UNIVERSIDAD CARLOS III DE MADRID

ESCUELA POLITÉCNICA SUPERIOR

INGENIERÍA DE TELECOMUNICACIÓN

Departamento de Estadística

PROYECTO FIN DE CARRERA

Plan de Control de Riesgos Operacionales en Telecomunicaciones

AUTOR: Carlos Junco Diez

TUTOR: José Ruiz-Canela López

TÍTULO: *Plan de Control de Riesgos Operacionales en Telelcomunicaciones.*

AUTOR: *Carlos Junco Diez*

TUTOR: *José Ruiz-Canela López*

La defensa del presente Proyecto Fin de Carrera se realizó el día 7 de Abril de 2011; siendo calificada por el siguiente tribunal:

PRESIDENTE: *Francisco Javier Prieto Fernández*

SECRETARIO: *Francisco Javier Nogales Martín*

VOCAL: *Ana García Armada*

Habiendo obtenido la siguiente calificación:

CALIFICACIÓN:

Presidente **Secretario** **Vocal**

A mis padres.

Risk comes from not knowing what you're doing.

Warren Buffett

Resumen

El presente documento describe el procedimiento seguido para la realización del Proyecto de Fin de Carrera del alumno Carlos Junco Diez y supone el último requisito academico para la obtención del título de Ingeniero Superior de Telecomunicación en la Universidad Carlos III de Madrid.

Ante la importancia en el sector empresarial, de prevenir situaciones críticas en el aspecto operacional, que puedan provocar cuantiosas pérdidas o incluso llevar a la quiebra a una empresa, surge la motivación original de este proyecto: desarrollar un Plan de Control del Riesgo Operacional en el sector de las telecomunicaciones.

Aunque existen distintos enfoques y métricas a la hora de determinar la eficacia de este tipo de plan, la rapidez de los procesos de actualización, dada una monitorización constante, y el número de amenazas que pueden ser detectadas y mitigadas son indicadores significativos de su efectividad. El primer paso de este proyecto ha sido realizar una introducción al concepto de Gestión de Riesgo Operacional, de forma abreviada llamado ORM (Operational Risk Management), posteriormente se ha procedido al desarrollo del plan de gestión del riesgo consistente en un modelo de cinco pasos: identificación, evaluación, análisis, implementación y supervisión. Se han generado medidas asociadas a los valores de impacto de las amenazas, costes y grado de corrección de las medidas de mitigación y control, y del coste de implantación de dichas medidas tomando como referencia el método Fine.

Abstract

The following document describes the procedure followed for the realization of Carlos Junco Diez´s Master Thesis and represents the last academic requirement for the obtention of the Telecommunications Engineering Degree by Univeridad Carlos III de Madrid.

Due to the need, in business, to prevent critical situations regarding operational aspects, that can lead a company to numerous losses or even bankruptcy, the motivation of this project arises: the development of an Operational Risk Management Plan in the telecommunications sector.

Although there are many different approaches and metrics when determining the efficiency of this kind of plan, the quickness of the updating processes, due to a constant monitorization, and the amount of threats that can be detected and mitigated are significant indicators of its effectiveness. The first step for the development of this project was to do a brief introduction to the concept of Operational Risk Management, then, a risk management plan has been developed as well. The latter consists on a five-step model: identification, assessment, analysis, implementation and monitoring. Data regarding values of the impact of the threats, costs and correction degree of the mitigation and control measures, and the cost of implementation of those measures have been generated through the use of the Fine Method for calculating risks, which has been taken as a reference.

Índice general

Índice de figuras

Índice de cuadros

Capítulo 1

Introducción y objetivos

La motivación de este proyecto surge ante la necesidad de prevenir situaciones de alto riesgo que puedan poner en peligro la operatividad de una empresa de telecomunicaciones y consecuentemente su continuidad. Un plan de control de riesgos operacionales proporciona un marco de actuación sistemático y eficaz a la hora de hacer frente a las amenazas. Este proyecto consiste en el desarrollo de un conjunto de pasos fundamentales, integrados a todos los niveles de la empresa, que son ejecutados cíclicamente.

1. Identificar amenazas.

2. Evaluar el riesgo.

3. Analizar y tomar de medidas de control del riesgo.

4. Implementar decisiones de control.

5. Supervisar y Revisar.

El objetivo desde el punto de vista económico es claro. Un procedimiento capaz de prevenir o minimizar los efectos causados por la materialización de una amenaza, supone un importante ahorro económico para la empresa. Además, es el sector de las telecomunicaciones, sobre el que se desarrolla gran parte de la actividad económica mundial. Un plan de control de riesgos operacionales en telecomunicaciones, supone una garantía en el desarrollo de la economía.

1.1. Fases del desarrollo

El desarrollo de este proyecto consiste e tres fases difrenciadas, que se detallan a continuación.

En primer lugar, tras una reunión inicial con el tutor del proyecto, comienza la tarea de investigación y documentación. A través de internet, páginas especializadas, recursos eléctronicos facilitados por la biblioteca de la universidad Carlos III y de algunos libros, se han desarrollado las ideas básicas y se han tomado una serie de posibles métodos que pueden ser utilizados para el desarrollo del proyecto.

El segundo paso del proyecto, una vez obtenida la documentación principal, consiste en elegir, de entre los posibles métodos de análisis disponibles , uno de ellos, el que más se ajuste a nuestros requisitos. Una vez establecido el método y las métricas que se usarán, se desarrolla cada uno de los pasos del método, generando resultados mediante documentos Excel.

Finalmente, tras el visto bueno del tutor, se procede a la redacción del proyecto, donde se reflejan los resultados obtenidos en el estudio y se redactan las conclusiones. El proyecto se da por finalizado tras una corrección final.

1.2. Medios empleados

A continuación se muestra una lista con los medios utilizados para la realización del proyecto.

Tipo	
HW	Ordenador portátil Lenovo 3000 N200
HW	Ordenador sobremesa HP Pavilion
HW	Monitor LG Flatron
HW	Wireless Router ZTE
HW	Conexión ADSL
HW	Cable RJ-45
SW	MS Windows 7
SW	MS Office 2007
SW	Linux Ubuntu 10.04
SW	Kile Latex editor + tex enviroment

Cuadro 1.1: Medios empleados.

1.3. Estructura de la memoria

A continuación se describe brevemente cómo esta estructurada la memoria del proyecto realizado:

Capítulo 1: Introducción

Capítulo 2: Presupuestos. Coste de realización del proyecto. Listado de planificación de tareas y material ulilizado.

Capítulo 3: Consiste en una breve introducción a los conceptos de riesgo operacional y gestión de riesgo, se define también el objetivo de la gestión operacional de los riesgos.

Capítulo 4: En este capítulo se describe el escenario sobre el que tendrá lugar el análisis de los riesgos operacionales, el sector de las telecomunicaciones. Se incluye un listado de actividades, servicios y activos que definen al sector.

Capítulo 5: En este capítulo se definen una serie de conceptos fundamentales, que ayudan a comprender el modelo de gestión de riesgos que se utilizará a lo largo del proyecto.

Capítulo 6: Modelo de actuación sobre el riesgo basado en cinco pasos fundamentales: identificar, evaluar, analizar, implementar y supervisar.

Capítulo 7: Define unas directivas básicas a la hora de gestionar el riesgo, especificando a qué nivel y sobre qué circunstancias se debe actuar sobre el riesgo.

Capítulo 8: Método Fine. este método establece una serie de métricas y fórmulas que permiten clasificar los riesgos y las medidas de control en función de diversos factores.

Capítulo 9: Idenficación de Amenazas. Primer paso del proceso gestión. Se enumeran las principales amenazas que pueden poner en peligro la operatividad de los servicios de telecomunicaciones.

Capítulo 10: Evaluación del riesgo. Es el segundo paso del proceso de gestión. A través del método Fine, se establece una matriz de riesgos para las amenazas identificadas en el paso anterior.

Capítulo 11: Análisis de medidas de control de riesgo. Se proponen una serie de medidas para controlar o mitigar los riesgos identificados, estableciendo grados de corrección y factores de coste para dichas medidas.

Capítulo 12: Implementación de decisiones de control. En función del paso anterior, se procede a la toma de decisiones sobre cuáles de las medidas propuestas serán implantadas y cuáles no lo serán.

Capítulo 13: Supervisión y revisión. Definición de responsabilidades para integrar el plan de gestión y mantener una monitorización contínua sobre el riesgo con el fin de aumentar su efectividad.

Capítulo 14: Coste de implantación del plan. Se aproxima, en función de datos proporcionados por el INE y la ONTSI, un presupuesto para la implantación del plan establecido en el sector de las telecomunicaciones.

Capítulo 15: Conclusiones.

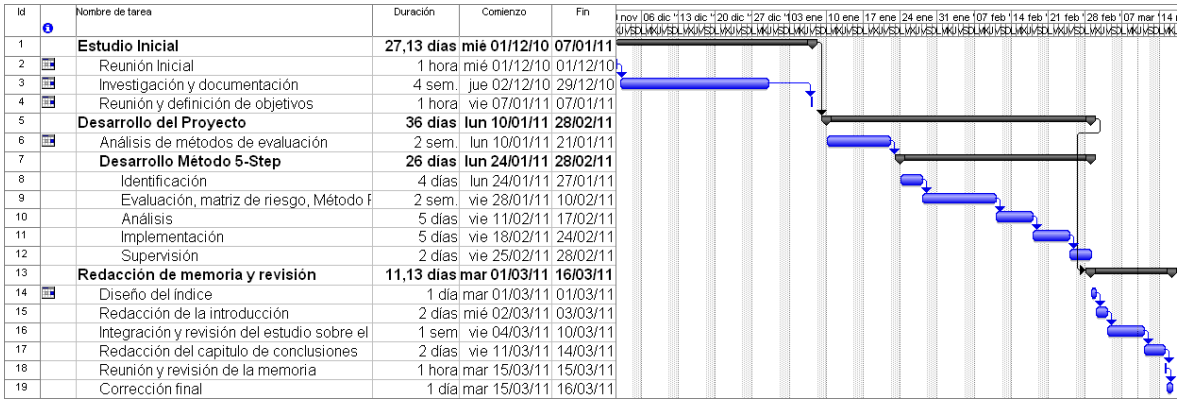
Capítulo 2

Presupuesto

En este capítulo se presentan los procedimientos y mecanismos puestos en práctica para garantizar una adecuada consecución de los objetivos del proyecto.
Se indican, además, los recursos materiales necesarios para la realización del proyecto con sus principales características. Éstos se tendrán en cuenta, tras el establecimiento de la planificación, para realizar un cálculo de los costes y beneficios del presente proyecto.

2.1. Planificación

Tras una primera reunión inicial con el tutor del proyecto, se procede a la investigación y documentación sobre el tema prouesto. Después, tras una segunda reunión, se definen los objetivos a alcanzar.
La tarea "Desarrollo del Proyecto" se divide en dos sub-tareas. En primer lugar se han analizado los distintos métodos de cálculo de riesgo, por otra parte, se han estudiado los procedimientos a seguir a la hora de gestionarlo. Una vez seleccionado el método, se analiza cada uno de los pasos, de forma especifíca, estableciendo las métricas a través del método Fine.
Una vez concluídos los procesos de documentación y desarrollo del proyecto, se procede a su escritura. Una vez terminada, tiene lugar una nueva reunión con el tutor donde se revisa la memoria, para proceder así a una corrección final que de por concluído el proyecto. La figura 2.1 muestra la planificación del proyecto mediante un diagrama de Gannt.



Id	Nombre de tarea	Duración	Comienzo	Fin
1	**Estudio Inicial**	**27,13 días**	**mié 01/12/10**	**07/01/11**
2	Reunión Inicial	1 hora	mié 01/12/10	01/12/10
3	Investigación y documentación	4 sem.	jue 02/12/10	29/12/10
4	Reunión y definición de objetivos	1 hora	vie 07/01/11	07/01/11
5	**Desarrollo del Proyecto**	**36 días**	**lun 10/01/11**	**28/02/11**
6	Análisis de métodos de evaluación	2 sem.	lun 10/01/11	21/01/11
7	**Desarrollo Método 5-Step**	**26 días**	**lun 24/01/11**	**28/02/11**
8	Identificación	4 días	lun 24/01/11	27/01/11
9	Evaluación, matriz de riesgo, Método F	2 sem.	vie 28/01/11	10/02/11
10	Análisis	5 días	vie 11/02/11	17/02/11
11	Implementación	5 días	vie 18/02/11	24/02/11
12	Supervisión	2 días	vie 25/02/11	28/02/11
13	**Redacción de memoria y revisión**	**11,13 días**	**mar 01/03/11**	**16/03/11**
14	Diseño del índice	1 día	mar 01/03/11	01/03/11
15	Redacción de la introducción	2 días	mié 02/03/11	03/03/11
16	Integración y revisión del estudio sobre el	1 sem	vie 04/03/11	10/03/11
17	Redacción del capitulo de conclusiones	2 días	vie 11/03/11	14/03/11
18	Reunión y revisión de la memoria	1 hora	mar 15/03/11	15/03/11
19	Corrección final	1 día	mar 15/03/11	16/03/11

Figura 2.1: Planificación del proyecto con Diagrama de Gantt.

2.2. Gestión de recursos

En este apartado se describen los medios materiales y recursos utilizados para llevar a cabo este proyecto. El siguiente documento describe el coste de cada uno de los equipos, dispositivos y recursos y finalmente muestra el presupuesto total del proyecto.

UNIVERSIDAD CARLOS III DE MADRID
Escuela Politécnica Superior

PRESUPUESTO DE PROYECTO

1.- Autor:
Junco Diez, Carlos

2.- Departamento:
Estadística

3.- Descripción del Proyecto:
- Titulo: Plan de Control de Riesgos Operacionales en Telelcomunicaciones
- Duración (meses): 3,3
Tasa de costes Indirectos: 20%

4.- Presupuesto total del Proyecto (valores en Euros):
Euros 10.938

5.- Desglose presupuestario (costes directos)

PERSONAL

Apellidos y nombre	N.I.F.	Categoría	Dedicación (hombres mes) [a]	Coste hombre mes	Coste (Euro)
Junco Diez, Carlos	71277480	Ingeniero	3,3	2.694,39	8.891,49
		Hombres mes 3,3		Total	8.891,49

[a] 1 Hombre mes = 131,25 horas. Máximo anual de dedicación de 12 hombres mes (1575 horas)
Máximo anual para PDI de la Universidad Carlos III de Madrid de 8,8 hombres mes (1.155 horas)

EQUIPOS

Descripción	Coste (Euro)	% Uso dedicado proyecto	Dedicación (meses)	Periodo de depreciación	Coste imputable [d]
Ordenador Portatil Lenovo 3000 N20	680,00	100	3	60	37,40
Ordenador Sobremesa HP Pavilion	450,00	100	3	60	24,75
Monitor LG Flatron	120,00	100	3	60	6,60
Wireless Router ZTE	40,00	100	3	60	2,20
Cable RJ-45	5,00	100	3	60	0,28
MS Windows 7	120,00	100	3	60	6,60
MS Office 2007	100,00	100	3	60	5,50
Linux Ubuntu 10.04	0,00	100	3	60	0,00
Kile Latex editor + tex enviroment	0,00	100	3	60	0,00
				Total	83,33

[d] Fórmula de cálculo de la Amortización:

$$\frac{A}{B} x C x D$$

A = nº de meses desde la fecha de facturación en que el equipo es utilizado
B = periodo de depreciación (60 meses)
C = coste del equipo (sin IVA)
D = % del uso que se dedica al proyecto (habitualmente 100%)

OTROS COSTES DIRECTOS DEL PROYECTO[e]

Descripción	Empresa	Costes imputable
Conexión ADSL	Jazztel	140,00
	Total	140,00

[e] Este capítulo de gastos incluye todos los gastos no contemplados en los conceptos anteriores, por ejemplo: fungible, viajes y dietas, otros,...

6.- Resumen de costes

Presupuesto Costes Totales	Presupuesto Costes Totales
Personal	8.891
Amortización	83
Costes de funcionamiento	140
Costes Indirectos	1.823
Total	10.938

Figura 2.2: Presupuesto.

Capítulo 3

Introducción a la gestión de riesgos

3.1. Riesgo Operacional y Gestión de Riesgo

El primer paso en la medición del riesgo es contar con una definición del mismo. Según la Real Academia, riesgo se define como: "Contingencia o proximidad de un daño", es decir, la probabilidad de accidente o pérdida debida a la exposición a uno o varios peligros, incluyendo daño en las personas y pérdida de recursos. En el sector de las telecomunicaciones, las actividades diarias implican riesgo y requieren decisiones que incluyen evaluación y gestión del riesgo.[12]

El riesgo debe ser una parte completamente integrada en la planificación y ejecución de cualquier operación, no una forma de reaccionar cuando algún problema imprevisto ocurre. Una acertada selección de los posibles riesgos, junto con el análisis y el control de los peligros que pueden ocurrir, da lugar a un plan de acción que determina la forma de enfrentarse a estas dificultades.

El acuerdo de Basilea II (Junio 2004), que formula estándares y guías de supervisión con el fin de mejorar las prácticas bancarias, define el riesgo operacional como:

"El riesgo de pérdida resultante de una falta de adecuación o de un fallo de los procesos, el personal o los sistemas internos, o bien como consecuencia de acontecimientos externos" [15].

Es de gran importancia dar una definición, ya que hasta este momento no existía una en el sector. Ésto, supone un avance hacia el consenso y la homogeneización de términos. Basilea II aporta, en este sentido, un punto de partida básico y un marco de referencia a la hora

de tratar el riesgo.

El riesgo operacional es reconocido como algo distinto del riesgo de mercado o trade risk, aunque un fallo operacional puede desembocar en una perdida de control y en un incremento en la exposición de estas áreas también. Aún así, como sugiere la definición, la gestión del riesgo operacional, que también llamaremos ORM (del inglés, Operational Risk Management), queda confinada a la gestión de aquellos elementos que son competencia del negocio operacional. El riesgo operacional es a menudo considerado como relevante sólo para los bancos y la industria financiera, pero de hecho es una faceta de cada organización y refleja el hecho inevitable de que los activos, procesos y los recursos humanos pueden fallar, dando lugar a efectos imprevistos o indeseables para la empresa. Algunos ejemplos sencillos que podemos encontrar:

- Un ordenador se estropea y un día de trabajo está perdido, pagamos horas extra para recuperar.
- Un manager subestima la complejidad de una tarea y el proyecto se alarga.

