación.

Una vez que hemos analizado las probabilidades y la duración de un ataque de virus, pasaremos a realizar el estudio de los costes derivados del mismo. Es importante ser conscientes de que el problema de un ataque de virus puede ser el tiempo que se tarde en detectar que un sistema ha sido infectado. Si la naturaleza del ataque no es la destrucción o la caída del sistema de manera inmediata, el usuario final puede que solamente perciba una pérdida de rendimiento o un comportamiento extraño del sistema.

Esta situación puede ser tolerada durante mucho tiempo asumiendo que puede tratarse de un deterioro o un normal comportamiento del sistema debido al paso del tiempo. Esto deriva en un aumento importante de los costes provocados por la pérdida de eficiencia y dilatación del tiempo de trabajo pero, a su vez, es una situación muy difícil de cuantificar respecto a los costes que provoca. Por tanto, en el estudio únicamente nos basaremos en los costes que se producen una vez detectada la infección.

Para ello, haremos uso de una de las muchas herramientas disponibles en la red que han sido desarrolladas por diferentes empresas de antivirus y protección. Estas herramientas realizan un cálculo preciso de los costes derivados de tareas no productivas según el tipo de empresa y su actividad. Nos centraremos principalmente en la herramienta que provee Ozono Security en su web (Visualization of costs, 2011) y cuyos resultados podemos observar en la figura 4.13.

Así, para un ejemplo de una empresa con 100 empleados, en la que se tiene una media salarial de 30.000 €, una media de 200 correos electrónicos entrantes y una infección anual, provocaría unos costes derivados de 670.011,21 €.



Variables

Number of employees Total number of employees with Internet access	100
Annual Salary Average annual Salary	30000
Weekly average of internet use of a employee	0
Weekly average of incoming email	200
Number of Infections Average number of virus infections in a year	1

Cost by Hour (€) 15.63

ECONOMICAL IMPACT OF NON PRODUCTIVE ACTIVITIES

	Virus cleaning	Spam deleting	Non productive surfing
Total time of non productive activities (Hour x year x employee)	2.00	426.67	0.00
All employees (hours / year)	200.00	42667.00	0.00
Total economic impact in Euros	3126.00	666885.21	0.00

Total cost of non productive activities 670011.21

Figura 4.13: Estadísticas anuales de infección por Virus

Con lo visto anteriormente, obtenemos todos los datos relacionados con la probabilidad, duración y coste para la amenaza Virus.

Ataques de Denegación de Servicio (DoS)

Por último, trataremos la amenaza Denegación de Servicio. Al igual que para la amenaza Virus, hemos utilizado como fuente la información provista por la Shadowserver Foundation. En este caso, los datos reportados en los informes hacen referencia a ataques por Denegación de Servicio Distribuidos o DDoS (del inglés Distributed Denial of Service) detectados por Shadowserver. Los informes disponibles reflejan esta información desde el año 2006 a nivel global.

