



FACULTAD DE INFORMÁTICA
UNIVERSIDAD POLITÉCNICA DE MADRID

UNIVERSIDAD POLITÉCNICA DE MADRID

FACULTAD DE INFORMÁTICA

TRABAJO FIN DE CARRERA

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

AUTOR: Juan Manuel Matalobos Veiga
TUTOR: José Domingo Carrillo Verdún

*“La sociedad y la familia
se parecen al arco de un palacio;
quitas una piedra y todo se derrumba.”*

A mi familia.

AGRADECIMIENTOS

Quiero agradecer a mi mujer, María Amelia y a mis hijos, Juan Manuel y María Amelia, porque son el motivo, la inspiración y el apoyo que me anima siempre a avanzar y a mejorar.

También quiero agradecer a mis padres, Juan Manuel y Blanca, a mi hermana Blanca Susana, y en general a toda la familia que me ha dado todo lo que soy.

A mi tutor José Carrillo, que me ha permitido presentar este proyecto y me ha ayudado a desarrollarlo.

A Víctor Maojo, que me ha apoyado largos años con infinita paciencia.

A la lista interminable de amigos, compañeros y profesores que me han ayudado, inspirado, retado, enseñado y corregido, y de esa forma me han facilitado el camino que he seguido hasta ahora.

ÍNDICE

Índice de contenidos

Agradecimientos	i
Índice.....	iii
Índice de contenidos.....	iii
Índice de figuras	ix
Índice de tablas.....	xii
Glosario.....	xv
Glosario de términos	xv
Glosario de abreviaturas.....	xxiv
Resumen.....	xxvii
1. Introducción	1
1.1. Seguridad de la Información.....	1
1.2. Análisis de riesgos	3
1.3. Consideración del riesgo.....	5
2. Objetivos	9
2.1. Racionalizar la inversión en seguridad de la información.....	9
2.2. Formalizar la toma de decisiones.....	12
2.3. Cumplir con las normativas aplicables	13
3. Planteamiento del problema.....	17
4. Estado de la cuestión.....	19
4.1. Análisis de riesgos de seguridad de la información.....	19
4.1.1. Conceptos generales.....	19

4.1.1.1.	Elementos del modelo	19
4.1.1.2.	Pérdida esperada (Single Loss Expectancy – SLE)	20
4.1.1.3.	Pérdida anual esperada (Annual Loss Expectancy – ALE)	21
4.1.1.4.	Cálculo del efecto de las salvaguardas.....	22
4.1.1.5.	Relaciones entre los activos	23
4.1.1.6.	Métodos cualitativos	25
4.1.1.7.	Métodos mixtos.....	30
4.1.1.8.	Ejemplo	30
4.1.2.	ISO TR 13335:1997 Tecnología de la información – Guías para la gestión de la seguridad de las TI	37
4.1.3.	ISO/IEC 27005:2008 Tecnologías de la información – Técnicas de seguridad – Gestión del riesgo de seguridad de la información.....	41
4.1.4.	UNE 71504:2008 Metodología de análisis y gestión de riesgos para los sistemas de información	44
4.1.5.	BS 7799-3:2006 Sistemas de Gestión de Seguridad de la Información – Parte 3: Guías para la gestión de riesgos de seguridad de la información 47	
4.1.6.	AS/NZS 4360:2004 Gestión de riesgos.....	49
4.1.7.	MAGERIT – Metodología de Análisis y GEstión de Riesgos de IT	50
4.1.8.	OCTAVE – Operationally Critical Threat, Asset and Vulnerability Evaluation.....	52
4.1.9.	CRAMM – CCTA Risk Analysis and Management Method.....	56
4.1.10.	NIST SP 800-30 Guía de gestión de riesgos para sistemas de tecnología de la información.....	59
4.1.11.	IRAM – Information Risk Analysis Methodologies	62
4.1.12.	CORAS – COConstruct a platform for Risk Analysis of Security critical systems	63
4.1.13.	SOMAP – Security Officers Management and Analysis Project.....	65
4.1.14.	FAIR – Factor Analysis of Information Risk.....	67
4.1.15.	Otras metodologías.....	70
4.1.16.	Metodologías comerciales	71
4.1.17.	Tablas comparativas	72
4.2.	Otros tipos de análisis de riesgos	82

4.2.1.	Enterprise Risk Management (ERM)	82
4.2.2.	Strategic Risk Management (SRM).....	83
4.2.3.	Evaluación de riesgo financiero	84
4.2.4.	Basilea II y Solvencia II	84
4.2.5.	Análisis de riesgos de auditoria.....	85
4.2.6.	Análisis de riesgos de proyectos.....	85
4.2.7.	Análisis de vulnerabilidades.....	86
4.2.8.	Riesgos laborales	86
4.2.9.	Protección de infraestructuras críticas.....	87
5.	Plan de proyecto.....	91
5.1.	Fases del proyecto.....	91
5.2.	Planificación del proyecto.....	93
5.3.	Equipo de trabajo	94
6.	Fase I: Definición de la metodología	99
6.1.	Definición de requerimientos.....	99
6.2.	Desarrollo del modelo.....	100
6.2.1.	Modelo de la metodología	100
6.2.2.	Fases de la metodología.....	102
6.2.2.1.	Valoración de procesos de negocio.....	102
6.2.2.2.	Valoración de activos de información.....	103
6.2.2.3.	Valoración de recursos de información.....	107
6.2.2.4.	Dependencias entre activos y recursos de información	108
6.2.2.5.	Valoración de vulnerabilidades.....	109
6.2.2.6.	Valoración de amenazas.....	109
6.2.2.7.	Cálculo del riesgo intrínseco	112
6.2.2.8.	Valoración de salvaguardas.....	114
6.2.2.9.	Cálculo del riesgo efectivo.....	119
6.2.2.10.	Gestión de riesgos	121
6.2.2.11.	Cálculo del riesgo residual.....	123
6.3.	Desarrollo de inventarios	125
6.4.	Desarrollo de plantillas	127