Gestión de riesgo o risk management, consiste básicamente en un proceso preventivo sobre el riesgo, no reactivo, esto es, desarrollar mecanismos que permitan anticipar la aparición de un peligro. Esta aproximación está basada en la filosofía de que, es irresponsable y anti-económico esperar a que tenga lugar un accidente, para saber cómo prevenirlo la próxima vez que vuelva a suceder.

La gestión del riesgo tiene lugar cada vez que modificamos la forma en la que hacemos algo para aumentar lo máximo posible las posibilidad de éxito de una acción, mientras que de la misma forma intentamos reducir al máximo las posibilidades de fracaso o pérdida. Es de sentido común aproximarse al equilibrio de los riesgos frente a los beneficios que pueden obtenerse en una situación y por tanto eligiendo la forma más efectiva de actuar.

La gestión del riesgo operacional, es una herramienta de decisión para ayudar sistemáticamente a identificar los riesgos y beneficios operacionales y para determinar los mejores procesos de acción para actuar en cualquier situación.

En contraste a otros análisis de riesgo, que se realizan durante el desarrollo de un proceso, ORM se desarrolla durante el uso operacional. Este proceso de gestión del riesgo, al igual que otros, está diseñado para minimizar riesgos con el fin de reducir los contratiempos, conservar los activos y salvaguardar la salud y el bienestar.

3.2. Objetivo de la gestión del riesgo operacional

La siguiente figura ilustra los objetivos de la gestión del riesgo: proteger a las personas, equipos y otros recursos, a la vez que se hace el uso más efectivo posible de ellos.

Minimizando el riesgo de pérdida, se reduce el coste y se continua de forma puntual con el programa establecido. Además, el objetivo fundamental de la gestión del riesgo es aumentar la efectividad del personal y del material determinando [4].

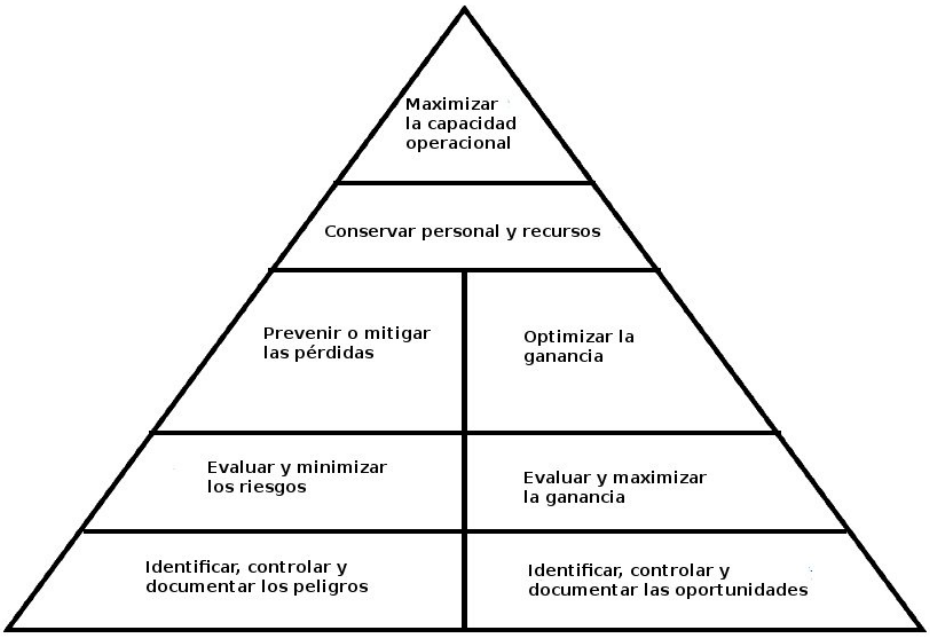


Figura 3.1: Objetivos de ORM.

Capítulo 4

Escenario

El escenario en el que se desarrolla el proyecto de control de riesgo operacional comprende de forma genérica el sector de las telecomunicaciones. Según el Instituto Nacional de Estadística, se deben tener en cuenta aquellas industrias de servicios TIC que se dedican a [7]:

- Actividades de telecomunicaciones por cable.
- Actividades de telecomunicaciones inalámbrica.
- Actividades de telecomunicaciones por satélite.
- Otras actividades de telecomunicación.

Los servicios que proporcionan estas empresas de telecomunicaciones son los indicados en el cuadro 4.1.

Servicios de telecomunicaciones
•Servicios de telefonía fijos - acceso y uso.
•Servicios de telefonía fijos - servicios de dirección de llamada.
•Servicios de telecomunicaciones móviles - acceso y uso.
•Servicios de telecomunicaciones móviles - servicios de dirección de llamada.
•Servicios de transmisión de información.
•Servicios de red privados.
•Otros Servicios de telecomunicaciones.
•Servicios vertebrales de internet.
•Servicios de acceso de banda estrecha de internet.
•Servicios de acceso de banda ancha de internet.
•Otros servicios de telecomunicaciones de internet.

Cuadro 4.1: Servicios de telecomunicaciones.

Para poder realizar una estimación del coste de un proyecto de gestión de riesgo operacional para el sector, se debe considerar el inmovilizado material, esto es, el conjunto de elementos patrimoniales reflejados en el activo, con carácter permanente, que no están destinados a la venta y que son utilizados en la producción de bienes y servicios. Se han considerado los siguientes activos:

- Ordenadores y equipos periféricos (Cuadro 4.2).
- Material de telecomunicaciones (Cuadros 4.3, 4.4, 4.5).
- Software para el negocio (Cuadro 4.6).
- Datos: Información de la organización.
- Instalaciones: Incluye los edificios, mobiliario, etc.

Listado de activos: Ordenadores y equipos periféricos
•Máquinas capaces de conectarse a una máquina de procesamiento de datos o a una red
•Máquinas automáticas de procesamiento de datos, ordenadores, etc.
•Periféricos de entrada (teclado, joystick, ratón, etc.)
•Escáneres (excepto combinación de impresora, escáner, copiadora y/o fax)
•Impresoras de tinta usadas con máquinas de procesamiento de datos
•Impresoras de láser usadas con máquinas de procesamiento de datos
•Otras impresoras usadas con máquinas de procesamiento de datos
•Unidades que realizan dos o más de las funciones siguientes: impresión, exploración, copiar, fax
•Otros dispositivos periféricos de entrada o salida
•Unidades de almacenaje de medios de comunicación fijas
•Unidades de almacenaje de medios de comunicación desprendibles
•Otras unidades de máquinas automáticas de procesamiento de datos
•Partes y accesorios de maquinas informáticas
•Monitores y proyectores, principalmente usados en un sistema automático de procesamiento de datos
•Dispositivos de almacenaje permanentes en estado sólido

Cuadro 4.2: Listado de Activos: Ordenadores y equipos periféricos.

Listado de activos: Telecomunicaciones
Equipos de conmutación local en oficinas centrales
•Equipos O.C. automáticos.
•Equipos O.C. autocombinados.
•Equipos O.C. batería central.
•Equipos O.C. magneto.
•Equipos de fuerza.
•Equipos de tasación.
•Equipos de radio.
•Equipos canalizadores y repetidores en O.C.
Equipos de conmutación L.D. en oficinas centrales
•Posiciones de larga distancia.
•Equipos de radio.
•Equipos canalizadores y repetidores en O.C.
Otros equipos de O.C.
•Teléfonos calculógrafos y sillas de operadoras:
Equipos seguridad industrial en oficinas centrales.
•Equipos industriales de climatización.
Equipos para subscriptores.
•Teléfonos automáticos.
•Teléfonos batería central.
•Teléfonos magneto.
•Equipos especiales.
•Alambres bajantes.
•Alambre interior.
•PABX automáticos.
•PBX automáticos.
•PBX batería central.
•PBX magneto.
•Locutorios.
•Equipos fax.

Cuadro 4.3: Activos de Telecomunicaciones.

Listado de activos: Telecomunicaciones (cont.)
Equipos planta externa local.
•Postes y crucetas de madera.
•Postes y crucetas de hierro.
•Postes de cemento.
•Antenas y líneas de transmisión.
•Cables aéreos y bobinas de carga.
•Cables subterráneos y bobinas de carga.
•Cables interiores.
•Cables aéreos desnudos.
•Equipos canalizadores y repetidores en postes.
•Conductos y cámaras.
•Cables y enlaces.
•Sala de cables y MDF.
•Armarios de distribución.
•Cajas terminales, doble conexión.
•Empalmes de cables aéreos y subterráneos.
•Sistema gráfico de manejo de redes.
•Cables de fibra óptica.
•Cámaras y ductos.

Cuadro 4.4: Activos de Telecomunicaciones.(cont.)

Listado de activos: Telecomunicaciones (cont.)
Equipos planta externa L.D.
•Postes y crucetas de madera.
•Postes y crucetas de hierro.
•Postes de cemento.
•Antenas y líneas de transmisión.
•Cables aéreos y bobinas de carga.
•Cables subterráneos y bobinas de carga.
•Alambre aéreos desnudos.
•Equipos canalizadores y repetidores en postes.
•Conductos y cámaras.
•Equipos de control automático.
•Estaciones satelitales terrenas.
•Cables de fibra óptica.
•Equipos de fibra óptica.
•Segmento espacial.

Cuadro 4.5: Activos de Telecomunicaciones.(cont..)

Listado de activos: Software
•Sistemas operativos.
•Software de red.
•Software de gestión de datos.
•Instrumentos de desarrollo y software de lenguajes de programación.

Cuadro 4.6: Activos de software.

Capítulo 5

Conceptos fundamentales

El modelo de riesgo ilustrado en la figura 5.1 ofrece una representación gráfica que ayuda a comprender de forma más visual el proceso de la gestión del riesgo operacional y la relación entre los distintos conceptos.

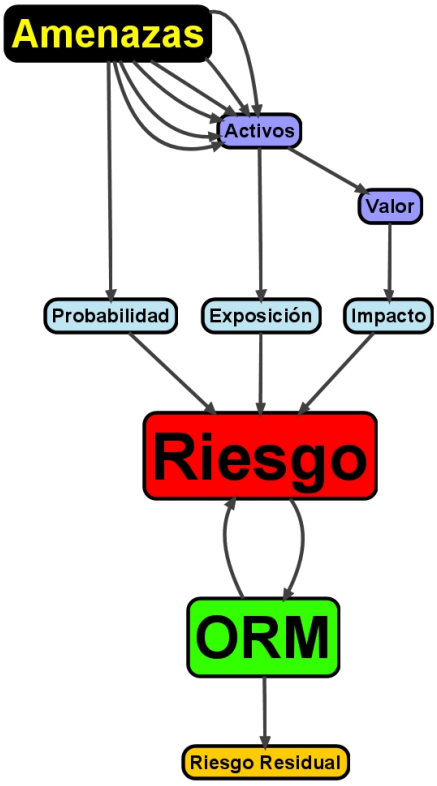


Figura 5.1: Modelo de gestión de riesgo.

5.1. Causas o amenazas

Las causas de los problemas siempre se encuentran mas allá de nuestra percepción normal del control operativo. Son conocidas como amenazas o peligros (ocurrencia de un evento que cause un impacto no deseado) y hay muchas a considerar. Incluyen eventos tales como los errores humanos o catástrofes meteorológicas, terrorismo, etc.

5.2. Dependencia

Muchas de las amenazas simplemente son evitadas por la organización debido a las medidas básicas de recuperación. Pero cuando una amenaza consigue atravesar los sistemas de defensa, sus efectos se pueden extender más allá de la propia organización afectando a clientes y mercados, de forma que se convierten en visibles de manera externa. Hay eventos de carácter extremo que pueden afectar a grandes sectores de un mismo negocio, a éstos los llamamos crisis, catástrofes, etc.
La propagación del efecto a través de un negocio se debe a la interdependencia de los procesos. Consecuentemente toda materialización de una amenaza sobre los activos de una empresa tiene un efecto directo sobre su valor.

5.3. Perfil de riesgo

El riesgo tiene tres componentes principales: probabilidad, exposición e impacto.

Probabilidad es un indicador de con qué frecuencia podemos esperar que un evento en particular ocurra.

La exposición representa el grado de protección actual de los activos en el caso de que la amenaza llegase a materializarse sobre estos.

El impacto es un reflejo del daño o la pérdida, por lo general en términos económicos, provocado por un evento.

En conjunto, representan un indicador de cuánto se espera que suframos como resultado de un evento que no está planeado.

- Probabilidad: Es una medida cuantitativa y se aplica normalmente en ausencia de información estadística. Las medidas cuantitativas incluyen, por ejemplo, que haya un incendio cada 10 años en una determinada compañía. Las estimaciones cualitativas son normalmente comparativas.

- Exposición: Refleja el estado de protección al daño, identificando dónde se encuentran huecos o vulnerabilidades, esto es, debilidad o ausencia de medidas de salvaguarda y superposiciones.

- Impacto: Representa un reflejo de la pérdida financiera a raíz de un incidente, las pérdidas financieras pueden ser complejas, incluyendo valor del crédito, pérdida de oportunidad, multas, penalizaciones y restricciones. La pérdida también incluye medidas cualitativas como puede ser, por ejemplo, la reputación, imagen, moral, lealtad, confianza y credibilidad.

Cada uno es únicamente característico de la organización y sustancialmente define la implementación y el coste del plan de ORM.

5.4. Ciclo de vida de un proceso ORM

Para gestionar el riesgo operacional debemos primero concebir formas de medida, priorización y monitorización y de reducción de la exposición al riesgo.
El ciclo de vida ORM, dada su importancia, será tratado de forma más minuciosa en el siguiente capítulo. A grandes rasgos, sus características son las siguientes:

- Evaluación del Riesgo: La evaluación del riesgo implica la recopilación de la información relacionada a las personas, procesos, sistemas y circunstancias del entorno que culminan en un perfil de amenaza. Esto es, una lista descriptiva de las amenazas que actualmente pueden afectar a una organización con una cierta probabilidad. Con esto se identifican vulnerabilidades en la empresa que permitirían la propagación de amenazas con potencial de destrucción. La evaluación combina análisis de impacto e información estadística para priorizar la conexión de los gaps, de tal forma que se puedan establecer propuestas de estrategias para la mitigación.

- Mitigación o degradación: Hay tres puntos fundamentales en torno a los cuáles el flujo del modelo de riesgo puede ser interrumpido y su riesgo reducido. Las amenazas pueden ser prevenidas, reducidas o evitadas. Gaps, vulnerabilidades y debilidades pueden ser rectificados a través de medidas de salvaguarda (medidas de control para reducir el riesgo asociado a una determinada amenaza), de forma que se contengan la propagación de los efectos a lo largo de la organización. Pueden también presentarse medidas de recuperación, para en el caso de que lo peor ocurra, la duración del corte de servicios y sus correspondientes efectos sea reducida. El modelo ofrece una visión simple de cómo comprendiendo, podemos gestionar el riesgo operacional. Por lo general, es fácil para la gente comprender y visualizar la actividad en este contexto.

- Planificación continua: Consiste en un conjunto de actividades que ayudan a asegurar la continuidad en los planes de trabajo. La práctica fomenta que el personal que trabaja en una empresa desarrolle un entendimiento consistente sobre aspectos del riesgo y de la continuidad, creando familiaridad con hechos que podrían tener lugar. Ensayos y tests proporcionan formas controladas a la hora de simular incidentes reales, limando los problemas bajo un entorno de prueba seguro. La planificación contínua o BCP (Plan de Continuidad del Negocio) proporciona el respaldo definitivo donde las medidas de mitigación de riesgo fallan y donde la organización afronta una catástrofe potencial. BCP identifica lo que la organización debe proporcionar a las personas, procesos, sistemas y otras estructuras para asegurar su supervivencia.

5.5. Riesgo residual

Riesgo remanente una vez los controles han sido identificados y seleccionados.

5.6. Diseño del programa

ORM es potencialmente una tarea muy complicada y que potencialmente tenga que llevarse a cabo indefinidamente.

Requiere un nivel de control, respaldo y estructuración y un programa que englobe otras iniciativas como TQM (Gestión de Calidad Total) BPR (Ingeniería de Procesos de Negocio).

5.7. Analisis de Impacto

BIA (Business Impact Analysis) es la técnica utilizada para determinar la tolerancia de una organización y el patrón característico de pérdida debido a la interrupción que produce la aparición de un fallo. La información sobre prioridad y el marco de tiempo resultantes es utilizada para determinar la pérdida de incidentes específicos y es usada en la evaluación del riesgo. Esta técnica se usa también para establecer el tiempo requerido para la recuperación de las funciones, procesos y sistemas tras la pérdida.

5.8. Valor de la gestión de riesgo operacional

De una manera u otra gestionamos la exposición al riesgo operacional de forma habitual: cerrar puertas y ventanas por la noche, uso de antivirus, etc. pero muchas compañías deciden hacerlo a posteriori: tras un robo, después de que un sistema haya fallado. Como resultado, lo que se obtiene muchas veces es un simple parcheado de esos problemas, solapando unos sobre otros para tapar el fallo. Lo único que ésto refleja es el legado de decisiones erróneas, una detrás de otra, tomadas en el pasado que además, rara vez se adaptan a las necesidades reales de la empresa. Aún así dan la falsa impresión de mantener a la empresa en un estado “seguro”.

Es necesario un procedimiento que permita a las empresas estar prevenidas frente a la aparición de imprevistos que puedan tener consecuencias fatales para la propia empresa, sus activos o las personas que trabajen o dependan de ella. ORM es una respuesta lógica a estos requerimientos, es decir:

- Sistemático, asegurando que todos los riesgos sean identificados y tratados apropiadamente.
- Repetible, como parte de un proceso que facilita el cambio.
- Auditable, evidenciando las decisiones de dirección.
- Enteramente a la disposición del negocio, eliges aceptar o mitigar un riesgo basado enteramente en las evidencias que están ante tí.