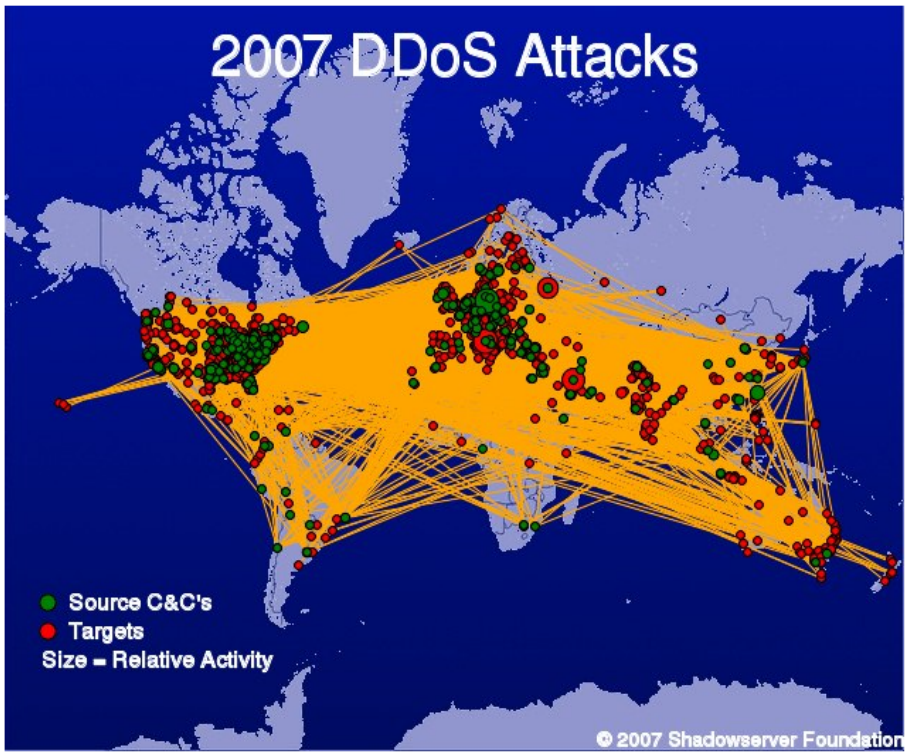


Figura 4.14: Representación de la distribución de los ataques DDoS durante el año 2007

Year	Unique C&C	Unique C&C ASN	Unique C&C Geo	Target Count	Unique Targets	Unique Target ASN	Unique Target Geo
2006	414	214	40	50650	25953	3079	133
2007	848	390	67	35566	15755	1633	107
2008	618	332	66	202678	21312	1870	117
2009	590	272	53	7058221	10991	1491	110
2010	430	157	41	1545208	13757	1697	106
2011	322	98	30	275459	5327	756	72

- **Unique C&C** - How many unique Command and Controls conducted DDoS attacks
- **Unique C&C ASN** - How many Unique ASN's did the Command and Control servers reside in that participated in DDoS attacks
- **Unique C&C Geo** - How many unique countries did the Command and Control servers reside in that participated in DDoS attacks
- **Target Count** - How many different targets were DDoS'ed
- **Unique Targets** - How many DDoS attacks occurred during that period
- **Unique Target ASN** - How many unique ASN's were affected by the DDoS's
- **Unique Target Geo** - How many unique countries were affected by the DDoS's

Figura 4.15: Número total de ataques DDoS

De los datos mostrados en la tabla anterior, nos centramos en los correspondientes a la columna *Unique Targets*, que hace referencia al número total de ataques DDoS ocurridos durante cada año, y en los datos mostrados en la columna *Target Count*, que alberga

el número total de objetivos afectados por ataques DDoS. Al igual que hicimos con las amenazas antoriores, nos basaremos en esta información para estimar la **probabilidad de ocurrencia de un ataque DDoS en un año**. En esta ocasión, gracias a que disponemos de datos históricos de 2006 a 2010, haremos una aproximación más precisa incluyéndolos todos en el cálculo. Partimos de la distribución a priori:

$$\beta(1,1)$$

Teniendo en cuenta las observaciones de las que disponemos para el año 2006, tenemos la siguiente distribución a posteriori:

$$\beta(1+x,1+n-x) -> \beta(1+25953,1+50650-25953)$$

donde x es el número de ataques por DDoS ocurridos en este periodo y n es el número total de objetivos que han recibido un ataque por DDoS.
Repitiendo el mismo método, concluimos para el año 2010

$$\beta(1+x_1+x_2+x_3+x_4+x_5, 1+(n_1-x_1)+(n_2-x_2)+(n_3-x_3)+(n_4-x_4)+(n_5-x_5)) ->$$
$$\beta(1+25953+15755+21312+10991+13757, 1+(50650-25953)+(35566-15755)+$$
$$(202678-21312)+(7058221-10991)+(1545208-13757))$$

De esta última, estimamos

$$\widehat{p} = \frac{1+x_1+x_2+x_3+x_4+x_5}{2+n_1+n_2+n_3+n_4+n_5} \simeq \mathbf{0,00987},$$

como la probabilidad de que, en un año, una institución reciba un ataque por DDoS.

Para completar la información, vamos a recurrir al artículo *The Trends And Changing Landscape Of DDoS Threats And Protection*, publicado por Forrester Consulting para VeriSign en Marzo de 2009. Para dicho artículo se utilizaron 400 fuentes diferentes con base tanto en Estados Unidos como en Europa, con el objetivo de obtener una imagen global de la situación actual en la prevención de ataques por Denegación de Servicio Distribuidos.

En lo referente a la probabilidad de verse afectado por un ataque DDoS, podemos extraer dicha información de este informe a partir de la siguiente figura.