7. Fase II: Desarrollo de la herramienta.....	129
7.1. Definición de requerimientos.....	130
7.2. Modelo de datos.....	130
7.3. Prototipo funcional	130
7.4. Prototipo de demostración	132
7.5. Versión final	132
8. Fase III: Análisis de riesgos	135
8.1. Arranque del proyecto	135
8.1.1. Equipo de trabajo.....	135
8.1.2. Definición del alcance	135
8.1.3. Adaptación de la metodología.....	136
8.2. Obtención de información	137
8.2.1. Preparación de cuestionarios	137
8.2.2. Solicitud inicial de colaboración	139
8.2.3. Reunión de arranque.....	139
8.2.4. Análisis de documentación.....	141
8.2.5. Entrevistas con interlocutores	143
8.3. Análisis de riesgos	144
8.3.1. Cálculo del riesgo intrínseco	144
8.3.2. Cálculo del riesgo efectivo	145
8.4. Presentación de resultados	145
9. Fase IV: Gestión de riesgos	147
9.1. Definición de umbrales.....	147
9.2. Identificación de riesgos no cubiertos	147
9.3. Elaboración del plan de acción	148

9.3.1. Selección de salvaguardas	148
9.3.2. Cálculo del riesgo residual	149
9.3.3. Definición de proyectos.....	149
9.3.4. Definición de planes de acción.....	152
9.3.5. Definición del plan de acción consolidado.....	154
9.4. Aprobación del plan de acción.....	155
10. Control y gestión del proyecto	157
10.1. Reunión de arranque del proyecto	157
10.2. Reuniones de seguimiento del proyecto	158
10.3. Reunión de cierre del proyecto	159
11. Líneas futuras de trabajo	161
11.1. Realización de pruebas	161
11.2. Análisis continuo de riesgos	163
11.3. Implantación del SGSI.....	165
11.4. Implantación del Plan de Seguridad	167
11.5. Medición de los resultados.....	168
11.6. Integración con otras áreas.....	169
11.7. Evolución de las metodologías de análisis de riesgos	170
12. Conclusiones	173
13. Bibliografía	177
13.1. Bibliografía	177
13.2. Mapa de referencias bibliográficas	185
Anexo I: Estudios de tendencias en materia de Seguridad de la Información.....	187
Anexo II: Referencias legislativas, regulatorias y normativas al análisis de riesgos....	189
Referencias legislativas	189

Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.	189
Real Decreto 263/1996, de 16 de Febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.....	190
Referencias a códigos de buenas prácticas.....	190
Directrices de la OCDE para la seguridad de sistemas y redes de información: hacia una cultura de seguridad.	190
ISO/IEC 27001:2005 Tecnología de Información – Técnicas de seguridad – Sistemas de Gestión de Seguridad de la Información – Requerimientos	191
ISO/IEC 27002:2005 Tecnología de Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información	193
BS 25999:2006 Gestión de continuidad de negocio.....	195
PCI/DSS – Payment Cards Industry/Data Security Standards	196
ITIL – Information Technology Infrastructure Library.....	197
ISO/IEC 20000 Tecnología de información – Gestión del servicio.....	199
COBIT – Control OBJECTives for Information and related Technology.....	201
Criterios de Seguridad, Normalización y Conservación de las aplicaciones utilizadas para el ejercicio de potestades. Ministerio de Administraciones Públicas, 2004.	210
NIST SP 800-53 Controles de seguridad recomendados para los sistemas de información federales.	211
Anexo III: Requerimientos de seguridad	215
Definición de los requerimientos de seguridad	215
Escala de valoración de requerimientos de seguridad.....	216
Anexo IV: Tipos de recursos de información	217

Anexo V: Inventario de amenazas	221
Anexo VI: Inventario de salvaguardas	225
Anexo VII: Herramientas	231
Definición de requerimientos	231
Prototipo funcional	252
Prototipo de demostración	254
Versión final	255
Módulo usuarios	256
Módulo inventarios	257
Módulo metodologías	258
Módulo activos	259
Módulo análisis	261
Módulo valoraciones	262
Módulo reporting	262
Anexo VIII: Cuestionarios	265

Índice de figuras

Figura 1: Coste de la seguridad y de la inseguridad	11
Figura 2: Ejemplo análisis de riesgos	31
Figura 3: Procesos de gestión de seguridad de la información de ISO/IEC 13335	39
Figura 4: Proceso de análisis detallado de riesgos de ISO/IEC 13335	40
Figura 5: Proceso de gestión de riesgos de seguridad de la información de ISO/IEC 27005:2008	43
Figura 6: Modelo UNE 71504	46
Figura 7: Modelo de procesos de gestión de riesgos de BS 7799-3	48
Figura 8: Proceso de gestión de riesgos de AS/NZS 4360:2004	49