Capítulo 6

Ciclo de un proceso ORM: Modelo de 5 pasos

El procedimiento a la hora gestionar el riesgo operacional consiste en un modelo de cinco pasos explicado a continuación [5]:

1. Identificar amenazas.
2. Evaluar el riesgo.
3. Analizar y tomar de medidas de control del riesgo.
4. Implementar decisiones de control.
5. Supervisar y Revisar.

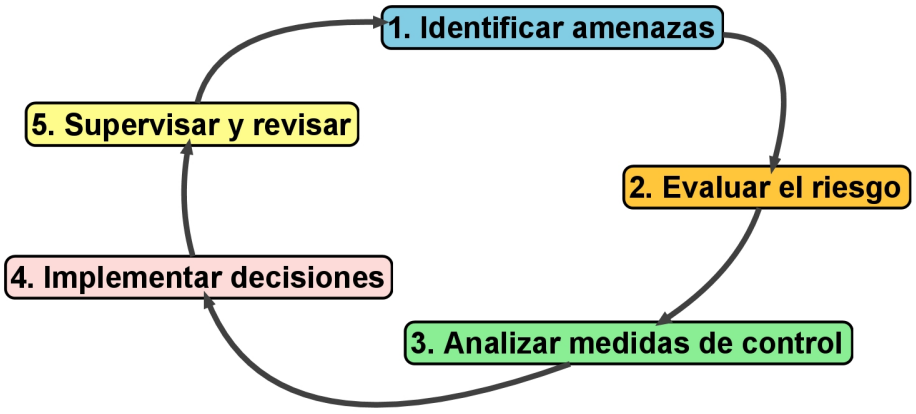


Figura 6.1: Modelo de 5 pasos.

6.1. Identificar las amenazas

Un peligro o amenaza se define como toda condición, real o potencial, que puede causar degradación, lesiones, enfermedad, muerte, pérdida o daños a la propiedad.
Experiencia, sentido común y herramientas específicas de análisis ayudan a identificar los riesgos. La identificación de las amenazas consiste en un listado de todos los peligros asociados a cada paso del análisis operacional junto con las posibles causas de dichos peligros.

6.2. Evaluar el riesgo

La evaluación del riesgo consiste en la aplicación de medidas cuantitativas y cualitativas para determinar el nivel de riesgo asociado a peligros específicos.

Este proceso define la probabilidad y la gravedad de un accidente que puede darse como resultado de los peligros a los que están expuestos las personas o los recursos de la compañía. Se llevará a cabo a través de la matriz de riesgo.

6.3. Analizar y tomar las medidas de control del riesgo

Investigar estrategias y herramientas específicas para reducir, mitigar o eliminar el riesgo.

Todo riesgo tiene tres componentes: probabilidad de aparición, gravedad del peligro y exposición al riesgo de las personas y los recursos.

Las medidas de control efectivo eliminan o reducen al menos una de las anteriores. El análisis debe tener en cuenta los costes y beneficios totales de las acciones correctivas, priorizando aquellos aspectos más importantes para el negocio. Además en este paso se tomarán las **decisiones de control**, esto es, identificar la toma de decisión adecuada. Esa toma de decisión debe proporcionar, el mejor control o la mejor combinación de controles, basándose en el análisis del paso anterior.

6.4. Implementar decisiones de control

La gestión debe establecer un plan para aplicar las medidas de control que han sido seleccionadas, definir los procesos y procedimientos, proporcionar los plazos, materiales y personal necesario para llevar a cabo las mismas.

6.5. Supervisar y Revisar

Una vez que los mecanismos de control han sido establecidos, el proceso debe ser monitorizado y periódicamente reevaluado para asegurar su efectividad. Los trabajadores y encargados a cada nivel deben cumplir respectivamente sus misiones para asegurar que los controles se realizan con continuidad.

El proceso de la gestión del riesgo continua a lo largo del ciclo de vida del sistema, de la misión o de la actividad que se está analizando.

Para obtener el máximo beneficio de esta herramienta, es esencial:

- **Aplicar los pasos de forma secuencial:** Cada paso es un bloque que construye el siguiente y por tanto debe ser completado antes de avanzar al siguiente paso. Si la identificación de un peligro es interrumpida para centrarse en el control de un peligro en particular, entonces otros peligros pueden pasarse por alto. Hasta que todos los peligros sean identificados, no podremos dar el paso por finalizado de forma efectiva.
- **Mantener el equilibro en el proceso:** Los cinco pasos son importantes. Debe asignarse tiempo y recursos para realizarlos todos.
- **Aplicar el proceso de forma cíclica:** El paso de "supervisar y revisar" debe incluir una nueva visión a la operación que está siendo analizada, para ver si se pueden identificar nuevos peligros.
- **Involucrar al personal en el proceso:** Estar convencidos de que el control del riesgo es una misión de apoyo, y que las personas que forman parte del trabajo lo vean como algo positivo. Además, las personas que están expuestas al riesgo, conocen normalmente qué acciones funcionan y cuáles no.

Capítulo 7

Niveles del proceso de gestión y principios de actuación

El proceso ORM se da en tres niveles: la decisión de cuál de los tres niveles es el necesario estará basada en función de la situación, del nivel de competencia (capacidad) del personal y el tiempo y recursos disponibles. Mientras podría ser preferible realizar de forma deliberada un proceso ORM en profundidad para todas las evoluciones, el tiempo y los recursos disponibles para hacerlo no están siempre disponibles.

Uno de los objetivos de la práctica de ORM es desarrollar la suficiente capacidad a la hora de aplicar el proceso, de tal forma que ORM se convierta en una parte automática o intuitiva de nuestra metodología de toma de decisiones.

En el entorno operacional, cada encargado debe ser capaz de utilizar el proceso de tiempo-crítico para tomar decisiones periódicamente que generen tempo y faciliten resultados decisivos. Los tres niveles son los siguientes [5].

7.1. Velocidad de respuesta

Velocidad de respuesta o “Time Critical“ a nivel de ORM es utilizado por el personal ya experimentado para considerar el riesgo mientras se toman decisiones en una situación en la que se dispone poco tiempo. Es el nivel normal usado de ORM durante la ejecución de

la fase de preparación y también la que se plantea en escenarios de respuesta a una crisis. Representa una ayuda a la hora de elegir la dirección adecuada de actuación, cuando tiene lugar un suceso imprevisto durante la ejecución de una operación que si que está planeada.

7.2. Deliberación

La aplicación completa del proceso de cinco pasos, ayudará a la hora de planificar una operación o de evaluar los procedimientos usados. Básicamente utiliza la experiencia y la lluvia de ideas para identificar los peligros y desarrollar sistemas de control y es por tanto más efectivo cuando se realiza en grupo. Ejemplos posibles de deliberación incluyen: planificación de operaciones, revisión, mantenimiento y preparación de procedimientos y control de daños como también planificación de respuesta a catástrofes.

7.3. Exhaustividad (in-depth)

El proceso de deliberación implica evaluación del riesgo exhaustiva (dos primeros pasos del proceso). La investigación sobre la información disponible, uso de diagramas, herramientas de análisis, tests regulares o seguimiento a largo plazo de los peligros asociados con la operación realizada (a veces con la ayuda de expertos) se usa también para identificar y acceder a los peligros. Se utiliza para estudiar los peligros de una forma más exhaustiva en sistemas u operaciones complejas, o cuando los peligros no se han comprendido a la perfección. Ejemplos de aplicaciones en profundidad incluyen planificación a largo plazo de operaciones complejas, presentación de nuevo material, desarrollo de tácticas y formación y sistemas de revisión.

ORM incorpora los siguientes principios [4]:

7.4. No aceptar riesgos innecesarios

Un riesgo innecesario es aquel que no tiene un retorno proporcional en términos de beneficios u oportunidades. Toda acción conlleva un riesgo. La elección más lógica para realizar con éxito una operación es aquella que cumpla todos los requisitos con el mínimo riesgo aceptable.

7.5. Tomar decisiones de riesgo al nivel adecuado

Cualquiera puede tomar una decisión sobre el riesgo. Sin embargo, la decisión adecuada la toma aquella persona o grupo capaz de asignar los recursos de forma que reduzca o elimine el riesgo y además implemente controles sobre dicho riesgo. La persona encargada de tomar la decisión debe estar autorizada para aceptar niveles típicos de riesgo sobre la operación planificada.

7.6. Aceptar el riesgo cuando el beneficio supera el coste

Todos los beneficios deben ser comparados con los costes. Incluso operaciones de alto riesgo pueden ser superadas si existe claro conocimiento de que la suma de los beneficios superará a los costes totales. El balance entre costes y beneficios es un proceso subjetivo y debe ser determinado a la hora de tomar la decisión.

7.7. Integrar ORM a la planificación en todos los niveles

Los distintos riesgos deben ser evaluados y gestionados en las fases de planificación de toda operación. Estos cambios son hechos en el proceso de planificación y ejecución, de esta forma se reducen los costes y se fortalece la efectividad total del proceso ORM.

Capítulo 8

Método Fine para el análisis de riesgos

8.1. Método Fine

El método Fine [8] es un procedimiento originalmente previsto para el control de los riesgos cuyas medidas correctoras eran de alto coste. Se considera que puede tener utilidad en la valoración y jerarquización de los riesgos. Dicho método permite calcular el grado de peligrosidad de los riesgos y en función de éste, ordenarlos por su importancia. Los conceptos empleados son los siguientes:

- Impacto: se define como el daño económico, debido al riesgo que se considera, incluyendo desgracias personales y daños materiales. Se asignan valores numéricos en función del cuadro 8.1.

Impacto	Daños	I
Catástrofe	a partir de 900.000€	100
Critico	entre 450.000€ y 900.000€	50
Grave	entre 90.000€ y 450.000€	25
Moderado	entre 9.000€ y 90.000€	15
Menor	entre 900€ y 9.000€	5
Insignificante	hasta 900€	1

Cuadro 8.1: Matriz de impacto.

- Exposición: es la frecuencia con que se presenta la situación de riesgo. Siendo tal que

el primer acontecimiento indeseado iniciaría la secuencia del accidente. Se valora desde "continuamente" con 10 puntos hasta "remotamente" con 0,5 puntos. La valoración se realiza según el cuadro 8.2.

Exposición		**E**
Continuamente	Muchas veces al día	10
Frecuentemente	Una vez al día aprox.	6
Ocasionalmente	De una vez a la semana, a una vez al mes	3
Irregularmente	De una vez al mes, a una vez al año	2
Raramente	Cada bastantes años	1

Cuadro 8.2: Matriz de exposición.

- Probabilidad: la posibilidad de que, una vez presentada la situación de riesgo, se origine el accidente. Habrá que tener en cuenta la secuencia completa de acontecimientos que desencadenan el accidente. Se valora en función del cuadro 8.3.

Probabilidad		**P**
Certera	Resultado más probable y esperado	10
Probable	Completamente posible	6
Posible	Coincidencia rara, pero posible	3
Improbable	Coincidencia muy rara	1
Excepcional	Coincidencia remota	0,5

Cuadro 8.3: Matriz de probabilidad.

Según la puntuación obtenida en cada una de las variables anteriores se obtendrá el Grado de Peligrosidad de un Riesgo, lo que se consigue aplicando la siguiente fórmula:

$$Riesgo = Impacto \times Exposicion \times Probabilidad \tag{8.1}$$

Una vez se ha calculado el Factor de Riesgo o Grado de Peligrosidad de cada uno de los riesgos detectados, éstos se clasifican según la gravedad relativa de sus peligros. Clasificaremos el riesgo y actuaremos sobre él en función del grado. A modo de guía se presenta el cuadro 8.4.

Dicho método se completa con el estudio de la justificación de la inversión realizada para eliminar los riesgos, siendo función del Grado de Peligrosidad, del coste de las medidas correc-

Factor de Riesgo	R	Actuación frente al riesgo
Muy Alto	mayor que 400	Detención inmediata de la actividad peligrosa
Alto	entre 200 y 400	Corrección inmediata
Notable	entre 70 y 200	Corrección necesaria urgente
Moderado	entre 20 y 70	Debe corregirse
Aceptable	menor que 20	Puede omitirse la corrección, pero deben establecerse medidas

Cuadro 8.4: Factor de riesgo.

toras y del grado de corrección conseguido. El cuadro 8.5 asocia el coste de la instauración de la medida de control del riesgo a un número, en función del valor del mismo.

Factor de Coste	F.C.
Muy Alto	10
Alto	6
Medio	4
Bajo	3
Muy Bajo	2
Mínimo	1

Cuadro 8.5: Factor de coste.

La relación entre el factor de riesgo inherente, es decir, anterior a la instauración de las medidas de control de riesgo y el riesgo residual, el cual sigue presente tras la instauración de dichas medidas, representa lo que llamamos grado de corrección.

$$G.Correccion = 100 - (R.Residual \div R.Inherente) \times 100 \tag{8.2}$$

En función del porcentaje de riesgo corregido se asignará un valor al grado de corrección como indica el cuadro 8.6.

Grado de corrección	G.C.
Riesgo eliminado al 100 %	1
Riesgo reducido al menos al 75 %	2
Riesgo reducido del 50 % al 75 %	3
Riesgo reducido del 25 % al 50 %	4
Riesgo reducido menos del 25 %	6

Cuadro 8.6: Grado de corrección.

Finalmente queda por saber si la implantación de la medida de control está o no justificada, en términos económicos. El método Fine establece la justificación sobre una medida de control de riesgo relacionando el Riesgo Inherente con el Factor de Coste de una medida y con el Grado de corrección de la siguiente forma:

$$Justificacion = R.Inherente \times (F.C. \times G.C.) \tag{8.3}$$

El cuadro 8.7 refleja en qué casos, según el método, la inversión está justificada.

Justificación de la inversión	J
Justificado	mayor de 20
Probable justificación	entre 10 y 20
No justificado	menor de 10

Cuadro 8.7: Justificación de la inversión.

El resultado de una evaluación de riesgos debe servir para hacer un inventario de acciones, con el fin de diseñar, mantener o mejorar los controles de riesgos. Es necesario contar con un buen procedimiento para planificar la implantación de las medidas de control que sean precisas después de la evaluación de riesgos. Una vez identificados y valorados los riesgos, decidiremos sobre cuáles debemos intervenir en primer lugar. A este proceso lo denominamos priorización. En función del Grado de Peligrosidad o Grado de Riesgo se actuará prioritariamente sobre [6]:

- Los riesgos más severos.
- Ante riesgos de la misma severidad, actuar sobre los que tienen mayor probabilidad de ocurrencia.

- Ante riesgos que implican consecuencias muy graves y escasa probabilidad de ocurrencia, actuar antes, que sobre riesgos con mayor probabilidad de ocurrencia pero que implican consecuencias pequeñas.
- En función del número de trabajadores expuestos, actuar sobre los riesgos que afectan a un mayor número de trabajadores.
- En función del tiempo de exposición de los trabajadores al riesgo, actuar sobre aquellos riesgos a los que los trabajadores están expuestos durante más horas, dentro de su jornada laboral.

Capítulo 9

Identificación de amenazas

El análisis de las posibles amenazas es fundamental para cualquier negocio. A través de este análisis, se reconocen todos aquellos peligros a los que se enfrenta la organización. De esta manera, se pueden conocer los potenciales problemas que pueden surgir y el grado de seguridad existente para poder evitarlos. Una vez conocidas las amenazas que planean sobre la organización, se podrán estudiar los mecanismos de prevención y recuperación existentes para poder determinar si éstos son válidos o necesitan ser corregidos.
A continuación se muestra una lista de las posibles amenazas a las que nuestra empresa podría llegar a enfrentarse [13]:

- Cortes de corriente
- Cortes de comunicación
- Fallo de Hardware
- Fallo de Software
- Seguridad de la información
- Seguridad física
- Incendio
- Inundación

La figura 9.1 muestra las principales amenazas a las que una empresa está expuesta. Para cada tipo de amenaza se indica, en porcentaje, el grado de peligrosidad [17].

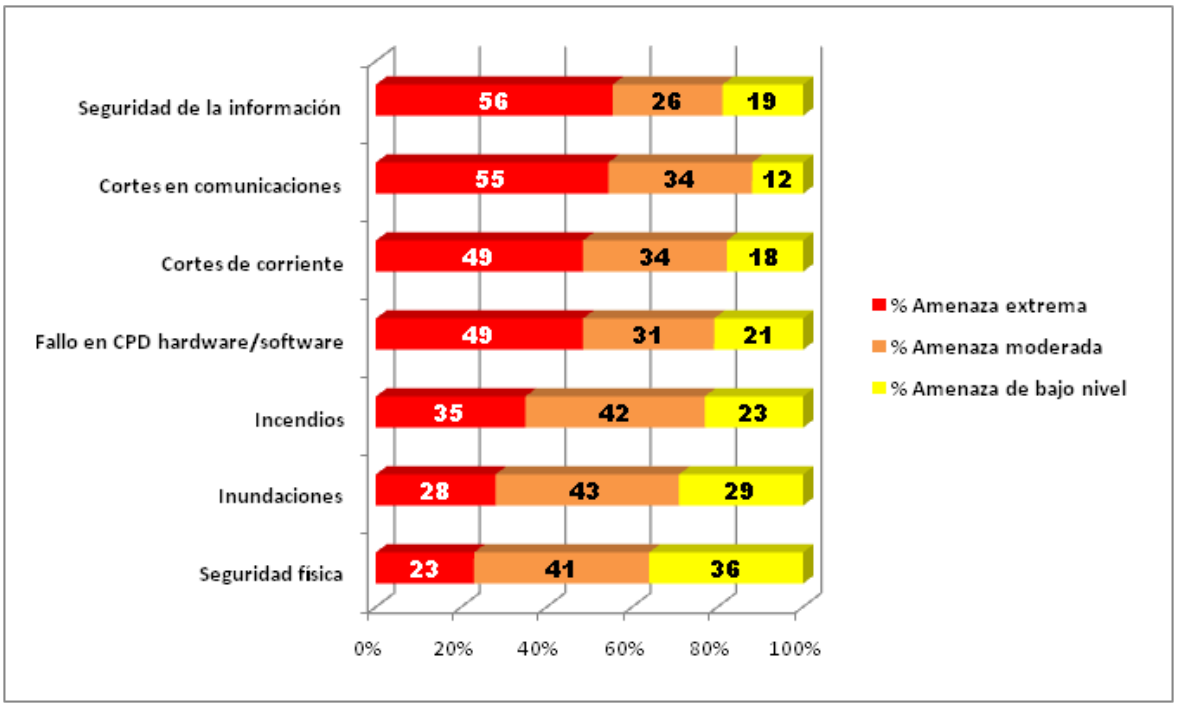


Figura 9.1: Identificación de Amenazas.