Figura 4.16: Instituciones afectadas, o no, por ataques DDoS durante 12 meses

El 74 % de los encuestados recibieron al menos un ataque por DDoS durante los 12 meses del estudio, pero sólamente un 31 % del total vieron interrumpido su servicio a causa del ataque. Por lo tanto, deducimos que la **probabilidad de verse afectado por algún ataque DDoS en un año** según este artículo sería:

$$\widehat{p} = 0,31$$

Si comparamos este último dato (0,31) frente al obtenido anteriormente con el histórico de datos de Shadowserver (0,009870197) observamos que existe una gran diferencia. Analizando que los datos de Forrester se basan en un solo año y en un grupo cerrado de empresas y que, por el contrario, la información recogida por Shadowserver abarca un período de cinco años hasta 2010 sobre un número mayor de empresas, nos quedaremos con éste último como dato definitivo para nuestro estudio.

Una vez tomada esta decisión, concluimos que el número de ataques por denegación de servicio al año sigue una distribucion de Poisson $e^{-\lambda}\frac{\lambda^k}{k!}$ donde λ se deduce de la probabilidad de que haya cero ataques:

$$p(0) = 1 - \widehat{p} = 0,990129803 = e^{-\lambda}$$

con lo que despejamos $\lambda = 0{,}00991923$. A partir de este valor podemos completar la tabla de probabilidades para DoS. La distribución de Poisson quedaría de la siguiente manera:

$$\text{P(k ataques DDoS)} = e^{-0,00991923}(\frac{0,00991923^k}{k!})$$

DDoS	
k	*Probabilidad*
0	$0,9901$
1	$0,009870197$
2	$9,74E-05$
3	$4,83E-07$
4	$1,60E-09$
5	$3,96E-12$
...	...

Tabla 4.4: Tabla de probabilidad para la amenaza DoS

Pasamos ahora evaluar la posible duración de un ataque por Denegación de Servicio. En este caso, hemos seleccionado dos fuentes de información diferentes, pero que vienen a confirmar una misma conclusión.

En primer lugar, volvemos a trabajar sobre el artículo *The Trends And Changing Landscape Of DDoS Threats And Protection*, publicado por Forrester Consulting para VeriSign, el cual nos muestra esta información en la figura 4.17. En ella se muestran la distribución del tiempo de recuperación entre los 124 encuestados que sufrieron pérdida de servicios debido a un ataque por DDoS del total de 400 entidades que se sometieron al estudio durante 12 meses.

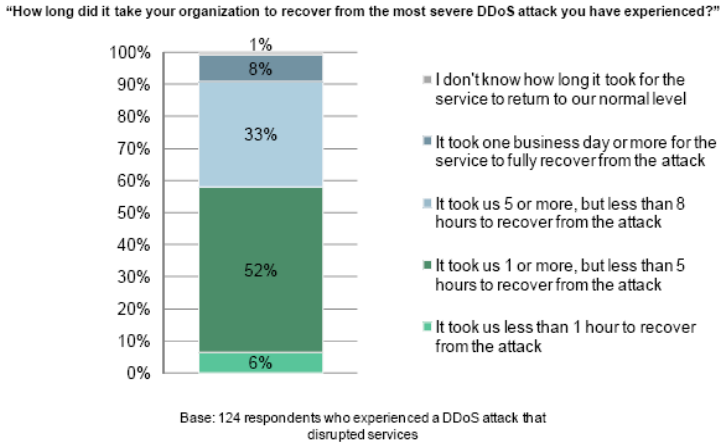


Figura 4.17: Tiempo de recuperación del Servicio tras un ataque DDoS

En la imagen anterior queda reflejado cómo más del 50 % tardaron en recuperarse del ataque entre una y cinco horas. Este dato concuerda con el ofrecido por la empresa Arbor Networks, dedicada a la monitorización y seguridad en la red, en el artículo *The Internet goes to War* publicado en el año 2010.

Flooding DDoS Attack Statistics

Data is from 5,000 confirmed attacks in ATLAS data set between December 1, 2009 and December 1, 2010.

	Mbps	Pps	Hours
Median	34	33,519	0.8
Average	349	258,347	3.1
95th	1,055	703,438	10.7
max	22,000	12,354,606	114.6

Figura 4.18: Estadísticas de ataques DDoS, de Diciembre de 2009 a Diciembre de 2010

Este artículo utiliza como fuente 5.000 ataques confirmados durante los 12 meses previos a Diciembre de 2010. En la figura 4.18 podemos observar cómo el tiempo medio de recuperación del servicio tras un ataque resultó ser de 3,1 horas. Viendo que ambos datos, tanto los ofrecidos por Forrester Consulting como los ofrecidos por Arbor Networks, conducen a valores muy similares, utilizaremos el valor ofrecido por Arbor Networks. Por tanto, definimos que, para nuestro estudio, el tiempo medio de recuperación después de un ataque por DDoS será de 3,1 horas.