Figura 9: Modelo MAGERIT	52
Figura 10: Fases del proceso OCTAVE	55
Figura 11: Modelo de análisis y gestión de riesgos de CRAMM.....	57
Figura 12: Principales actividades de análisis y gestión de riesgos de CRAMM .	59
Figura 13: Proceso de análisis de riesgos de NIST SP 800-30.....	60
Figura 14: Proceso de gestión de riesgos de NIST SP 800-30	61
Figura 15: Los siete pasos de la metodología CORAS	64
Figura 16: Modelo de datos de SOMAP (ORIMOR).....	67
Figura 17: Modelo de decisiones de gestión de riesgos de FAIR	68
Figura 18: Taxonomía de factores de los riesgos de información de FAIR	69
Figura 19: Modelos de Control Interno y de Gestión de Riesgos Corporativos (ERM) de COSO	83
Figura 20: Fases del proyecto.....	91
Figura 21: Planificación del proyecto.....	93
Figura 22: Organización del equipo de trabajo	94
Figura 23: Modelo general de la metodología de análisis de riesgos.....	101
Figura 24: Ciclo de vida en espiral.....	129
Figura 25: Modelo de datos de la aplicación.....	130
Figura 26: Estructura societaria de la Organización.....	135
Figura 27: Plantilla resumen de plan de proyecto	152
Figura 28: Plan de acción - Calendario	154
Figura 29: Mapa de referencias bibliográficas	186
Figura 30: Modelo de Seguridad de la información de ITIL.....	197
Figura 31: COBIT - Áreas del gobierno de TI	201

Figura 32: COBIT - Metas y métricas proceso PO9.....	205
Figura 33: COBIT - Dependencias del proceso PO9.....	207
Figura 34: Prototipo funcional - Modelo de datos.....	252
Figura 35: Prototipo funcional – Operaciones.....	252
Figura 36: Prototipo de demostración - Inventario de activos.....	254
Figura 37: Prototipo de demostración - Valoración de amenazas	254
Figura 38: Prototipo de demostración – Generación de informes	255
Figura 39: Aplicación final - Autenticación de usuarios.....	255
Figura 40: Aplicación final - Gestión de usuarios	256
Figura 41: Aplicación final - Gestión de perfiles	256
Figura 42: Aplicación final - Inventario de amenazas.....	257
Figura 43: Aplicación final - Inventario de salvaguardas.....	257
Figura 44: Aplicación final - Gestión de metodologías.....	258
Figura 45: Aplicación final - Gestión de requerimientos de seguridad	258
Figura 46: Aplicación final - Gestión de escalas de valoración	259
Figura 47: Aplicación final - Inventario de activos	259
Figura 48: Aplicación final - Inventario de recursos	260
Figura 49: Aplicación final - Gestión de proyectos de análisis de riesgos.....	261
Figura 50: Aplicación final - Proyecto de análisis de riesgos	261
Figura 51: Aplicación final - Valoración de activos.....	262
Figura 52: Aplicación final - Informe de riesgo intrínseco	262
Figura 53: Aplicación final - Gráfico de riesgo intrínseco	263
Figura 54: Aplicación final - Informe riesgo efectivo	263
Figura 55: Aplicación final - Gráfico riesgo efectivo.....	264

Figura 56: Cuestionarios - Portada	265
Figura 57: Cuestionarios - Control de documentación	266
Figura 58: Cuestionarios - Índice	267
Figura 59: Cuestionarios - Objetivo	268
Figura 60: Cuestionarios - Descripción general	269
Figura 61: Cuestionarios - Organización	270
Figura 62: Cuestionarios - Procesos de negocio	271
Figura 63: Cuestionarios - Activos de información	271
Figura 64: Cuestionarios - Recursos de información	272
Figura 65: Cuestionarios - Anexo I Documentación	272
Figura 66: Cuestionarios - Anexo II Valoración	273
Figura 67: Cuestionarios - Anexo III Recursos de información	273
Figura 68: Cuestionarios - Anexo IV Amenazas	274
Figura 69: Cuestionarios - Anexo V Tipos de controles	274

Índice de tablas

Tabla 1: Cálculo cualitativo del impacto	27
Tabla 2: Cálculo cualitativo del riesgo	27
Tabla 3: Cálculo cualitativo del riesgo residual	28
Tabla 4: Cálculo cualitativo mediante la función mínimo	28
Tabla 5: Cálculo cualitativo mediante la función máximo	29
Tabla 6: Cálculo cualitativo mediante la función media	29
Tabla 7: Cálculo cualitativo utilizando dos escalas	29
Tabla 8: Cálculo cualitativo utilizando dos escalas	30