9.1. Cortes de corriente

Las causas más comunes que suelen provocar este tipo de contingencias son:

- Conmutaciones en la red eléctrica y fluctuaciones de tensión, como por ejemplo, picos de tensión.
- Averías en el suministro eléctrico.

9.2. Cortes en comunicaciones

Los cortes de comunicaciones son aquellas contingencias que impiden o interrumpen de forma más o menos prolongada la transmisión de datos o de voz. Es por tanto crítico para los procesos de negocio, la pérdida de comunicación eventual.

Las causas que suelen provocar este tipo de contingencias son la destrucción total o parcial de las infraestructuras telefónicas.

9.3. Fallo de Hardware

Un fallo de hardware es una de las contingencias más críticas que puede darse, ya que en caso de avería de un servidor podrían paralizarse varios de los procesos más importantes para el negocio. También tiene consecuencias secundarias graves como la pérdida de información de las bases de datos.

Si la avería se produce en equipos de trabajo, PC´s, entonces sería sería menos grave, pero podría impedir el trabajo de un técnico durante un tiempo determinado. Si se diese un error de hardware en periféricos también se retrasarían algunas funciones y podría rebajarse el nivel de servicio.

9.4. Fallo en Software

Los fallos de software pueden afectar a aplicaciones y datos de la organización, llegando a alterar e incluso parar procesos críticos del negocio. Hay una amplia gama de errores de software, entre los que destacan:

- Errores de programación: Aplicaciones, normalmente internas, con fallos graves de programación que son detectados en algún momento de la ejecución de éstas.
- Errores del sistema operativo: Son errores que suelen causar una interrupción involuntaria de la actividad en un PC o incluso en servidores.
- Errores en la gestión de cambios de software: La gestión de cambios abarca todas aquellas operaciones y protocolos que se llevan a cabo cuando es necesario realizar cambios en algún software.

9.5. Seguridad de la información

La seguridad informática es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta, incluyendo la información contenida. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo

lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas.

Las amenazas más conocidas son las siguientes [3]:

- Virus.
- Ataques de denegación de servicio, DoS.
- Intrusiones, hacking.

[18][19]

9.6. Incendio

Las causas principales que pueden provocar un incendio son:

- Eléctricas (cortocircuitos, líneas recalentadas, etc.) o chispas mecánicas de aparatos y cables en mal estado.
- Electricidad estática.

Las mencionadas a continuación han sido descartadas al quedar fuera del entorno de una empresa de telecomunicaciones.

- Cigarrillos y fósforos.
- Ignición espontánea.
- Chispas de combustión.
- Llamas abiertas.
- Soldadura.

9.7. Inundación

Las inundaciones en el lugar de trabajo pueden causar daños graves en los activos de la organización. Las causas más frecuentes suelen ser:

- Rotura de tuberías.
- Humedades.
- Filtraciones.
- Lluvias torrenciales.

9.8. Seguridad física

Se han contemplado estas amenazas por ser las más probables en el ámbito que se está tratando:

- Robo.
- Sabotaje.
- Terrorismo.

Capítulo 10

Evaluación del riesgo

El primer paso a la hora de evaluar el riesgo es realizar un análisis cuantitativo de los riesgos, estimando las pérdidas derivadas de la ocurrencia de una amenaza, el coste de implantación de medidas de prevención, control y recuperación y el beneficio que se conseguiría implantando estas medidas.

- Matriz de riesgos: Esta matriz representa las posibles amenazas, el riesgo asociada a éstas para cada grupo de activos, la valoración de las medidas de control existentes para cada amenaza y el riesgo residual resultante de las medidas de control para cada amenaza. El valor del riesgo residual determina de manera relativa las vulnerabilidades existentes respecto a las distintas amenazas [20].

10.1. Matriz de evaluación de riesgos

Para realizar el segundo paso del proceso ORM se puede utilizar una matriz de evaluación de riesgos. Con la matriz se cuantifican y priorizan los riesgos, aunque no reduce la naturaleza subjetiva de la gestión de los mismos. Sin embargo, una matriz proporciona un marco consistente para evaluar el riesgo.

Aunque las matrices pueden ser usadas para distintas aplicaciones, cualquier herramienta de gestión del riesgo debería incluir los elementos de "severidad del peligro" que también llamaremos impacto y la "probabilidad de accidente".

La RAC o Risk Assessment Matrix que utilizaremos representa el grado de riesgo asociado al peligro, considerando estos dos elementos además del grado de exposición. Mientras que el grado de riesgo es subjetivo en la naturaleza, la RAC sí refleja de forma más exacta la cantidad relativa de riesgo percibido entre varios peligros.

La matriz analiza los riegos totales y residuales para cada amenaza y tipo de activo. Para cada amenaza, se indica una probabilidad de que dicha amenaza pueda llegar a concretarse. Esta medida es una aproximación.

Para cada uno de los tipos de activos a proteger, se establece un importe aproximado de la pérdida media que ocasionaría esa amenaza en todos los activos clasificados según ese tipo. A ese valor se le conoce como impacto de la amenaza.

Posteriormente, se calcula el valor del riesgo total para cada amenaza, multiplicando la probabilidad de que ocurra dicha amenaza por el impacto sobre cada tipo de activo y por la exposición. De esta forma, se conoce el valor que acarrearía a la organización la materialización de cada amenaza.

Después de calcular el riesgo total, se establece el porcentaje de la efectividad del control. Esto es, el porcentaje del riesgo total que se mitigaría con la medida o medidas de control y prevención que existen para reducir los efectos probables de la ocurrencia de una amenaza. Finalmente, se calcula el valor del riesgo residual, que consiste en aplicar la efectividad del control al riesgo total [8].

10.2. Cortes de corriente

Las causas principales que provocan cortes en la corriente son varias, entre las más habituales se encuentran:

- Los apagones originados por exceso de consumo de electricidad en verano, por el uso de aparatos de aire acondicionado y aquellos provocados por tormentas o hielo que se acumula en las lineas de alta tensión. El hecho de que haga mucho calor o nieve algún día del año, no implica que se produzca un corte de corriente, por tanto, se asigna un

factor de exposición “irregular“ y de probabilidad “posible“. De media, en Europa, la duración de los mismos no suele ser superior a los 12 minutos [9], es decir, impacto moderado.

- Caída de tensión persistente, provocada por la ruptura de cables subterráneos o por alguna avería en el suministro eléctrico. Tiene un impacto mayor en el negocio ya que el suministro eléctrico queda interrumpido hasta la reparación de la línea.

- Cuando la la corriente queda restablecida, pueden producirse picos de tensión que dañarán los equipos en caso de que no estén protegidos, esto tendría un impacto muy alto si muchos de los equipos fueran dañados.

Cortes de corriente				
Amenaza	Impacto	Probabilidad	Exposición	F. de Riesgo
Apagones	15	3	2	**90**
Caídas de tensión persistente	15	3	2	**90**
Picos de tensión	15	3	3	**135**

Cuadro 10.1: Matriz de Riesgo Inherente: Cortes de corriente.

10.3. Cortes en comunicaciones o Downtime

Las causas que pueden provocar un corte en las comunicaciones son diversas, bugs, mal funcionamiento de los equipos y otras. En muchos casos es debido a altas tasas de error de bit, sobrecargas en la capacidad del canal, fallos en cadena, etc. Los cortes en comunicaciones también pueden ser programados, paradas previstas para realizar actualizaciones de software o ampliación de recursos. Las principales amenazas que se han considerado son las siguientes:

- Colapso por congestión en la red: Es el fenómeno producido cuando a la red (o a parte de ella) se le ofrece más tráfico del que puede cursar. Los paquetes se reciben demasiado deprisa para ser procesados (lo que produce que se llene la memoria de entrada). Además puede ser que en la memoria de salida haya demasiados paquetes esperando para ser atendidos, entonces se llena la memoria de salida, por tanto el nodo es incapaz de procesar toda la información que le llega, con lo que hará que se saturen las colas.

De producirse y consolidarse esta amenaza, el impacto sobre los usuarios sería muy alto, ya que quedarían sin servicio.

- Fallo en hardware/software de comunicaciones: Los problemas de software y hardware que están directamente relacionados con las redes de comunicaciones se incluyen en esta categoría. Éstos, acumulan más de un tercio de los fallos de las infraestructuras de telecomunicaciones.

  Para comprender mejor la naturaleza de este tipo de fallos es muy útil establecerlos en el contexto de modelo OSI. La figura 10.1 muestra la distribución de errores a lo largo de las capas del modelo OSI en redes de área local [11]. Las causas de fallos para las capas física y de red, son normalmente debidas a tarjetas de red defectuosas, cables y conexiones en mal estado, fallos en bridges, routers y switches, errores de checksum, y errores en el tamaño de paquetes.

  Con la evolución de las tecnologías de red, se han conseguido reducir los fallos en las capas inferiores, pero ha aumentado la tasa de fallos en la capa de aplicación, dada la complejidad del software.

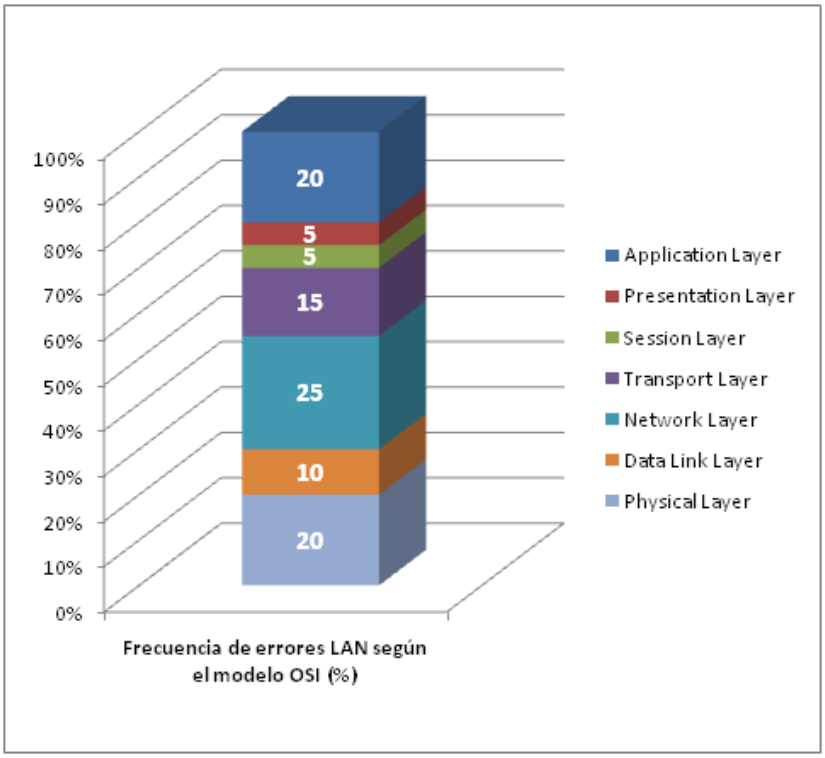


Figura 10.1: Frecuencia de errores en LAN según el modelo OSI.

- Destrucción de infraestructuras de telecomunciaciones: Tormentas, incendios, o incluso animales salvajes pueden provocar la destrucción de cables que obligarían a suspender el servicio.

Cortes en comunicaciones				
Amenaza	Impacto	Probabilidad	Exposición	F. de Riesgo
Congestión en la red	50	3	2	**300**
Fallo en hardware/software de comunicaciones	50	3	3	**450**
Destrucción de infraestructuras	5	10	3	**150**

Cuadro 10.2: Matriz de Riesgo Inherente: Cortes en comunicaciones.

10.4. Fallo en hardware

Los suministradores de equipos de telecomunicaciones aseguran que aproximadamente el 25 % de todos los fallos en una red de telecomunicaciones ocurren como resultado de problemas en el hardware, fallos en los equipos [11].

- Fallo de alimentación: La pérdida repentina de alimentación, es la mayor razón para los fallos en hardware. Si se produce un corte en la corriente mientras se trabaja con un equipo, se puede dañar el disco duro y perder la información.

- Fallo en memoria: Provocados por la falta de sistemas de detección y corrección de errores o conflictos de acceso a memoria provocados por los periféricos, que pueden derivar en también pérdida de información o corrupción de los datos.

- Fin de la vida útil: La vida útil de los componentes de hardware es limitada, cuando ésta se supera, la tasa de fallos aumenta de forma exponencial [16].

- Fallo en instalación: Tomas de corriente en mal estado, cables sueltos, o placas mal clavadas, son también motivo fallo en hardware,

Las consecuencias de los fallos en hardware son graves si no existen medidas. Si la información se pierde, no se puede volver a recuperar.

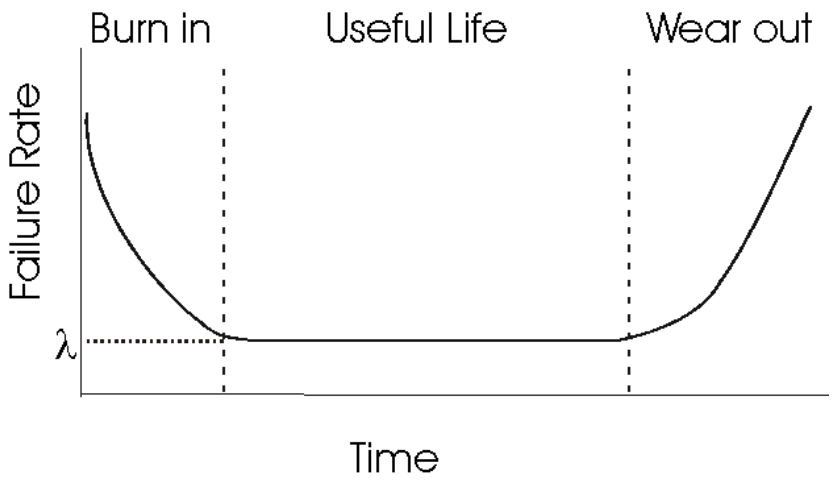


Figura 10.2: Curva de fiabilidad del hardware.

Fallo en hardware				
Amenaza	Impacto	Probabilidad	Exposición	F. de Riesgo
Fallo de alimentación	25	3	3	**225**
Fallo en memoria	25	3	3	**225**
Fallo en instalación	15	3	3	**135**

Cuadro 10.3: Matriz de Riesgo Inherente: Fallo en hardware.

10.5. Fallo en software

Hoy en día, las redes de las empresas conectan un gran número de servidores que proporcionan funcionalidad a multitud de usuarios que usan las aplicaciones de software. Los sistemas ampliamente distribuidos son habituales en empresas geográficamente dispersas. La red proporciona conectividad entre los clientes de plataformas diversas.

En sistemas de semejante complejidad, incluso con una planificación y una monitorización muy cuidadosas, es difícil predecir la demanda de servicios en la red.

Los fallos pueden originarse por falta de capacidad, retrasos excesivos durante períodos de exceso de demanda o incluso pueden ser debidos a fallos catastróficos provocados por la

pérdida de algún recurso que sea fundamental para para el funcionamiento del sistema.

Los problemas de software son aproximadamente iguales a los provocados por errores de hardware, un 25 % [11], entre ellos destacamos:

- Errores de programación: Los fallos originados en una red de telecomunicaciones debidos a fallos en software pueden ser provocados por diversos motivos, como fallos en la implementación de programas y su manejo.
- La instalación de actualizaciones de software: Tal y como indica la figura 10.3 [16], cada vez que se actualiza un programa aumenta la tasa de errores durante la vida útil del programa.
- Fallos en el sistema operativo: Las anomalías y fallos en los sistemas operativos son también causa fundamental de la caída de sistemas en entornos de comunicaciones.

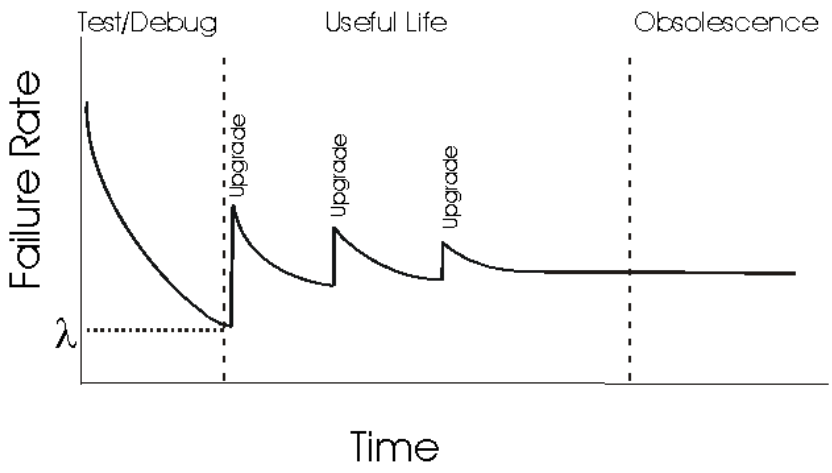


Figura 10.3: Curva de fiabilidad del software.

10.6. Seguridad de la información

Los términos seguridad en la red y seguridad de la información son habitualmente usados como sinónimos. El primero, se utiliza generalmente cuando se hace referencia al hecho de proporcionar protección dentro de los límites de una organización, manteniendo alejados a los intrusos (hackers). El segundo, se centra explícitamente en proteger los recursos de

Fallo en software				
Amenaza	Impacto	Probabilidad	Exposición	F. de Riesgo
Errores de programación	25	6	6	**900**
Problemas con las actualizaciones	15	6	3	**270**
Fallos en el sistema operativo	25	6	6	**900**

Cuadro 10.4: Matriz de Riesgo Inherente: Fallo en software.

la información, de los ataques de software nocivo, malware, o de los fallos provocados por miembros de la propia organización, por medio de técnicas de prevención de pérdida de datos.