Por último, analizamos los costes producidos por una ataque por Denegación de Servicio. Al igual que hicimos en la sección de Cortes Eléctricos, vamos a hacer uso del estudio realizado en 2002 por la Universidad de Berkeley para realizar la estimación de los costes derivados de una interrupción del servicio. Los resultados obtenidos para la empresa Amazon.com ofrecían unos resultados de 4.405.148 $ por hora de interrupción de servicio. Sabiendo que la duración media de un ataque por Denegación de Servicio es de 3,1 horas, obtendríamos que, para la empresa Amazon.com un ataque por Denegación de Servicio podría suponer unos costes medios aproximados de **13.655.959 $.**

Finalizamos así la obtención de los datos para la probabilidad, duración y coste de la amenaza DDoS.

4.2. Resultados globales del estudio

Hacemos ahora una recopilación de los resultados obtenidos, comenzando por las probabilidades de aparición de cada una de las amenazas.

Fuego		**Corte Eléctrico**		**Virus**		**DDoS**	
Núm.	*Probabilidad*	*Núm.*	*Probabilidad*	*Núm.*	*Probabilidad*	*Núm.*	*Probabilidad*
0	$0,9786$	0	$0,9931$	0	$0,7866$	0	$0,9901$
1	$0,0214$	1	$0,0069$	1	$0,2134$	1	$0,009870197$
2	$0,000457942$	2	$4,72E-05$	2	$0,04532153$	2	$9,74E-05$
3	$4,95E-06$	3	$1,63E-07$	3	$0,005439386$	3	$4,83E-07$
4	$3,57E-08$	4	$3,74E-10$	4	$0,000435215$	4	$1,60E-09$
5	$1,93E-10$	5	$6,44E-13$	5	$2,61E-05$	5	$3,96E-12$
...	...	...	...	...	...	...	...

Tabla 4.5: Tabla de probabilidades para las distintas amenazas

En lo referente a la duración, tanto para la amenaza Fuego como para la amenaza Corte Eléctrico, ambas siguen una distribución $Gamma(k,\theta) = \frac{x^{k-1}exp(-\frac{x}{\theta})}{\Gamma(k)\theta^k}$, donde para la amenaza Fuego tendríamos los valores

$$\text{x} = \text{número de fuegos}$$
$$\text{k} = 0{,}0536224$$
$$\theta = 191,5311$$

y para la amenaza Corte Eléctrico

$$\text{x} = \text{número de cortes eléctricos}$$
$$\text{k} = 1{,}926359$$
$$\theta = 88,06397$$

En cuanto a la duración para las amenazas Virus y DoS, basándonos en los datos consultados durante el estudio, se concluye que en el caso de una infección por virus será de una hora o menos, mientras que en un ataque DoS la duración media será de 3,1 horas.

Finalizamos con los datos referentes a los costes derivados de cada una de las amenazas. Los producidos por la amenaza Fuego se calculan a partir de un informe que recoge los datos relativos a pérdidas directas, indirectas, y gastos en protección antiincendios en edificios, todo ello relativo al PIB de una selección de países.

Para las amenazas Corte Eléctrico y DoS, apoyándonos en un estudio realizado por la Universidad de Berkeley, calculamos los costes que dichas amenazas causarían por cada hora de interrupción del servicio.

Por último, en el caso de la amenaza Virus, los costes anuales se obtienen a través de una herramienta web, la cual hace uso de ciertos parámetros de entrada que definen el tipo de entidad y el número de ataques recibidos.

Reuniendo toda esta información, estaríamos en disposición de formular un problema continuo para el análisis y la gestión de riesgos TIC.

Capítulo 5

Conclusiones y trabajos futuros

Durante la elaboración de este trabajo hemos realizado un intenso estudio de las diferentes metodologías para la gestión y el análisis de riesgos TIC vigentes en la actualidad. Dichas metodologías aportan gran valor en ciertos campos como la catalogación de los activos, amenazas y salvaguardas a considerar en todo problema de análisis de riesgos. Por tanto, son un importante soporte sobre el cual los responsables de la toma de decisiones en este ámbito pueden sustentar sus políticas en seguridad. Aún así, creemos que es importante tener en cuenta el carácter dinámico que presenta este tipo de problemática y que, consideramos, no se trata con todo el rigor necesario en las metodologías en uso actualmente.