Tabla 9: Planteamiento del caso práctico de análisis de riesgos – Listado de activos	32
Tabla 10: Planteamiento del caso práctico de análisis de riesgos - Listado de recursos	32
Tabla 11: Caso práctico de análisis de riesgos: cálculo de la degradación	33
Tabla 12: Caso práctico de análisis de riesgos - Cálculo de la pérdida esperada..	34
Tabla 13: Caso práctico de análisis de riesgos - Cálculo de la pérdida anual esperada.....	35
Tabla 14: Caso práctico de análisis de riesgos - Cálculo del riesgo efectivo	36
Tabla 15: Ciclo de Deming aplicado a la gestión de riesgos de seguridad de la información	44
Tabla 16: Comparativa de metodologías de análisis de riesgos - Responsables ...	73
Tabla 17: Comparativa de metodologías de análisis de riesgos - Alcance considerado	74
Tabla 18: Comparativa de metodologías de análisis de riesgos - Tipo de análisis	75
Tabla 19: Comparativa de metodologías de análisis de riesgos - Tipo de riesgo..	76
Tabla 20: Comparativa de metodologías de análisis de riesgos - Elementos del modelo.....	77
Tabla 21: Comparativa de metodologías de análisis de riesgos – Objetivos de seguridad	78
Tabla 22: Comparativa de metodologías de análisis de riesgos - Inventarios.....	80
Tabla 23: Comparativa de metodologías de análisis de riesgos - Ayudas a la implantación.....	81
Tabla 24: Valoración de la eficacia de los controles	117
Tabla 25: Requerimientos de análisis de riesgos de PCI DSS	196
Tabla 26: Proceso COBIT de evaluación y administración de riesgos de TI.....	203

Tabla 27: Diagrama RACI de las funciones relacionadas con el proceso PO9...	204
Tabla 28: Criterios de valoración de activos	216
Tabla 29: Macro para el cálculo del riesgo intrínseco.....	253
Tabla 30: Macro para el cálculo del riesgo efectivo.....	253

GLOSARIO

Glosario de términos

En este glosario se presentan los términos de uso frecuente en el entorno del análisis de riesgos. Junto a la definición de cada término se ha introducido la traducción al inglés, para facilitar la comprensión de la literatura técnica escrita en ese idioma.

En la elaboración de este glosario se han tenido en cuenta las definiciones recogidas en los principales estándares que se detallan en el apartado de Estado de la Cuestión. Para cada término se ha seleccionado el que se ha considerado más adecuado en el contexto del proyecto, y en algunas entradas se ha preparado una nueva definición que se ha considerado más apropiada para este entorno.

Aceptación (*Aceptation*): Estrategia de gestión de riesgos que consiste en la aceptación del nivel de riesgo actual. Puede seleccionarse automáticamente si el nivel de riesgo es inferior al umbral de riesgo considerado tolerable o tras un análisis coste/beneficio considerando las alternativas disponibles para reducir o eliminar un riesgo superior.

Activo (*Asset*): Cualquier elemento valioso o necesario para que la Organización cumpla sus objetivos. Cfr. [ISO13335-1.04], Cfr. [ALBER01]

Activo de información (*Information asset*): Cualquier información valiosa o necesaria para que la Organización cumpla sus objetivos.

Ver nota en la entrada *Recurso de información*.

Acuerdo de nivel de servicio (*Service level agreement*): Acuerdo entre dos partes en relación a las características mínimas exigibles a un servicio prestado entre ellas.

Amenaza (*Threat*): Causa potencial de un incidente que puede resultar en un daño a un sistema o a una organización. [ISO13335-1.04], [ISO27002.05]

Análisis cualitativo (*Qualitative analysis*): Análisis basado en el uso de escalas de valoración. Cfr. [ISO13335-1.04]

Análisis cuantitativo (*Quantitative analysis*): Análisis basado en cuantificación numérica de magnitudes, generalmente en términos económicos. Cfr. [ISO13335-1.04]

Análisis de impacto sobre el negocio (*Impact analysis*): Estudio de las consecuencias que tendría la realización de una determinada amenaza sobre la Organización. Cfr. [MAGE06]

Análisis de riesgos (*Risk analysis, risk assessment*): Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización. [MAGE06], Cfr. [ISO13335-1.04]

Análisis mixto (*Mixed analysis*): Análisis que emplea una combinación de términos cuantitativos y cualitativos. Cfr. [ISO13335-1.04]

Apetito de riesgo (*Risk appetite*): Cantidad de riesgo que una Organización está dispuesta a gestionar para lograr los objetivos establecidos.

Ataque (*Attack*): Amenaza de origen intencionado. Cfr. [MAGE06]

Ataque de día cero (*Zero day attack*): Ataque que se produce antes de la publicación de la vulnerabilidad que explota.

Autenticidad (*Authenticity*): Propiedad que asegura que la identidad de un elemento o recurso es la que se le supone. La autenticidad aplica a elementos como usuarios, procesos, sistemas e información. [ISO13335-1.04]

Ciclo de Deming (*PDCA cycle*): Ver ciclo de la mejora continua.

Ciclo de la mejora continua (*PDCA cycle*): Herramienta de gestión para la evolución de los procesos que define cuatro fases (planificación, ejecución, comprobación, actuación).

Concienciación (*Awareness*): Conjunto de medidas definidas para que las personas relacionadas con la organización (personal, personal subcontratado, clientes, proveedores, etc.) conozcan los riesgos de seguridad y los controles que pueden y deben aplicar para colaborar en su mitigación.

Confidencialidad (*Confidentiality*): Propiedad de que la información no está disponible ni es divulgada a personas, procesos o dispositivos no autorizados. [ISO13335-1.04], Cfr. [ISO27002.05], Cfr. [MAGE06], Cfr. [ALBER01]

Contramedida (*Countermeasure*): Ver salvaguarda.

Control (*Control*): Ver salvaguarda.

Control alternativo (*Alternative control*): Ver control mitigante.

Control correctivo (*Corrective control*): Control definido para reducir o eliminar el impacto de incidente de seguridad ocurrido.