La vulnerabilidad informática en las empresas es debida generalmente a fallos en la configuración de los programas, fallos en el software por una incorrecta implementación, como se verá más adelante, etc. En este apartado se tratarán los ataques más comunes a una organización:

- DoS: Ataque de denegación de servicio o Denial-of-Service. Es un ataque a un sistema de computadoras o red que causa que, un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima. Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le dice "denegación", pues hace que el servidor no dé a basto a la cantidad de usuarios [1].

- Virus: Se considera virus todo código malicioso insertado en el código fuente de cualquier aplicación. Un virus normalmente se introduce en el sistema cuando es ejecutado en éste al menos una vez, provocando alteraciones, pérdida de información o errores graves [19].

- Intrusiones, hacking: son aquellas personas que consiguen acceder a los datos o programas de los cuales no tienen acceso permitido (cracker, defacer, script kiddie o Script boy, viruxer, etc.).

Seguridad de la información				
Amenaza	Impacto	Probabilidad	Exposición	F. de Riesgo
Virus	50	6	10	**3000**
DoS	50	6	10	**3000**
Intrusiones, hacking	50	6	10	**3000**

Cuadro 10.5: Matriz de Riesgo Inherente: Seguridad de la información.

10.7. Seguridad física

- Robo: Los robos son aquellas acciones perpetradas por empleados o por personas ajenas a la organización para quedarse en propiedad activos pertenecientes a la empresa.

  El mayor peligro de estas de amenazas son los robos de datos sensibles de clientes de la organización, ya que esto no sólo supondría una pérdida económica inmediata, sino que además llevaría a una pérdida de prestigio muy importante y a una disminución de la cartera de clientes potenciales.

- Sabotaje: El sabotaje incluye todo tipo de daños intencionados realizados en los activos o procesos de la organización, realizados normalmente por alguna persona propia de la organización, a fin de perjudicar los intereses de la empresa.

  Las causas más comunes suelen ser actos de venganza o de reivindicación por parte de trabajadores despedidos o descontentos con la propia empresa.

- Terrorismo: Son acciones llevadas a cabo por personas ajenas a la organización que atentan contra la integridad de los empleados y de los activos de la empresa. Las causas de las acciones terroristas suelen ser políticas.

Seguridad física				
Amenaza	Impacto	Probabilidad	Exposición	F. de Riesgo
Robo	50	3	3	**450**
Sabotaje	25	3	2	**150**
Terrorismo	100	3	3	**900**

Cuadro 10.6: Matriz de Riesgo Inherente: Seguridad física.

10.8. Incendio

Los causas principales por las que se puede producir un incendio son:

- Eléctricas: Cortocircuitos debidos a cables gastados, tomas de corrientes defectuosas, etc. Líneas recargadas, que se recalientan por excesivos aparatos eléctricos conectados y/o por gran cantidad de derivaciones en las líneas, sin tener en cuenta la capacidad eléctrica instalada, mal mantenimiento de los equipos eléctricos, etc.

- Electricidad estática: Muchas operaciones industriales generan electricidad estática. Cuando no existen conexiones a tierra, y la humedad relativa del aire es baja, (inferior a 40 %), ésta se descarga en forma de chispas, que en contacto con vapores o gases inflamables u otros materiales combustibles, generan un incendio o una explosión.

Incendio				
Amenaza	Impacto	Probabilidad	Exposición	F. de Riesgo
Eléctricas	100	3	2	**600**
Electricidad estática	100	3	2	**600**

Cuadro 10.7: Matriz de Riesgo Inherente: Incendio.

10.9. Inundación

Las inundaciones en el lugar de trabajo pueden causar daños graves en los activos de la organización. Las causas más frecuentes suelen ser:

- Rotura de tuberías: La falta de mantenimiento en los edificios de la compañía puede tener graves efectos sobre los activos, pudiendo inutilizar gran cantidad de equipos electrónicos.
- Filtraciones.
- Lluvias torrenciales: A pesar de su escasa probabilidad, su impacto, en caso de producirse, es muy elevado, sobre todo, si en las dependencias de la empresa que se encuentran en sótanos o al nivel del suelo.

Inundación				
Amenaza	Impacto	Probabilidad	Exposición	F. de Riesgo
Rotura de tuberías	100	3	1	**300**
Filtraciones	15	6	1	**90**
Lluvias torrenciales	100	1	1	**100**

Cuadro 10.8: Matriz de Riesgo Inherente: Inundación.

Capítulo 11

Análisis de medidas de control de riesgo

Estudio de vulnerabilidades: A partir de la fase anterior, se determinan los puntos débiles de la Organización para cada amenaza existente, se analizan las posibles medidas de salvaguarda a implantar.

11.1. Cortes de corriente

Los cortes de corriente pueden dejar parados los procesos de negocio de la organización durante el tiempo que éstos duran. Además, pueden producir otros efectos colaterales, como son la pérdida de información o la inestabilidad en los sistemas. Existen una serie de medidas preventivas instaladas y otras medidas para paliar los posibles efectos de la ocurrencia de una incidencia de este tipo, que son:

- Sistema de alimentación ininterrumpida (SAI), para los servidores situados en los CPD (centros de procesamiento de datos).
- Mantenimiento del sistema eléctrico.
- Protector de sobre-tensión para proteger a los equipos de los picos de corriente.

Normalmente, los cortes de corriente en una organización se dan por averías o fallos del suministro eléctrico, y no suelen ser de larga duración. Por tanto, se ha considerado un alto porcentaje de eficacia de las medidas protectoras contra los cortes de corriente, ya que la mayor parte de cortes de corriente de corta duración se resuelven mediante el uso de los sistemas

de alimentación ininterrumpida. Se proponen otras medidas alternativas o complementarias para asegurar una mayor eficacia en la prevención y control de los cortes de corriente:

- Sistemas de generación de energía de reserva activados por motores (para cortes de larga duración).
- Establecer un suministro de energía independiente.

La tabla 11.1 muestra la asignación de medidas de control de riesgo entre las mencionadas anteriormente, con su correspondiente factor de coste. Se ha suprimido de la lista las caídas transitorias por su bajo factor de riesgo.
En el cuadro 11.2 se muestra la matriz de riesgo residual tras la implantación de las medidas.

Asignación: Cortes de corriente		
Amenaza	Medida	Factor de coste
Apagones	Suministro independiente de energía	6
	Sistema de generación de energía de reserva	3
	Total	**9**
Caídas de tensión persistente	Mantenimiento del sistema eléctrico	3
	SAI	2
	Total	**5**
Picos de tensión	Protector de sobre-tensión	2
	Total	**2**

Cuadro 11.1: Asignación de medidas: Cortes de corriente.

Riesgo residual: Cortes de corriente				
Amenaza	Impacto	Probabilidad	Exposición	F. de Riesgo
Apagones	1	1	15	**15**
Caídas de tensión persistente	1	1	15	**15**
Picos de tensión	1	1	15	**15**

Cuadro 11.2: Matriz de Riesgo Residual: Cortes de corriente.

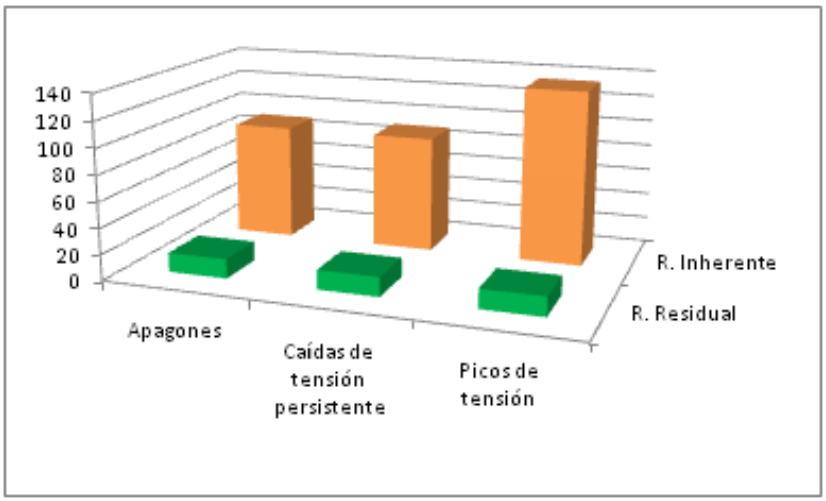


Figura 11.1: Comparación entre Riesgo Inherente y Residual: Cortes de corriente.

La tabla 11.3 representa el porcentaje de riesgo reducido tras la implantación de las medidas de mitigación.

G.C.: Cortes de corriente				
Amenaza	R.I.	R.R.	%	G.C.
Apagones	90	15	83,33	2
Caídas de tensión persistente	90	15	83,33	2
Picos de tensión	135	15	88,89	2

Cuadro 11.3: Grado de corrección: Cortes de corriente.

11.2. Cortes de comunicaciones

Las técnicas de gestión del riesgo utilizadas para mitigar el impacto provocado por una caída en el sistema de comunicaciones, comienzan por invertir en componentes de calidad. La compra de componentes fiables garantiza una reducción en la probabilidad de materialización de una amenaza.

Es importante contar con equipos redundantes, así se hace posible que en caso de materializarse una amenaza, el tiempo de pérdida de servicio sea mínimo. Es fundamental para minimizar la probabilidad de que se produzca una caída de la red, que ésta esté bien diseñada,

ya que en caso de producirse, un sistema bien diseñado reducirá los efectos de la caída, teniendo localizados los puntos de fallo para poder solucionar el problema lo antes posible.
El sistema tiene que estar preparado para localizar fallos en el funcionamiento, a través de un sistema de monitorización de la red y restablecer el funcionamiento a condiciones normales de trabajo. Ésto generalmente implica la existencia de un equipo de trabajo dedicado a la gestión y mantenimiento de la red, formado por ingenieros y por personal de mantenimiento.
Un sistema de gestión de red también puede ser utilizado para detectar componentes en mal estado o que no funcionen, con el objetivo de anticiparse a las quejas de los clientes.

Entre las medidas propuestas se han asignado para cada amenaza las del cuadro 11.4.
En el cuadro 11.5 se muestra la matriz de riesgo residual tras la implantación de las medidas.

Asignación: Cortes en com.		
Amenaza	Medida	Factor de coste
Congestión en la red	Monitorización	2
	Planificación de rutas alternativas	3
	Total	**5**
Fallo en hardware/software de comunicaciones	Mantenimiento de equipos	3
	Redundancia de equipos	4
	Total	**7**
Destrucción de infraestructuras	Mantenimiento de infraestructuras	3
	Total	**3**

Cuadro 11.4: Asignación de medidas: Cortes en comunicaciones.

Riesgo residual: Cortes en comunicaciones				
Amenaza	Impacto	Probabilidad	Exposición	F. de Riesgo
Congestión en la red	5	1	2	**10**
Fallo en hardware/software de comunicaciones	1	3	2	**6**
Destrucción de infraestructuras	1	1	1	**1**

Cuadro 11.5: Matriz de Riesgo Residual: Cortes en comunicaciones.

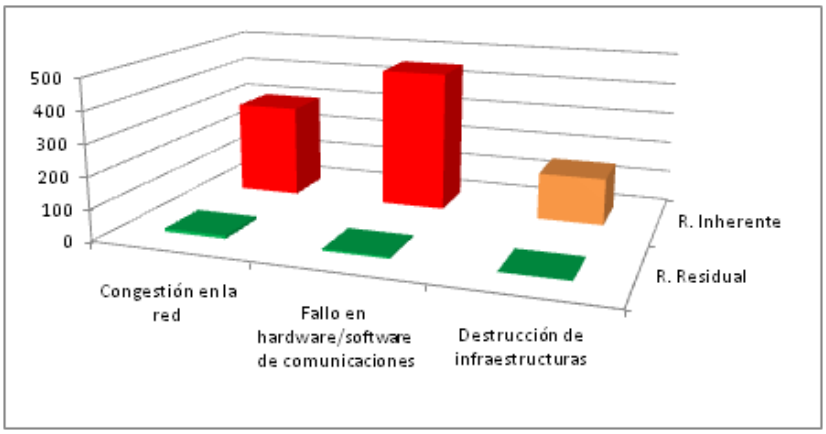


Figura 11.2: Comparación entre Riesgo Inherente y Residual: Cortes en comunicaciones.

La tabla 11.6 representa el porcentaje de riesgo reducido tras la implantación de las medidas de reducción y mitigación.

G.C.: Cortes en comunicaciones				
Amenaza	R.I.	R.R.	%	G.C.
Congestión en la red	300	10	96,67	2
Fallo en hardware/software de comunicaciones	450	6	98,67	2
Destrucción de infraestructuras	150	1	99,33	1

Cuadro 11.6: Grado de corrección: Cortes en comunicaciones.

11.3. Fallo en Hardware

El fallo físico del disco duro de un ordenador o fallos en otros componentes del hardware, son las razones más evidentes por las cuales son necesarias las copias de seguridad o backups. No hay hecho más claro para comprender la necesidad de copias de seguridad que haber sufrido una pérdida irrecuperable provocada por un fallo en el hardware. Dado que el disco duro del ordenador almacena todos los datos de valor y los programas, es el componente cuyo fallo nos afectará más.

Para mejorar la fiabilidad total del hardware en los sistemas de telecomunicaciones, los fabricantes proporcionan redundancia a sus productos. Un diseñador de redes puede elegir

y desarrollar equipamiento con un cierto grado de opciones de redundancia. Hoy en día es posible obtener en el mercado componentes hardware para equipos de telecomunicaciones capaces de proporcionar MTBS desde 80.000 horas hasta varios cientos de miles de horas [10].

En el desarrollo actual de las redes de telecomunicaciones las variaciones van más allá de los componentes elegidos. Estas variaciones incluyen la calidad de los equipos utilizados, la calidad de la planificación y del diseño de la red y la complejidad de la implementación. Para contrarrestar el posible efecto de la ocurrencia de un fallo de hardware se han decidido las siguientes medidas:

- Contratos de mantenimiento de equipos informáticos, servidores, impresoras, escáneres, monitores, switches y otros periféricos por parte del suministrador de hardware.

- Provisión de recursos de hardware de sustitución para poder trabajar si la reparación de un recurso es de larga duración.

- Replicación de la información de los PCs en discos de los servidores con frecuencia semanal.

- Realización de copias de seguridad de los discos de los servidores.

El proveedor de recursos hardware de la organización se encarga de las reparaciones de los equipos en garantía y la sustitución de los que no admiten reparación. Otras posibles medidas para mejorar la eficacia en la prevención y control de los fallos de hardware son:

- Almacenamiento de las copias de seguridad de los discos de los servidores en un lugar alejado del centro, granjas de ordenadores, etc.

La asignación de medidas de control de riesgo para la protección del hardware se ha realizado según indica el cuadro 11.7.

En el cuadro 11.8 se muestra la matriz de riesgo residual tras la implantación de las medidas.

Asignación: Fallo en hardware		
Amenaza	Medida	Factor de coste
Desgaste o Fallo de alimentación	Mantenimiento de equipos	4
	Provisión de recursos de hardware	4
	Total	**8**
Fallo en memoria	Backups o copias de seguridad	3
	Provisión de recursos de hardware	4
	Total	**7**
Fallo en instalación	Mantenimiento de equipos	2
	Total	**2**

Cuadro 11.7: Asignación de medidas: Fallo en hardware.

Riesgo residual: Fallo en hardware				
Amenaza	Impacto	Probabilidad	Exposición	F. de Riesgo
Fallo de alimentación	5	1	1	**5**
Fallo en memoria	5	1	1	**5**
Fallo en instalación	15	1	1	**15**

Cuadro 11.8: Matriz de Riesgo Residual: Fallo en hardware.

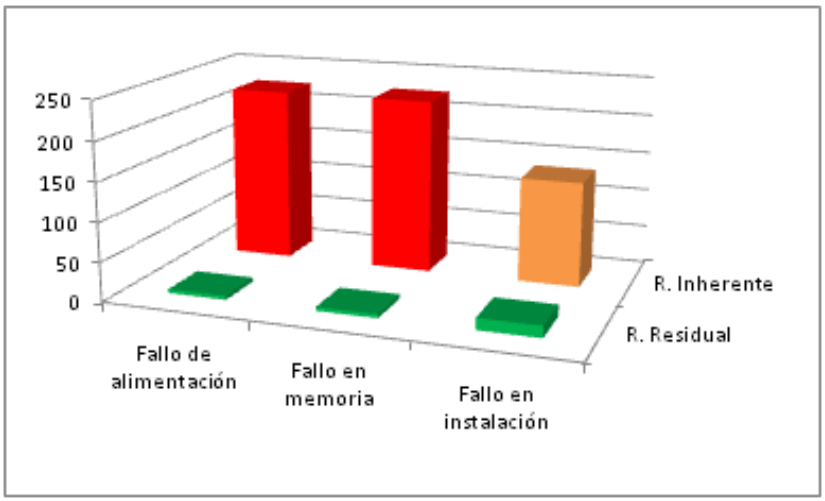


Figura 11.3: Comparación entre Riesgo Inherente y Residual: Fallo en Hardware.

La tabla 11.9 representa el porcentaje de riesgo reducido tras la implantación de las medidas de reducción y mitigación.

G.C.: Fallo en hardware				
Amenaza	R.I.	R.R.	%	G.C.
Fallo de alimentación	225	5	97,78	2
Fallo en memoria	225	5	97,78	2
Fallo en instalación	135	15	88,89	2

Cuadro 11.9: Grado de corrección: Fallo en hardware.

11.4. Fallo de Software

Entre las posibles opciones para mitigar los fallos en el software disponemos de las siguientes:

- Cambios evolutivos en las aplicaciones: Extensión o reducción de las funcionalidades de una aplicación.
- Cambios correctivos en las aplicaciones: Pequeñas modificaciones realizadas en un software para corregir posibles errores o comportamientos.
- Instalación de aplicaciones: Implantación de software de nuevo uso en el sistema.