Uno de nuestros objetivos, por tanto, ha sido dotar de un enfoque eminentemente probabilístico al problema, aprovechando los puntos fuertes de las metodologías actuales. De esta manera, definiendo de manera minuciosa las interdependencias entre los distintos componentes y mediante el cálculo de utilidades, pretendemos dar una mayor robustez y exactitud al modelo propuesto. Otro punto a destacar en este modelo es la optimización de la inversión en el uso de salvaguardas, característica muy destacable y de gran utilidad teniendo en cuenta las habituales restricciones presupuestarias.

En última instancia, se ha intentado dar un enfoque realista al problema planteado con anterioridad. Para ello creamos un escenario basado en los datos reales recogidos en diversos informes y estudios disponibles públicamente, el cual nos aporta la base necesaria para la construcción de un modelo dinámico de gestión y análisis de riesgos TIC. Esto, a priori interesante, debe ser tomado con la cautela de saber que no se trata de datos centrados en un ejemplo concreto, sino que deben servir de base para poder realizar un estudio detallado de la entidad real donde se quiera realizar un análisis.

En referencia a los posibles trabajos futuros, proponemos trabajar en la elaboración de un modelo dinámico para la gestión de riesgos TIC con los resultados presentados en este proyecto. Una vez alcanzado este objetivo, podría plantearse la implementación de dicho modelo como aplicación informática, para lo cual podría utilizarse la herramienta *SMILE* (de las siglas en Inglés Structural Modeling, Inference, and Learning Engine), la cual permite la creación de modelos gráficos para su uso en problemas probabilísticos.

Bibliografía

[1] R Anderson. *Security Engineering*. Wiley, 2001.

[2] The Geneva Association. World fire statistics, information bulletin of the world fire statistics center. http://www.genevaassociation.org/PDF/WFSC/GA2010-FIRE26.pdf, 2010.

[3] R Clemen. *Making Hard Decisions: An Introduction to Decision Analysis*. Duxbury Press, 2007.

[4] European Commission. European commission proposal for a council framework decision on attacks against information systems. 2002.

[5] Forrester Consulting. The trends and changing landscape of ddos threats and protection. 2009. http://verisigninc.com/assets/whitepaper-ddos-threats-protection-forrester.pdf.

[6] International Association of Fire CTIF and Rescue Service. World fire statistics. http://www.ctif.org/Introduction,25, 2008.

[7] Ministerio de Administraciones Públicas. Metodología de análisis y gestión de riesgos de los sistemas de información. *MAGERIT versión 2*, 2006.

[8] Ayto. de Vitoria-Gasteiz. Memoria09, servicio de prevención y extinción de incendios. http://www.vitoria-gasteiz.org/wb021/http/contenidosEstaticos/adjuntos/31583.pdf, 2009.

[9] Ayto. de Vitoria-Gasteiz. Sistema de información de indicadores urbanos. http://www.vitoria-gasteiz.org, 2009.

[10] Shadow Server Foundation. Viruses. http://www.shadowserver.org/, 2011.

[11] Amazon.com Inc. Annual report. http://phx.corporate-ir.net/phoenix.zhtml?c=97664&p=irol-reportsother, 2010.

[12] Trend Micro Inc. The real cost of a virus outbreak. http://www.biznetvigator.com/chi/pdf/real_cost_of_virus_outbreak.pdf, 2002.

[13] G. Kunreuther, H.; Heal. Interdependent security. *Journal of Risk and Uncertainty*, 2-3, 2003.

[14] Decision Systems Laboratory. Smile (structural modeling, inference, and learning engine). http://genie.sis.pitt.edu/about.html.

[15] Arbor Networks. The internet goes to war. http://asert.arbornetworks.com/2010/12/the-internet-goes-to-war/, 2010.

[16] County of Los Alamos. 2010 saidi report. http://www.losalamosnm.us/utilities/Pages/ReliabilityandOutageReporting.aspx, 2010.

[17] Dave Patterson. A simple way to estimate the cost of downtime. *EECS Department; University of California, Berkeley*, 2002. http://roc.cs.berkeley.edu/talks/pdf/LISA.pdf.

[18] Ozono Security. Visualization of costs. http://www.ozonosecurity.com/en/recursos/costes.asp?, 2011.

[19] Hye-Kyung Chung Soon-Jae Lee. Building a framework to measure and minimize information risks. *The Information Management Journal*, 2008.

[20] La Enciclopedia Libre Wikipedia. Exponential smoothing. http://en.wikipedia.org/wiki/Exponential_smoothing, 2011.