Control detectivo (*Detective control*): Control definido para detectar la ocurrencia de un incidente de seguridad y permitir la reacción ante el mismo.

Control disuasorio (*Dissuasive control*): Control preventivo definido para hacer desistir a un potencial atacante antes de que se produzca el ataque.

Control general (*Pervasive control*): Control que sirve de soporte para un conjunto amplio de activos, recursos y otros controles.

Control mitigante (*Mitigating control*): Control definido para suplir las deficiencias de otro control.

Control preventivo (*Preventive control*): Control definido para dificultar o impedir la ocurrencia de un incidente de seguridad.

Declaración de aplicabilidad (*Statement Of Applicability, SOA*): Documento formal en el que, para un conjunto de salvaguardas, se indica si son o no de aplicación en el sistema de información bajo estudio. Cfr. [MAGE06] (Bajo la entrada “Documento de selección de controles”)

Degradación (*Degradation*): Pérdida del valor de un activo como consecuencia de la realización de una amenaza. Cfr. [MAGE06]

Disponibilidad (*Availability*): Propiedad de que la información y sus activos asociados sea accesible y utilizable bajo la demanda por una entidad autorizada. Cfr [MAGE06], Cfr. [ISO27002.05], Cfr. [ISO7498-2.89]

Efectividad (*Effectiveness*): Ver eficacia.

Eficacia (*Effectiveness*): Propiedad de que se cumplen todos los objetivos de negocio definidos para un determinado elemento. Cfr. [ISACA07].

Eficiencia (*Efficiency*): Propiedad de que un requerimiento de negocio se alcanza realizando un consumo óptimo de los recursos disponibles para ello. Cfr. [ISACA07].

Escenario de riesgos (*Risk scenario*): Descripción del efecto de un conjunto determinado de amenazas sobre un determinado conjunto de activos, recursos y salvaguardas, teniendo en cuenta determinadas hipótesis definidas. Cfr. [ISO13335-1.04]

Estimación de riesgos (*Risk estimation*): Proceso utilizado para asignar valores de probabilidad e impacto asociados a un riesgo. [ISO73.05]

Evaluación de riesgos (*Risk evaluation*): Comparación del riesgo estimado contra un determinado criterio para determinar su significatividad. [ISO73.05]

Evaluación de salvaguardas (*Safeguard assessment*): Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que mitigan. Cfr. [MAGE06]

Evitación (*Avoidance*): Estrategia de gestión de riesgos que consiste en eliminar los activos y los recursos que suponen un riesgo superior al considerado tolerable.

Fiabilidad (*Reliability*): Propiedad de mantener de forma consistente un comportamiento y unos resultados. [ISO13335-1.04]

Frecuencia (*Frequency*): Tasa de ocurrencia de una amenaza. [MAGE06]

Gestión de riesgos (*Risk management, risk treatment*): selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados. [MAGE06], Cfr. [ISO13335-1.04], Cfr. [ISO27002.05].

Impacto (*Impact*): Consecuencia potencial que sobre un activo tiene la realización de una amenaza. Cfr. [MAGE06]

Impacto residual (*Residual Impact*): Consecuencia potencial que sobre un activo tiene la realización de una amenaza, una vez considerados los efectos mitigantes de las salvaguardas implantadas.

Incidente (*Incident*): Evento inesperado o indeseado que puede causar un compromiso de las actividades de negocio de la seguridad de la información. [ISO13335-1.04]

Integridad (*Integrity*): Propiedad de que la información y los métodos de procesamiento sean exactos y completos. Cfr. [MAGE06], Cfr. [ISO13335-1.04], Cfr. [ISO27002.05]

Línea base de controles (*Controls baseline*): Conjunto mínimo de salvaguardas definido para un sistema u organización. [ISO13335-1.04]

Mapa de riesgos (*Risk map*): Relación de las amenazas valoradas a las que están expuestos los activos. Cfr. [MAGE06]

No repudio (*Non repudiation*): Propiedad de que un elemento que ha realizado una determinada acción en el sistema no puede negar su realización.

Normativa de seguridad (*Security regulation*): Conjunto de documentos que desarrollan la política de seguridad.

Objetivo de punto de recuperación (*Recovery Point Objective*): Punto en el que un determinado proceso se recupera tras un incidente. Determina el volumen tolerable de transacciones que puede perderse en caso de un incidente.

Objetivo de tiempo de recuperación (*Recovery Time Objective*): Periodo de tiempo objetivo definido para recuperar el funcionamiento de un determinado proceso tras un incidente. Cfr. [BS25999-1.06]

Pérdida anual esperada (*Annual loss expectancy*): Pérdidas anuales estimadas por la realización de una determinada amenaza sobre un recurso de información.

Pérdida esperada (*Single loss expectancy*): Pérdidas estimadas por la realización de una determinada amenaza sobre un recurso de información.

Plan de continuidad de negocio (*Business continuity plan*): Colección documentada de procedimientos e información desarrollada, recopilada y mantenida de modo que esté disponible para su uso en caso de incidentes y permita a la organización continuar la ejecución de sus actividades críticas a un nivel aceptable predefinido. [BS25999-1.06]

Plan de recuperación de desastres (*Disaster recovery plan*): Conjunto de medidas definidas para recuperar un determinado servicio de soporte al negocio tras una interrupción provocada por un incidente.