Otras posibles medidas para la previsión y el control de los errores de software son:

- Protocolo para la gestión de cambios: Existe un protocolo para poner en funcionamiento cualquier cambio en aplicaciones instaladas (actualización de versiones, parches, instalación de aplicaciones nuevas, etc.). Antes de realizar la gestión de cambios directamente en un entorno de producción, se realizará un simulacro en un entorno de pruebas.

- Entorno de pruebas fiable, con una configuración similar al entorno de producción.

- Utilizar únicamente software de confianza. Control de licencias.

- Política de administración de máquinas: Los empleados que tengan perfil de técnico en las máquinas, no podrán instalar aplicaciones en sus PCs. Únicamente el responsable del Departamento de Desarrollo puede acceder como administrador local a todos los ordenadores e instalar aplicaciones nuevas.

Estas medidas aseguran en un buen porcentaje, la prevención de errores de software. Además también se podría:

- Establecer un procedimiento para controlar los accesos a los servidores de aplicaciones, mediante ficheros de log, que deberán ser revisados periódicamente por el encargado del Departamento de Desarrollo.

- Poner en funcionamiento un departamento de calidad, o al menos un encargado, que realice las funciones de control de las aplicaciones instaladas, supervisión de la gestión de cambios y de la documentación de todas las aplicaciones instaladas en la organización.

La tabla 11.10 muestra la asignación de medidas de control de riesgo para software de entre las propuestas anteriormente.
En el cuadro 11.11 se muestra la matriz de riesgo residual tras la implantación de las medidas.

Asignación: Fallo en software		
Amenaza	Medida	Factor de coste
Errores de programación	Utilizar software de confianza	2
	Control de aplicaciones instaladas	2
	Total	**4**
Problemas con las actualizaciones	Protocolo para gestión de cambios	1
	Total	**1**
Fallos en el sistema operativo	Utilizar software de confianza	2
	Protocolo para la gestión de cambios	1
	Total	**3**

Cuadro 11.10: Asignación de medidas: Fallo en software.

Riesgo residual: Fallo en software				
Amenaza	Impacto	Probabilidad	Exposición	F. de Riesgo
Errores de programación	25	1	2	**50**
Problemas con las actualizaciones	25	1	2	**50**
Fallos en el sistema operativo	25	1	2	**50**

Cuadro 11.11: Matriz de Riesgo Residual: Fallo en software.

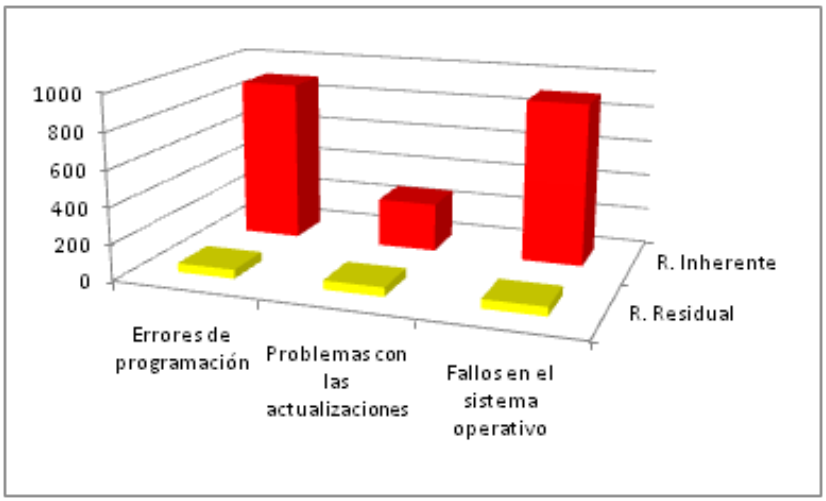


Figura 11.4: Comparación entre Riesgo Inherente y Residual: Fallo en software.

La tabla 11.12 representa el porcentaje de riesgo reducido tras la implantación de las medidas de reducción y mitigación.

G.C.: Fallo en software				
Amenaza	R.I.	R.R.	%	G.C.
Errores de programación	900	50	94,44	2
Problemas con las actualizaciones	270	50	81,48	2
Fallos en el sistema operativo	900	50	94,44	2

Cuadro 11.12: Grado de corrección: Fallo en software.

11.5. Seguridad de la información

A la hora de proteger la información de la empresa existe un conjunto de requisitos que se deben garantizar:

- Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no les correspondan (sin una supervisión minuciosa).

- Asegurar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido.

- Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro.

- Asegurar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.

- Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.

- Actualizar constantemente las contraseñas de accesos a los sistemas de cómputo [3].

Para asegurar dichos las condiciones anteriores, existen una serie de medidas preventivas:

- Antivirus: Es una herramienta centralizada que permite controlar y administrar la protección contra amenazas de toda la red. Permite la monitorización en tiempo real de todos los elementos de esta red para poder controlar en cualquier momento las posibles infecciones de malware.

- Actualizaciones antivirus: La herramienta anterior actualiza cada hora su catálogo de malware de forma automática.

- Medidas contra ataques externos: Los firewalls y el uso de proxies actúan como muro de protección contra ataques externos.

- Normas y procedimientos de seguridad, control de acceso: No está permitida la ejecución de programas que no vengan de una fuente de confianza.No está permitida la instalación de aplicaciones en los equipos por los técnicos informáticos. Será el Responsable de Desarrollo quién realice esta función para todos los equipos.

Las medidas tomadas para proteger a la empresa de ataques informáticos se muestra en el cuadro 11.13.
En el cuadro 11.14 se muestra la matriz de riesgo residual tras la implantación de las medidas.

Asignación: Seguridad de la información		
Amenaza	Medida	Factor de coste
Virus	Antivirus	1
	Total	**1**
DoS	Firewalls	1
	Application front end hardware	1
	Proxies	1
	Total	**3**
Intrusiones, hacking	Control de acceso a datos	2
	Total	**2**

Cuadro 11.13: Asignación de medidas: Seguridad de la información.

Riesgo residual: Seguridad de la inf.				
Amenaza	Impacto	Probabilidad	Exposición	F. de Riesgo
Virus	5	1	10	**50**
DoS	5	1	10	**50**
Intrusiones, hacking	5	1	10	**50**

Cuadro 11.14: Matriz de Riesgo Residual: Seguridad de la información.

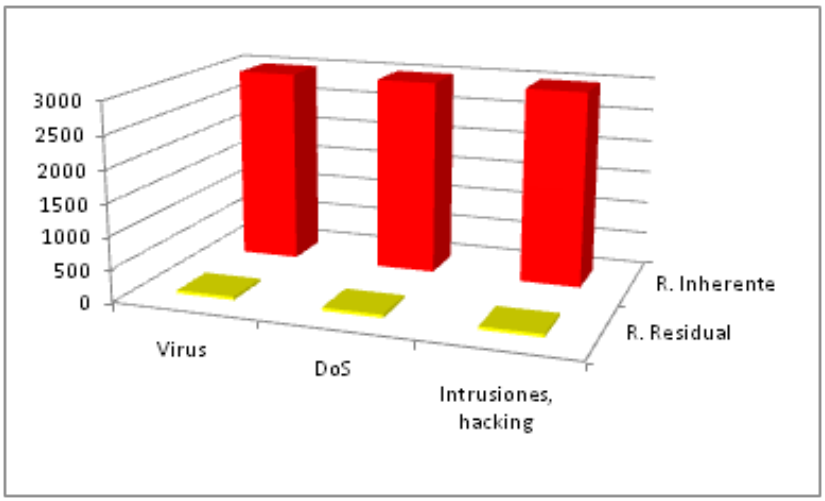


Figura 11.5: Comparación entre Riesgo Inherente y Residual: Seguridad de la información.

La tabla 11.15 representa el porcentaje de riesgo reducido tras la implantación de las medidas de reducción y mitigación.

G.C.: Seguridad de la información				
Amenaza	R.I.	R.R.	%	G.C.
Virus	3000	50	98,33	2
DoS	3000	50	98,33	2
Intrusiones, hacking	3000	50	98,33	2

Cuadro 11.15: Grado de corrección: Seguridad de la información.

11.6. Seguridad física

En la actualidad, se han constatado una serie de medidas para evitar y minimizar los riesgos y efectos de posibles robos o sabotajes:

- Sistemas de vigilancia y seguridad:
  - Control de accesos: Una empresa de seguridad que se encargue del control y supervisión de los accesos a los inmuebles de la organización.
  - Sistemas de seguridad: Cámaras conectadas en circuito cerrado, que vigilan y controlan el acceso a las oficinas. Las imágenes recogidas son almacenadas y tratadas

por las empresas de seguridad contratadas.

- Instalar sistemas de prevención de robos de datos en los equipos por medio de USB. Existen herramientas software que impiden que se ejecute el auto arranque de los dispositivos USB.

- Políticas de seguridad:

  - Distribución de contraseñas de bases de datos únicamente a los responsables de dichas bases de datos.
  - Restringir los accesos a información de tipo sensible sólo a las personas que estrictamente sean necesarias.
  - Protocolo de actuación en caso de abandono de empleado: En caso de despido o baja voluntaria de un empleado, establecer una serie de actuaciones a realizar respecto a su equipo de trabajo y usuarios asignados.
    - Reclamar al empleado saliente todo aquél material de la empresa que pudiera tener prestado para realizar sus funciones (móvil de empresa, material de oficina, etc.).
    - Entrega de la tarjeta de entrada a las oficinas del empleado a la empresa de seguridad para su desactivación y destrucción.
    - Eliminar claves de acceso del usuario, contraseñas, cuentas de correo, cuenta de usuario en el dominio, etc.
    - Hacer una copia de seguridad de los discos duros del equipo de trabajo del empleado y guardarla en sitio seguro.
    - Formatear el PC del empleado y realizar un clonado con una maqueta para dejarlo disponible a una nueva incorporación.
  - Publicar un código o protocolo de buen uso de las herramientas informáticas dentro de la empresa, que delimite el uso que pueden hacer de éstas los empleados.
  - Existencia de una cláusula contractual que deben firmar los trabajadores de la empresa por la cual, se comprometen a hacer un buen uso de los materiales y tecnologías de la organización.

Estas medidas parecen razonables para evitar en gran medida los robos de equipos hardware o el sabotaje de los mismos. En este caso, los mecanismos de protección para los tres tipos

de amenaza son los mismos, como muestra el cuadro 11.16.

En el cuadro 11.17 se muestra la matriz de riesgo residual tras la implantación de las medidas.

Asignación: Seguridad física		
Amenaza	Medida	Factor de coste
Robo + Sabotaje + Terrorismo	Control de acceso, sistemas de autenticación	2
	Sistemas de vigilancia y seguridad	2
	Políticas de seguridad con los empleados	1
	Total	**5**

Cuadro 11.16: Asignación de medidas: Seguridad física.

Riesgo residual: Seguridad física				
Amenaza	Impacto	Probabilidad	Exposición	F. de Riesgo
Robo	5	1	2	**10**
Sabotaje	5	1	2	**10**
Terrorismo	15	1	1	**15**

Cuadro 11.17: Matriz de Riesgo Residual: Seguridad física.

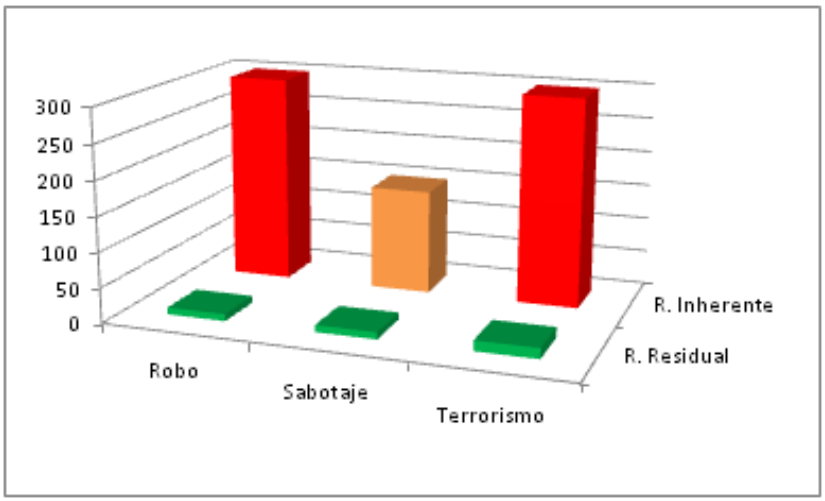


Figura 11.6: Comparación entre Riesgo Inherente y Residual: Seguridad física.

La tabla 11.18 representa el porcentaje de riesgo reducido tras la implantación de las medidas de reducción y mitigación.

G.C.: Seguridad física				
Amenaza	R.I.	R.R.	%	G.C.
Robo	300	10	96,67	2
Sabotaje	150	10	93,33	2
Terrorismo	300	15	95,00	2

Cuadro 11.18: Grado de corrección: Seguridad física.

11.7. Incendio

Un incendio puede provocar la destrucción o inutilización total de los activos que se ven afectados por él. Las medidas que existen actualmente en la organización para la prevención y paliación de los efectos de un incendio son:

- Aparatos de detección de humos situados en los techos de cada una de las salas de las sedes de la organización.
- Extintores situados en algunas salas, regulados y con las correspondientes revisiones en orden.
- Normas sobre situaciones de incendio.
- Formación del personal sobre situaciones de emergencia.

Estas medidas, aunque correctas y necesarias, no son suficientes para evitar o minimizar el riego de un incendio dentro las oficinas. Otras medidas de prevención y control anti-incendios contempladas son:

- Revisiones periódicas de las instalaciones eléctricas existentes (tomas de corriente, aparatos eléctricos obsoletos, etc.).
- Sistemas de detección y extinción automática de incendios, sprinklers (rociadores).
- Responsable de Seguridad con formación anti-incendios.

- Materiales de seguridad anti-incendios almacenados en un lugar estratégico.

- Señalización y almacenamiento de recipientes con materiales inflamables.

El cuadro 11.19 muestra las medidas tomadas para minimizar el impacto de un posible incendio.

En el cuadro 11.20 se muestra la matriz de riesgo residual tras la implantación de las medidas.

Asignación: Incendio		
Amenaza	Medida	Factor de coste
Incendio	Aparatos de detección de humo	1
	Sprinklers y sistemas de extinción	1
	Revisiones periódicas de las instalaciones	1
	Total	**3**

Cuadro 11.19: Asignación de medidas: Incendio.

Riesgo residual: Incendio				
Amenaza	Impacto	Probabilidad	Exposición	F. de Riesgo
Eléctricas	1	0,5	2	**1**
Electricidad estática	1	0,5	2	**1**

Cuadro 11.20: Matriz de Riesgo Residual: Incendio.

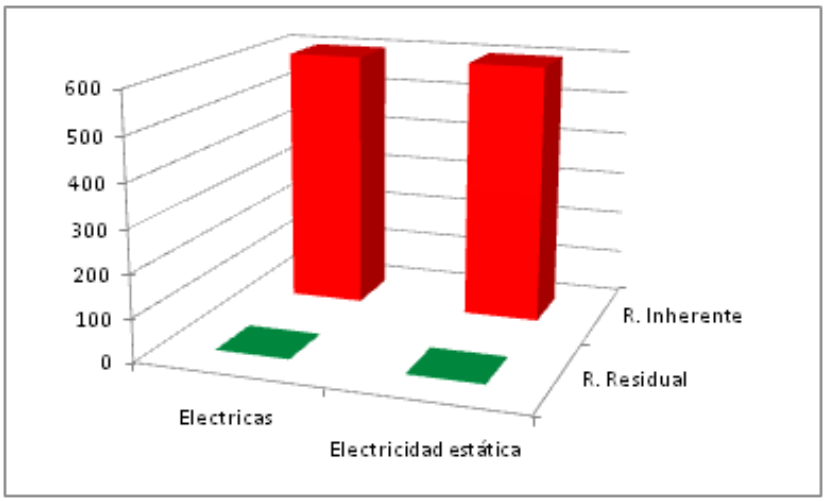


Figura 11.7: Comparación entre Riesgo Inherente y Residual: Incendio.

La tabla 11.21 representa el porcentaje de riesgo reducido tras la implantación de las medidas de reducción y mitigación.

G.C.: Incendio				
Amenaza	R.I.	R.R.	%	G.C.
Eléctricas	600	1	99,83	1
Electricidad estática	600	1	99,83	1

Cuadro 11.21: Grado de corrección: Incendio.

11.8. Inundación

Las inundaciones en el lugar de trabajo pueden causar daños graves en los activos de la organización. Con el fin de minimizar el impacto frente a posibles inundaciones se han decidido tomar las siguientes precauciones:

- Normas sobre situaciones de inundación.
- Formación del personal para casos de emergencia.
- Revisión cada cierto tiempo del estado de desagües y sumideros.
- Traslado de equipos a otras dependencias no situadas a nivel de sótano.

Las medidas tomadas se muestran en el cuadro 11.22.

En el cuadro 11.23 se muestra la matriz de riesgo residual tras la implantación de las medidas.

Asignación: Inundación		
Amenaza	Medida	Factor de coste
Rotura de canalizaciones	Mantenimiento periódico	1
	Conservar temperatura en días fríos	1
	Total	**2**
Filtraciones	Mantenimiento periódico	1
	Total	**1**
Lluvias torrenciales	Normas sobre situaciones de inundación	1
	No ubicar equipos en sótanos o bajos	1
	Revisiones periódicas de desagües y sumideros	1
	Total	**3**

Cuadro 11.22: Asignación de medidas: Inundación.

Riesgo residual: Inundación				
Amenaza	Impacto	Probabilidad	Exposición	F. de Riesgo
Rotura de tuberías	50	1	1	**50**
Filtraciones	5	0,5	1	**3**
Lluvias torrenciales	50	1	1	**50**

Cuadro 11.23: Matriz de Riesgo Residual: Inundación.