Plan de seguridad (*Security plan*): Conjunto de proyectos de seguridad priorizados y presupuestados que permiten materializar las decisiones de gestión de riesgos. Cfr. [MAGE06]

Política de seguridad (*Security policy*): Conjunto de reglas, directivas y prácticas que gobiernan cómo se gestionan, protegen los activos y recursos de información. Cfr. [ISO13335-1.04]

Probabilidad (*Likelihood*): Medida de expectativa de que una amenaza se realice en un periodo de tiempo determinado, generalmente un año.

Proceso de gestión de la seguridad (*Security Management process*): Conjunto de objetivos, recursos, funciones, responsabilidades y tareas definidos para garantizar la seguridad de una organización.

Proyecto de seguridad (*Security project*): Conjunto de actividades interrelacionadas definidas para lograr un determinado objetivo en relación a la mejora o mantenimiento del nivel de seguridad de la información.

Recurso de información (*Information resource*): Cualquier elemento empleado en el tratamiento de activos de información.

Nota: en general los estándares de análisis de riesgos no diferencian la información como concepto abstracto y los recursos físicos y lógicos utilizados para su tratamiento, considerando ambos bajo el concepto de activos de información. En el contexto de este proyecto, se considera activo de información el concepto abstracto de la información necesaria para el funcionamiento de la organización y se considera recurso de información los medios físicos y lógicos utilizados para el tratamiento.

Reducción (*Reduction*): Estrategia de gestión de riesgos que consiste en la aplicación de salvaguardas para reducir un riesgo cuyo nivel supera el umbral de riesgo tolerable definido.

Requerimiento de seguridad (*Security requirement*): conjunto de propiedades de la información y sus recursos cuyo incumplimiento supone un incidente que tiene como consecuencia un daño para un sistema o la organización.

Riesgo (*Risk*): Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización. [MAGE06]

Riesgo acumulado (*Accumulated Risk*): Riesgo calculado tomando en consideración el valor propio de un recurso de información y el valor de los activos de información que dependen de él. Este valor se combina con la degradación y la frecuencia de las amenazas del recurso de información considerado. Cfr. [MAGE06]

Riesgo efectivo (*Effective Risk*): Riesgo remanente en el sistema tras la valoración de las salvaguardas actualmente implantadas.

Nota: si bien este término se considera habitualmente como sinónimo de riesgo residual, en el contexto de este proyecto se utiliza con significado distinto, diferenciando el riesgo calculado teniendo en cuenta las salvaguardas implantadas del riesgo calculado teniendo en cuenta las salvaguardas implantadas y las salvaguardas previstas en el plan de seguridad.

Riesgo intrínseco (*Intrinsic Risk*): Riesgo en el sistema sin valorar la eficacia de las salvaguardas implantadas o incluidas en el plan de seguridad. [MAGE06]

Riesgo repercutido (*Affected Risk*): Riesgo calculado tomando en consideración únicamente el valor propio de un activo de un activo de información. Este valor se combina con la degradación y la frecuencia de las amenazas de los recursos de información de los que depende. Cfr. [MAGE06]

Riesgo residual (*Residual Risk*): Riesgo remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información. [MAGE06]

Ver nota en la entrada *Riesgo efectivo*.

Salvaguarda (*Safeguard*): Medida establecida para la reducción del riesgo. Cfr. [MAGE06]

Seguridad (*Security*): Capacidad de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que pueden causar un daño a un sistema o a la organización. Cfr. [MAGE06]

Seguridad de la información (*Information Security*): Capacidad de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que pueden causar un daño a los activos de información de una organización. Cfr. [MAGE06]

Seguridad informática (*IT Security*): Capacidad de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que pueden causar un daño a los recursos de información tecnológicos de una organización. Cfr. [MAGE06]

Sistema de gestión de seguridad de la información (*Information Security Management System*): Herramienta a disposición de la Dirección de las organizaciones para llevar a cabo las políticas y los objetivos de seguridad. Comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información. Está basado en el ciclo de la mejora continua (PDCA). Cfr. [UNE71502.04]

Tasa anual de ocurrencia (*Annual rate of occurrence*): Estimación del número de veces que una determinada amenaza se realiza sobre un determinado recurso de información.

Tolerancia al riesgo (*Risk tolerance*): Cantidad de riesgo que una Organización es capaz de gestionar.

Transferencia (*Transfer*): Estrategia de gestión de riesgos que consiste en transferir un riesgo a una entidad externa que deba encargarse de su gestión y que asuma los daños en caso de ocurrencia de un incidente.

Trazabilidad (*Accountability*): Propiedad de que se puede determinar el elemento que ha realizado una determinada acción en el sistema. Cfr. [ISO13335-1.04]

Valor (*Value*): Estimación de la utilidad de un determinado activo de información para la organización, teniendo en cuenta los diferentes requerimientos de seguridad definidos.

Valor acumulado (*Accumulated value*): Valor de un determinado recurso de información teniendo en cuenta el valor de los activos de información que dependen de él. Cfr. [MAGE06]

Vulnerabilidad (*Vulnerability*): Debilidad en un recurso de información que puede ser explotada por una amenaza para causar un daño a un sistema o a la Organización. Cfr. [ISO27002.05]

Glosario de abreviaturas

En este glosario se presentan las abreviaturas de uso frecuente en este documento y en el dominio del análisis y la gestión de riesgos de seguridad de la información.

AGR: Análisis y Gestión de Riesgos.

ALARP: As Low As Reasonably Practicable, tan bajo como sea razonable (referido al nivel de riesgo).

ALE: Annual Loss Expectancy, pérdida anual esperada.

ARO: Annual Rate of Occurrence, tasa anual de ocurrencia.

BCP: Business Continuity Plan, plan de continuidad de negocio.

BIA: Business Impact Analysis, análisis de impacto sobre el negocio.

BSI: British Standards Institute, Instituto Británico de Estándares.

CMM: Capability Maturity Model, modelo de madurez de capacidades.

CPD: Centro de Proceso de Datos.

DRP: Disaster Recovery Plan, plan de recuperación de desastres.

IEC: International Electrotechnical Commission, Comisión Electrotécnica Internacional.

ISMS: Information Security Management System, Sistema de gestión de seguridad de la información.

ISO: International Organization for Standardization, Organización Internacional de Estandarización.

PCN: Plan de continuidad de negocio.

PDCA: Plan, Do, Check, Act. Planificar, Ejecutar, Comprobar, Actuar. Ciclo de Deming o de la mejora continua.

PRD: Plan de recuperación de desastres.

RACI: Responsible, Accountable, Consulted, Informed. Encargado, responsable, consultado, informado.

RPO: Recovery Point Objective, objetivo de punto de recuperación.

RTO: Recovery Time Objective, objetivo de tiempo de recuperación.

SGSI: Sistema de Gestión de Seguridad de la Información.

SLA: Service Level Agreement, acuerdo de nivel de servicio.

SLE: Single Loss Expectancy, pérdida esperada.

SOA: Statement Of Applicability, declaración de aplicabilidad.

TR: Technical Report, informe técnico.

RESUMEN

Este proyecto se enmarca en el desarrollo, por parte de la Organización, de un Plan Director de Seguridad de la Información y un Sistema de Gestión de Seguridad de la Información, cuyo desarrollo se ha definido como parte del Plan Estratégico Corporativo.

Específicamente, el proyecto ha consistido en la realización de un análisis de riesgos de seguridad de la información que permita cuantificar y comparar los requerimientos de seguridad de la información de la Organización con los controles implantados para su cumplimiento, y, en base a las diferencias encontradas, definir los controles adicionales necesarios para cumplir todos los requerimientos.

Para el desarrollo de este proyecto se ha definido una metodología de trabajo desarrollada a medida y basada en las principales metodologías de análisis y gestión de riesgos de uso habitual en el mercado de la seguridad de la información y en las necesidades, cultura y estructura específicas de la Organización.

Una vez definida la metodología se ha diseñado y desarrollado una herramienta informática de soporte, que permita aplicar la metodología de forma eficaz y eficiente.

Finalmente, tanto la metodología como la herramienta se han empleado en la realización del análisis de riesgos planteado como objetivo del proyecto.

1. INTRODUCCIÓN

1.1. Seguridad de la Información

La información, en todas sus formas (automatizada o no automatizada, formalizada o no formalizada, pública o reservada, etc.), es uno de los principales activos de cualquier Organización, necesario para el normal funcionamiento y la consecución de los objetivos que tenga marcados. [ISO27001.05] [ISO27001.05] [NIST800-12.95]

Debido a esa importancia, las Organizaciones necesitan proteger su información para asegurar que esté disponible cuando se necesite, que sea fiable y que su distribución esté controlada. Esta necesidad se ve agravada por el hecho de que la cantidad de información que maneja una Organización y su complejidad crece de forma exponencial, dificultando los esfuerzos para su protección. [ISO27005.08] [UNE71504.08] [MAGE06] [ALBER01] [NIST800-12.95]

Se entiende por Gestión de la Seguridad de la Información el proceso por el cual la Organización define, alcanza y mantiene unos niveles apropiados de confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad para la información que necesita para operar. [ISO13335-2.97] [ISO27005.08]

El proceso de Gestión de la Seguridad de la Información incluye, entre otros, los siguientes aspectos principales [ISO27005.08] [MAGE06]:

- Determinar los objetivos, estrategias y políticas de Seguridad de la Información.
- Determinar los requerimientos de Seguridad de la Información.
- Identificar y analizar las amenazas y las vulnerabilidades de los Activos de Información.
- Identificar y analizar los riesgos de seguridad.
- Especificar salvaguardas adecuadas teniendo en cuenta las amenazas, vulnerabilidades y riesgos identificados.

- Supervisar la implementación y el funcionamiento de las salvaguardas especificadas.
- Asegurar la concienciación de todo el personal en materia de Seguridad de la Información.
- Detectar los posibles incidentes de seguridad y reaccionar ante ellos.

De los análisis realizados en los últimos años relativos a las tendencias en materia de seguridad de la información (Ver anexo I) se pueden obtener algunos datos relevantes sobre la complejidad que puede alcanzar el proceso de Gestión de la Seguridad de la Información en las Organizaciones actualmente:

- Crecimiento de los incidentes provocados por el propio personal de la Organización, no por externos, que hacen ineficaces las medidas establecidas para proteger de los ataques procedentes del exterior por sí solas.
- Crecimiento de los ataques con motivación puramente económica, que conduce a una profesionalización de los atacantes, cada vez más organizados con personas especializadas en la ejecución de las diferentes fases y tareas. Los ataques se vuelven con ello más complejos abarcando el aprovechamiento de debilidades no sólo tecnológicas, sino también operativas, ingeniería social, etc.
- Crecimiento de los ataques diseñados específicamente para atacar objetivos determinados. La difusión de kits que permiten realizar ataques sofisticados a personas sin conocimientos tecnológicos elevados permite que el número de ataques dirigidos aumente.
- Un volumen significativo de pérdidas se debe a debilidades no tecnológicas, como el robo o la pérdida de soportes de información o el abuso de privilegios por parte de usuarios de sistemas de información.
- Aproximadamente la mitad de las Organizaciones encuestadas indica que ha sufrido al menos un incidente de seguridad de la información durante el último año.