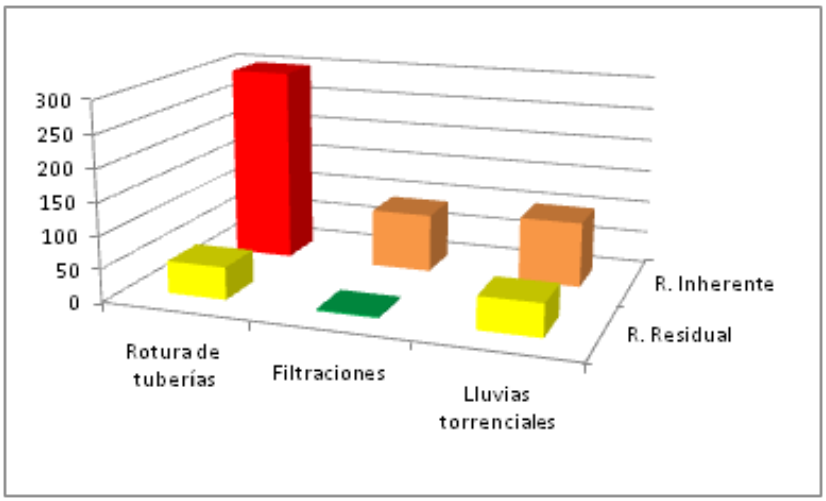


Figura 11.8: Comparación entre Riesgo Inherente y Residual: Inundación.

La tabla 11.24 representa el porcentaje de riesgo reducido tras la implantación de las medidas de reducción y mitigación.

G.C.: Inundación				
Amenaza	R.I.	R.R.	%	G.C.
Rotura de tuberías	300	50	83,33	2
Filtraciones	90	3	97,22	2
Lluvias torrenciales	100	50	50,00	3

Cuadro 11.24: Grado de corrección: Inundación.

Capítulo 12

Implementación de decisiones de control

En este paso se determinan cuáles de las medidas propuestas deben de ser implantadas finalmente en la empresa para mejorar la seguridad sin comprometer la economía de la organización innecesariamente. La finalidad de este método es conseguir mejorar la política de seguridad de la organización de una forma sostenible y responsable.

rEn primer lugar, es necesario nombrar un responsable de seguridad, que será responsable de supervisar y organizar aquellas tareas destinadas a prevenir, controlar y poner en marcha los planes de acción en caso de emergencia. Sus competencias serían las siguientes:

- Realizar una evaluación de riesgos.
- Asesorar sobre medidas de seguridad.
- Desarrollar procedimientos.
- Supervisar la administración y las políticas de seguridad.
- Ser el contacto con consultores y proveedores externos en materia de seguridad.

A continuación se detallan las medidas a implantar para cada tipo de amenaza.

12.1. Cortes de corriente

Los cortes de corriente suponen una parada temporal de los servicios de la organización durante el tiempo que dura éste. Pueden ocasionar, además, la pérdida de datos y fallos

graves de los procesos de negocio.

Como se puede observar en el cuadro 12.1, la implantación de medidas para la protección frente caídas de tensión transitorias y picos de tensión está justificada, principalmente porque con la adquisición de elementos tales como SAI´s o protectores de sobre-tensión, cuyo precio es asequible, se obtiene una elevada protección. Por otra parte, para las caídas de tensión persistentes o apagones, no se recomienda la implantación de ninguna de ellas, ya que tanto la instalación de sistemas de generación de energía activados por motores como el establecimiento de un sistema de alimentación externo e independiente, sería excepcionalmente caro e innecesario para los riegos que se pretenden mitigar.

Justificación: Cortes de Corriente					
Amenaza	R.I.	F.C.	G.C.	FC x GC	Justificación
Apagones	90	9	2	18	5
Caídas de tensión persistente	90	5	2	10	9
Picos de tensión	135	2	2	4	33

Cuadro 12.1: Justificación de la inversión: Cortes de corriente.

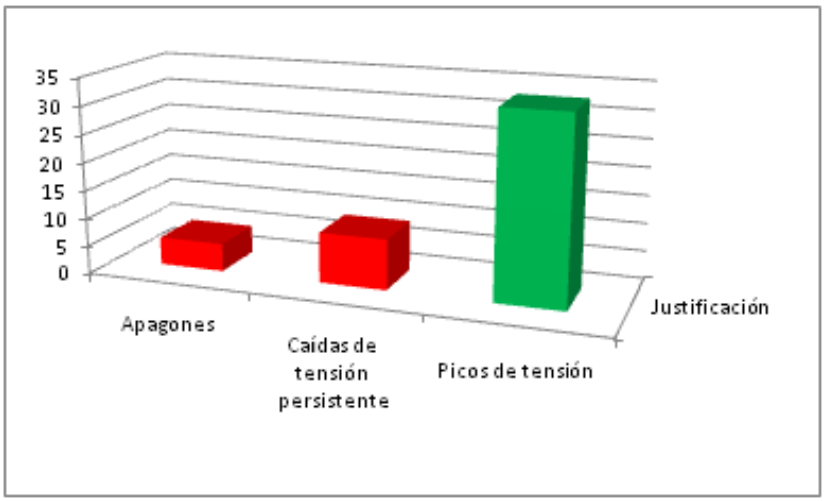


Figura 12.1: Justificación de la inversión: Cortes de corriente.

12.2. Cortes en comunicaciones

El corte de comunicación que más puede afectar al funcionamiento correcto de las actividades de negocio y a los servicios prestados por la empresa sería el corte de las comunicaciones de datos.

De las medidas adicionales propuestas anteriormente, se concluye, dado que éste es el ámbito general de una empresa de telecomunicaciones, que han de tomarse todas las medidas posibles para mitigar los posibles peligros que puedan tener lugar.

El cuadro 12.2 muestra los resultados con la justificación de la inversión. La planificación de esta tarea corresponde tanto al Administrador de Sistemas como a los Responsables del Departamento de Desarrollo y al Responsable del Departamento de Administración.

Justificación: Cortes en comunicaciones					
Amenaza	R.I.	F.C.	G.C.	FC x GC	Justificación
Congestión en la red	300	5	2	10	30
Fallo en hardware/software de comunicaciones	450	7	2	14	32
Destrucción de infraestructuras	150	3	1	3	50

Cuadro 12.2: Justificación de la inversión: Cortes en comunicaciones.

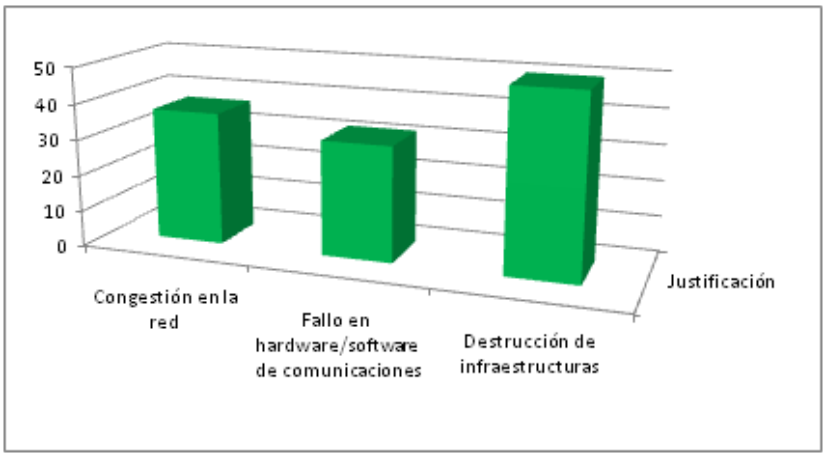


Figura 12.2: Justificación de la inversión: Cortes en comunicaciones.

12.3. Fallo en Hardware

Los fallos de hardware pueden ser críticos si se trata de averías que dejan sin funcionamiento a servidores o a dispositivos de comunicaciones de la empresa. La mejor manera para prevenir este tipo de contingencias es una labor periódica y continua de supervisión del estado de los equipos hardware, así como un control de las garantías de éstos. Los contratos con el proveedor de equipos hardware aseguran el mantenimiento y reparación de estos equipos durante el tiempo que dura la garantía, así como un contrato de sustitución de equipos obsoletos y averías que no puedan ser reparadas. Se recomienda poner en práctica las medidas propuestas anteriormente: Esta tarea deberá ser coordinada por el Responsable de Seguridad.

Justificación: Fallo en hardware					
Amenaza	R.I.	F.C.	G.C.	FC x GC	Justificación
Fallo de alimentación	225	8	2	16	14
Fallo en memoria	225	7	2	14	16
Fallo en instalación	135	2	2	4	33

Cuadro 12.3: Justificación de la inversión: Fallo en hardware.

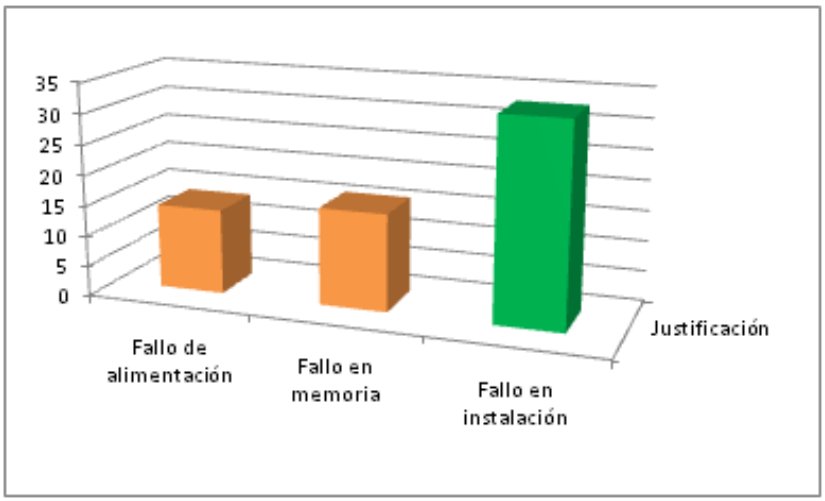


Figura 12.3: Justificación de la inversión: Fallo en hardware.

12.4. Fallos en Software

Existe una amplia variedad de errores ligados a fallos de software. Desde errores cometidos en la programación de las aplicaciones propias, a fallos del sistema operativo instalado en un equipo. Se recomienda la implantación de las medidas propuestas en el capítulo anterior:

- Establecer un procedimiento para controlar los accesos a los servidores de las aplicaciones instaladas, mediante ficheros de log, que deberán ser revisados periódicamente por el encargado del Departamento de Desarrollo.

- Poner en funcionamiento un departamento de calidad, o al menos un encargado, que realice las funciones de control de las aplicaciones instaladas, supervisión de la gestión de cambios y de la documentación de todas las aplicaciones instaladas en la organización.

Con la puesta en marcha de estas medidas, cualquier cambio que se realice en alguna aplicación o cualquier aplicación nueva que vaya a ser instalada, estará supervisado por un Responsable de Calidad.

Justificación: Fallo en software					
Amenaza	R.I.	F.C.	G.C.	FC x GC	Justificación
Errores de programación	900	4	2	8	112
Problemas con las actualizaciones	270	1	2	2	135
Fallos en el sistema operativo	900	3	2	6	150

Cuadro 12.4: Justificación de la inversión: Fallo en software.

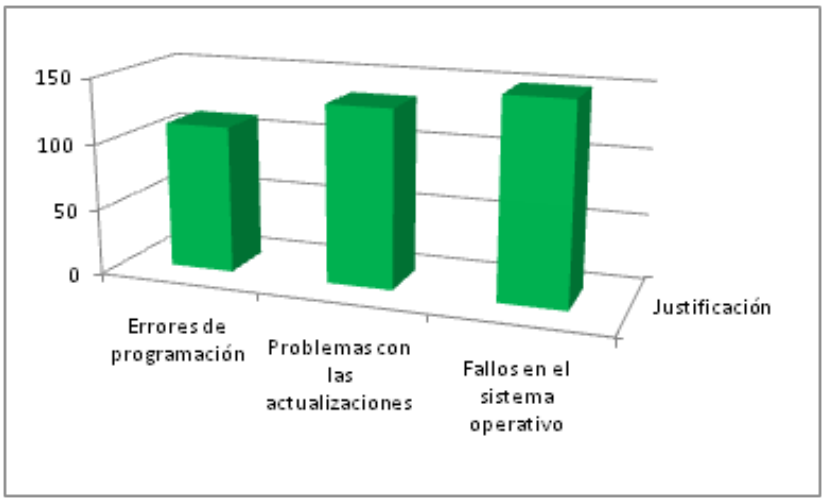


Figura 12.4: Justificación de la inversión: Fallo en software.

12.5. Seguridad de la información

La forma más sencilla de contraer un virus en los sistemas informáticos es mediante periféricos infectados que son conectados a los equipos. La probabilidad de recibir un ataque exterior queda mitigada, gracias a los firewalls instalados y a la utilización de proxies, las reglas de entrada/salida de los routers y la configuración de las redes de la organización están bien preparados para este tipo de ataques.

La planificación y puesta en marcha de estas medidas en los sistemas deberá corresponder al Administrador de Sistemas, con la supervisión y el control del Responsable de Seguridad.

Justificación: Virus					
Amenaza	R.I.	F.C.	G.C.	FC x GC	Justificación
Virus	3000	1	2	2	1500
DoS	3000	3	2	6	500
Intrusiones, hacking	3000	2	2	4	750

Cuadro 12.5: Justificación de la inversión: Seguridad de la información.

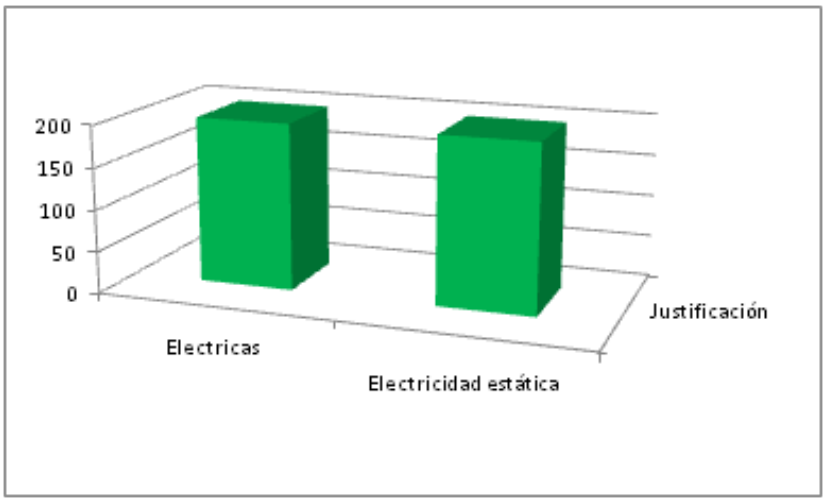


Figura 12.5: Justificación de la inversión: Seguridad de la información.

12.6. Seguridad física

Como se ha mencionado anteriormente, el tipo de robo más sensible para la organización es el robo de información de clientes. Es preciso establecer una política de seguridad antirrobos. Para garantizar la seguridad de la información de la organización, se debería establecer una serie de protocolos y normas para evitar robos de información. Estas medidas deben ser puestas en práctica por el Responsable de Seguridad y aprobadas por la dirección de la organización. El sabotaje, normalmente ocasionado por empleados de la propia empresa como actos de venganza o reivindicación, pueden ocasionar daños muy graves a los activos de los sistemas de información.

- Publicar un código o protocolo de buen uso de las herramientas informáticas dentro de la empresa, que delimite el uso que pueden hacer de éstas los empleados. La redacción y publicación deben ser llevadas a cabo por el Responsable de Seguridad.

- Existencia de una cláusula contractual que deben firmar los trabajadores de la empresa por la cual se comprometen a hacer un buen uso de los materiales y tecnologías de la organización.

La materialización de una amenaza terrorista supondría una serie de daños potenciales muy graves para la organización, si bien es cierto que la probabilidad de que lleguen a producirse

es muy remota.

Las medidas de seguridad elegidas así como una política de restricciones de accesos a lugares críticos, aseguran una protección eficiente aunque sencilla contra estos tipos de ataques.

Justificación: Seguridad física					
Amenaza	R.I.	F.C.	G.C.	FC x GC	Justificación
Robo	300	5	2	10	30
Sabotaje	150	5	2	10	15
Terrorismo	300	5	2	10	30

Cuadro 12.6: Justificación de la inversión: Seguridad física.

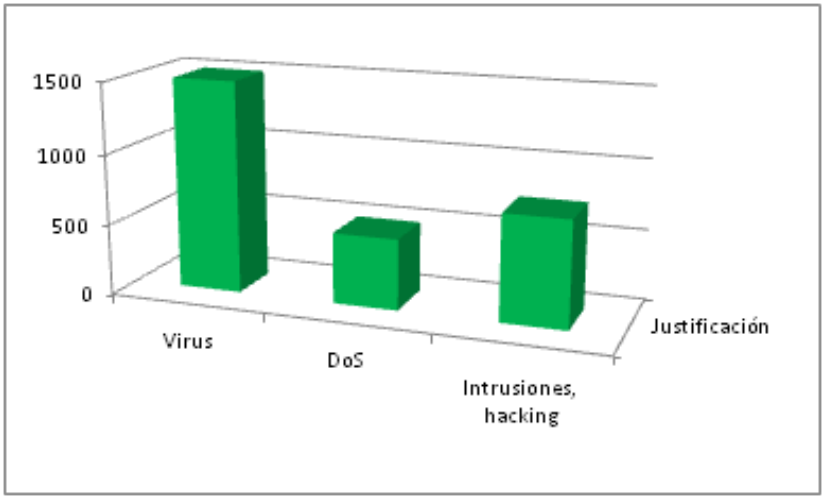


Figura 12.6: Justificación de la inversión: Seguridad física.

12.7. Incendio

Aunque la posibilidad de que se produzca un incendio grave es algo remota, las pérdidas que se producirían como consecuencias de éste serían muy cuantiosas, por lo tanto siempre es conveniente estar preparado ante una situación de tales consecuencias. Más probable de llegar a producirse sería el caso de un incendio de pequeñas consecuencias o una concentración alta de humos. Dado el riesgo residual estipulado, se concluye que se han de efectuar las siguientes

medidas correctoras:

- Revisión periódica de las instalaciones eléctricas existentes y de los sistemas de extinción. Esta labor ha de ser coordinada y supervisada por el Responsable de Seguridad.
- Formación del Responsable de Seguridad en prevención y control de incendios.

El Responsable de Seguridad debe añadir a su formación sobre situaciones de emergencia un conocimiento específico sobre las situaciones de incendio.

Justificación: Incendio					
Amenaza	R.I.	F.C.	G.C.	FC x GC	Justificación
Eléctricas	600	3	1	3	200
Electricidad estática	600	3	1	3	200

Cuadro 12.7: Justificación de la inversión: Incendio.

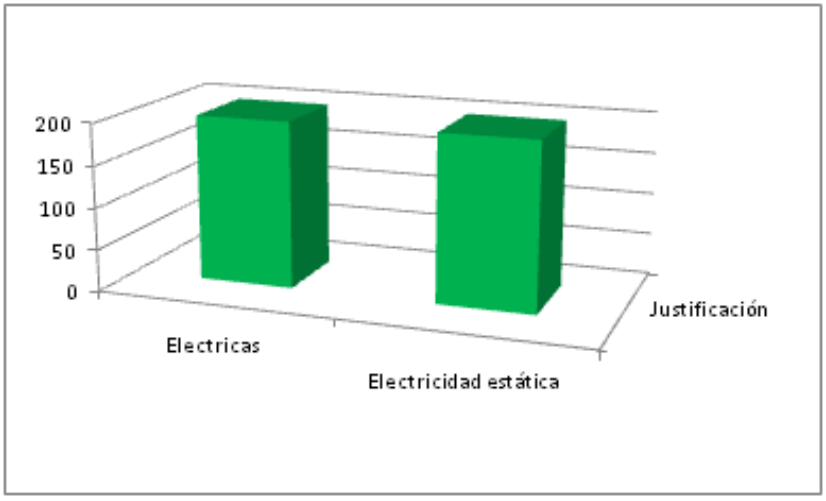


Figura 12.7: Justificación de la inversión: Incendio.

12.8. Inundación

El riesgo de una inundación a gran escala que pueda dañar gravemente los activos de la organización, aunque también tiene una escasa probabilidad, debe ser tenido en cuenta por los daños potenciales que puede causar. También se ha de poner especial hincapié en otros tipos de pequeñas inundaciones y humedades en algunas estancias de las oficinas.

De las medidas propuestas en el capítulo anterior, se han seleccionado las siguientes, de acuerdo al gasto que ocasionaría su puesta en funcionamiento y el riego residual resultante en el análisis anterior:

- Revisión y mantenimiento periódico del estado de desagües y sumideros. Esta tarea corresponde al Responsable de Seguridad.

De forma preventiva, si es posible y siempre que el coste no superara el riesgo inherente, los servidores no deben ubicarse en la planta baja o el sótano, dado que en caso de inundación no habría forma de protegerlos.

Justificación: Inundación					
Amenaza	R.I.	F.C.	G.C.	FC x GC	Justificación
Rotura de tuberías	300	1	2	2	150
Filtraciones	90	1	2	2	45
Lluvias torrenciales	100	3	3	9	11

Cuadro 12.8: Justificación de la inversión: Inundación.

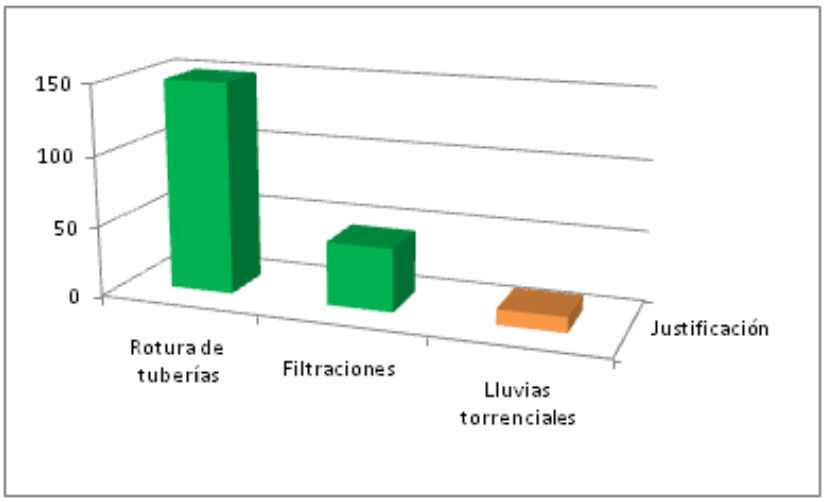


Figura 12.8: Justificación de la inversión: Inundación.

Capítulo 13

Supervisión y revisión

Uno de los factores críticos que afectan a la eficiencia y a la efectividad del proceso gestión de riesgo de una organización, es el establecimiento de un proceso continuo de supervisión y revisión. Este proceso asegura que el plan de gestión especificado permanece actualizado.

En el entorno de continuo cambio que viven las empresas hoy en día, aquellos factores que afectan a la probabilidad y al impacto de la materialización de una amenaza cambian constantemente. Esto es incluso más cierto para aquellos factores que afectan al coste de las soluciones para la gestión del riesgo. Es por tanto necesario repetir el ciclo de gestión de riesgo de forma regular.

Para convertir la gestión del riesgo en una parte de la cultura y la filosofía de una organización, se debe recopilar y documentar toda experiencia y conocimiento a través de un proceso de monitorización y revisión de eventos, planes, resultados y todo tipo de datos relevantes.

Cada fase del proceso de gestión del riesgo debe ser registrada de forma apropiada. Todo tipo de asunciones, métodos, fuentes de datos, resultados y razones por las cuales se toman decisiones deben ser incluidas en el registro. La supervisión de forma regular asegura que las acciones tomadas están gestionando el riesgo de forma efectiva, además ayudan a integrar la gestión de riesgos en las operaciones realizadas día a día [2].

13.1. Monitorización continua

La monitorización continua del plan de gestión de riesgo es un paso necesario para la supervivencia de la empresa.

- Monitorizar el plan de gestión de riesgo de forma continua asegura el progreso.
- Se deben incluir procedimientos en el plan de acción para tratar riesgos a través de programas de trabajos y planes en los proyectos.
- Toda acción debe quedar registrada en informes de progreso del plan de gestión de riesgo.
- Se debe revisar el perfil del riesgo de la empresa, siempre que se produzca un cambio significativo en la misma.

Es fundamental convertir la gestión del riesgo en una parte integral de la empresa.

- Incluir un análisis situacional y estrategias de identificación de riesgo en los planes estratégicos y planes de negocio anuales.
- Supervisar y revisar hitos claves en los programas y planes de trabajo cada mes.
- Incluir dichos hitos en las tareas de los trabajadores.

La revisión constante de los procesos asegurará que la gestión de riesgo mejore continuamente y pueda así cumplir con las necesidades especificas

- Analizar si las acciones tomadas para mitigar cada riesgo han sido efectivas. Centrarse principalmente en los riesgos medios y altos. Las consecuencias de un riesgo puede que no hayan cambiado, pero el control y la efectividad de la medida si puede haber mejorado con respecto a la que se usa actualmente.
- Re-evaluar solo aquellos riesgos en los cuales ha ocurrido un evento durante el último año,que haya podido cambiar nuestra percepción del mismo.
- Generar un nuevo perfil de riesgo.

13.2. La gestión del riesgo es responsabilidad de todos

Para llevar a cabo todas estas tareas es necesario, una integración del plan de gestión de riesgo, a todos los niveles. Es por ello que cada miembro de la empresa debe involucrarse en todo el proceso de gestión del riesgo. Según el papel que desempeñe cada empleado en la empresa, se le asignarán ciertas responsabilidades.

- Managers
  - Son responsables para una gestión efectiva del riesgo.
  - Eligen de entre las opciones de mitigación de riesgo recomendadas por el staff.
  - Aceptarán o rechazarán el riesgo basándose en el beneficio derivado de éste.
  - Entrenarán y motivarán al personal para que utilicen las técnicas de gestión de riesgo.
  - Llevarán las decisiones a un nivel superior si lo creen apropiado.
- Staff
  - Evalúan el riesgo y desarrollan alternativas de reducción del mismo.
  - Integran el control del riesgo en planes y órdenes.
  - Identifican controles de riesgo innecesarios.
- Supervisores
  - Aplican el proceso de gestión de riesgo.
  - Aplican consistentemente y de forma efectiva los métodos y conceptos de gestión de riesgo a las operaciones y tareas.
  - Delegan aquellos problemas relacionados con el riesgo que están por encima de su control a autoridades superiores, para que sean resueltas.
- Individuales
  - Deben comprender, aceptar e implementar los procesos de gestión de riesgo.
  - Deben prestar atención constante a los nuevos riesgos asociados a cada tarea u operación.

- Deben informar inmediatamente a sus supervisores de cualquier medida de mitigación no eficiente y de aquellos procedimientos de alto riesgo.

Capítulo 14

Coste de implantación del plan

Este proyecto abarca el plan de gestión para un sector completo, el de telecomunicaciones. Se ha estimado el presupuesto para su implantación en función de los datos proporcionados por el Observatorio Nacional de las Telecomunicaciones y de la SI [14].

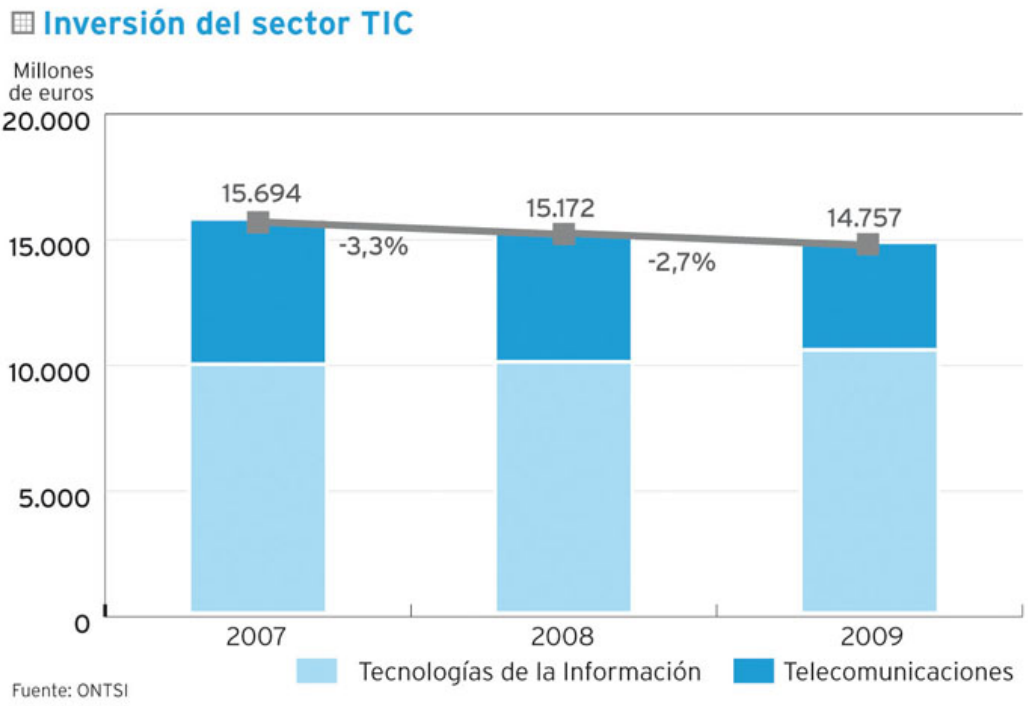


Figura 14.1: Inversión del sector TIC.

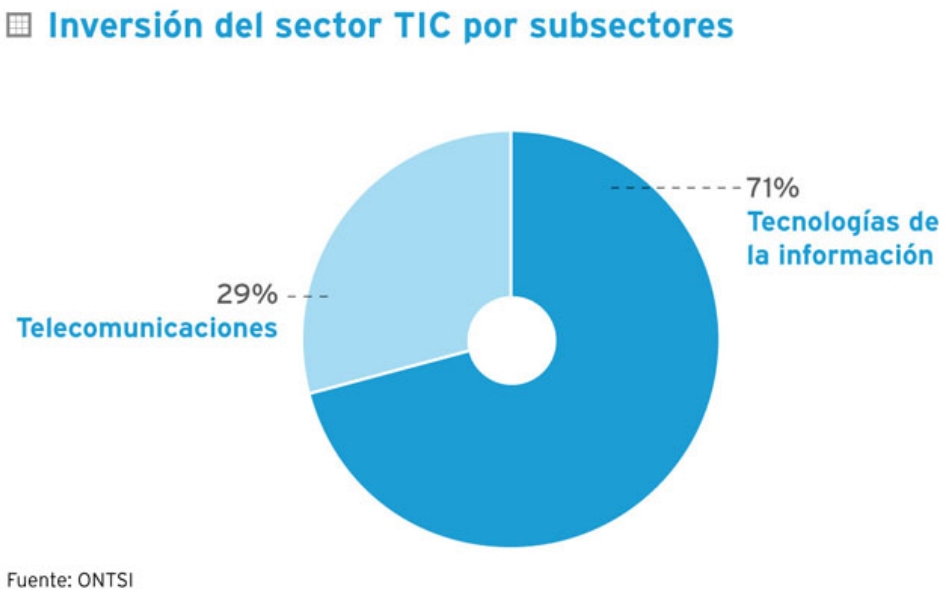


Figura 14.2: Inversión del sector TIC por subsectores.

La inversión en el sector de Telecomunicaciones en 2009 ascendió a más de 4.277 millones de euros. Según el ONTSI, el inmovilizado material alcanza el 40.5 % del total de la inversión, 1.732 millones de euros, de los que un 8 % estaría destinado a la gestión del riesgo operacional, 138 millones de euros anualmente.

Concepto	Coste
Implantación de plan ORM	138 millones de euros

Cuadro 14.1: Coste del proyecto.

Capítulo 15

Conclusiones

A lo largo del desarrollo de este proyecto se ha establecido un plan de control de riesgo operacional para el sector de las telecomunicaciones. El estudio se ha relizado tomando como referencia un mecanismo basado en cinco pasos de actuación: identificación, evaluación, análisis, implementación y supervisión.
Para calcular los factores de riesgo de las distintas amenazas y la justificación de la implantación de las medidas de mitigación, se han utilizado las métricas proporcionadas por el método Fine.

A la vista de los resultados obtenidos, la implantación de un plan de gestión de riesgo operacional asegura una reducción del riesgo en torno al 92 %, con una inversión del 8 % sobre el total de la inversión en activos inmóvilizados materiales del sector, estimados en 138 millones de Euros.
A primera vista, podría parecer una cifra elevada, pero es necesario tener en cuenta las consecuencias no operacionales que ocasiona la aparición de un fallo operacional.

El factor de pérdida económica tratado en este proyecto está reflejado en el valor del impacto, es decir, tan sólo hace referencia a la pérdida de valor operacional de negocio. En él, no se han reflejado las pérdidas propiciadas por el deterioro de la imagen de la compañía, ya que, nadie invertirá ni contratará a una empresa que no es capaz de ofrecer garantías en los servicios que proporciona. Tampoco se ha considerado el impacto económico que un fallo en telecomunicaciones ocasiona en las empresas que utilizan estos servicios para el desarrollo

de sus negocios.

A fecha de 2009, el 98.2 % de las empresas españolas tienen acceso a internet de banda ancha, de ellas, el 90 % utilizan páginas web para ofrecer sus productos.
El volumen de comercio eléctronico en España asciende a 156.607 millones de euros en compras y 168.864 millones en ventas [7]. En consecuencia, una única hora de inoperabilidad total en el servicio de internet en España, supone una pérdida en el volumen de negocio de 37 millones de euros.

Las telecomunicaciones representan uno de los pilares fundamentales del mundo globalizado en el que vivimos. Por tanto, es de vital importancia para el desarrollo de la economía mundial, la existencia de procedimientos, tales como el plan de gestión de riesgo operacional desarrollado en este proyecto, capaces de minimizar las consecuencias provocadas por la posible materialización de una amenaza, que pondría en peligro el desarrollo de gran parte de la actividad económica mundial.

Las telecomunicaciones evolucionan contínuamente, como también lo hacen las amenazas a las que están expuestas: nuevos virus informáticos, nuevas motivaciones terroristas, etc.
El proceso de gestión de riesgo es dinámico, debe evolucionar a la par que las telecomunicaciones y es una parte integral del proceso de desarrollo de las actividades operacionales de cada compañía.

Bibliografía

[1] Denial-of-service attack. URL `en.wikipedia.org`.

[2] Monitor and review. URL `http://www.enisa.europa.eu/`.

[3] Seguridad informática. URL `es.wikipedia.org`.

[4] Operational risk management. In *FAA System Safety Handbook*, 2000.

[5] *Operational Risk Management Prodecure (ORM)*, 2004.

[6] *Fases de un plan de prevención: Metodos para la evaluación del riesgo.* Cámara Madrid, 2005.

[7] Instituto Nacional de Estadística. URL `www.ine.es`.

[8] William T. Fine. *Mathematical Evaluations for Controlling Hazards.* in Widener, J., 1973.

[9] Adrian V. Gheorghe. *Critical infrastructures at risk: Securing the European Electric Power System.* Springer, 2006.

[10] Robert Hudyma. Causes of failure in it telecommunications networks, 2005.

[11] Othmar Kyas. *Network Troubleshooting.* Agilent Technologies, 2001.

[12] David Loader. *Operations Risk: Managing a Key Component of Operations Risk under Basel II.* Butterworth-Heinemann, 2007.

[13] Luis Eduardo Mendoza. Seguridad y control de sistemas de información, posibles amenazas. In *Sistemas de Información III*, 2008.

[14] Luis Muñoz. El informe del sector de las telecomunicaciones y de las tecnologías de la información en españa año 2009. Technical report, Observatorio Nacional de las Telecomunicaciones y la SI, 2010. URL `www.ontsi.red.es`.

[15] Basel Committee on Banking Supervision. *International Convergence of Capital Measurement and Capital Standards, A Revised Framework*. Bank for International Settlements, 2004.

[16] Jiantao Pan. Software reliability. Technical report, Carnegie Mellon University, 1999.

[17] Iron Mountain White Paper. The business case for disaster recovery planning: Calculating the cost of downtime. Technical report, Iron Mountain, 2005.

[18] Cisco Systems. What is the difference: Viruses, worms, trojans, and bots?

[19] Wikipedia. Virus informático. URL `es.wikipedia.org`.

[20] María Ángeles Nieto Giménez-Montesinos. El tratamiento del riesgo operaional en basilea ii. Technical report, Banco de España, 2005.