- Aumenta el número de ataques de día 0, que se producen antes de que se publique la existencia de la debilidad explotada. Esto supone la necesidad de establecer una disciplina de seguridad que proteja no sólo de las debilidades conocidas, sino también de las que puedan existir sin conocerse. Asimismo, supone la necesidad de reaccionar con presteza ante la publicación de nuevas debilidades, puesto que podrían estar ya siendo explotadas en ese momento.

En los últimos años, la disciplina de la Seguridad de la Información ha experimentado un rápido desarrollo, impulsada por la necesidad de formalizar todas las medidas de seguridad necesarias para proteger la información. De esta forma, el enfoque de la seguridad puramente basado en la tecnología (Seguridad Informática) ha pasado a un enfoque de la seguridad más global (abarcando aspectos tecnológicos, pero también legales, organizativos, culturales, etc.), planteada como un problema de negocio.

El enfoque global y de negocio de la Seguridad de la Información requiere de herramientas de gestión capaces de facilitar a los responsables la toma de decisiones. Entre estas herramientas de gestión, el análisis de riesgos permite identificar y valorar cuáles son aquellas amenazas más relevantes para la seguridad de la información desde un punto de vista de negocio y la eficacia de las salvaguardas establecidas para mitigar los riesgos asociados.

1.2. Análisis de riesgos

Todas las Organizaciones, ya sean públicas o privadas, formales o informales, se crean y mantienen con unos objetivos determinados. [COSO92] [COSO04] [OCDE04]

El universo formado por todos los posibles eventos que pueden afectar de forma negativa al cumplimiento de los objetivos establecidos puede considerarse infinito. Estos eventos pueden tener origen interno o externo, ser fortuitos o intencionados y tener naturalezas absolutamente dispares: riesgo financiero, operativo, tecnológico, de mercado, legal, de seguridad de la información, etc. [COSO92] [COSO04] [BIS03]

De la misma forma, el universo formado por todas las medidas de protección contra dichos eventos es inabarcable por razones de coste. Para gestionar esta complejidad es necesario definir un procedimiento que permita identificar aquellos riesgos que deben tenerse en consideración en contraposición con aquellos que, por su baja probabilidad de ocurrencia, por su bajo impacto o por la dificultad o coste de su mitigación, deberán ser asumidos por la Organización. [ISO13335-2.97] [ISO27005.08]

El análisis de riesgos es una herramienta que permite identificar, clasificar y valorar los eventos que pueden amenazar la consecución de los objetivos de la Organización y establecer las medidas oportunas para reducir el impacto esperable hasta un nivel tolerable. [ISO27005.08] [MAGE06] [ALBER01]

El ejercicio de análisis de riesgos no debe entenderse aislado del resto de iniciativas conducentes a asegurar un nivel de seguridad acorde con los requerimientos de la Organización. En particular, una línea base de seguridad que especifique un conjunto de medidas básicas de seguridad que deben cumplirse en todos los entornos de la Organización permite mitigar un elevado volumen de riesgos cuyo análisis individual sería de otra forma excesivamente compleja. Si existe esta línea base de seguridad, el análisis de riesgos puede centrarse en analizar aquellos riesgos que necesitan una atención, y por tanto, unas medidas de seguridad especiales. [ISO13335-2.97]

El análisis de riesgos de seguridad de la información puede tener distintos destinatarios dentro de la Organización. Cada destinatario necesita esta información con distintos fines, y por ello, necesita recibir la información presentada de forma diferente. Algunos de los principales destinatarios del análisis de riesgos son [UNE71504.08]:

- Responsables de seguridad de la información, en la medida en que les permite obtener y formalizar la información sobre la situación actual y deseable de seguridad, y así definir el plan de acción necesario para cumplir los requerimientos de la Organización.

- Dirección de la Organización, debido a la necesidad de que conozcan la necesidad de establecer medidas contra los riesgos que amenazan la consecución de los objetivos fijados. Asimismo, la Dirección necesita conocer el plan de acción propuesto para alcanzar el nivel de seguridad adecuado y la inversión asociada para tomar las decisiones oportunas y proporcionar la financiación necesaria.
- Auditores, debido a que necesitan obtener y mantener un profundo conocimiento de los riesgos existentes en la Organización, que emplean en su función de evaluar el cumplimiento de las políticas y procedimientos establecidos para mitigarlos.

1.3. Consideración del riesgo

El riesgo, en la medida en que supone una exposición potencial a un impacto negativo para el cumplimiento de los objetivos de una Organización, tiene una connotación negativa.

Sin embargo, el riesgo es una característica inherente a cualquier actividad, y por tanto, no puede considerarse un factor negativo, sino un factor que conviene conocer y gestionar.

El riesgo puede convertirse en una ventaja competitiva para las Organizaciones que sean capaces de gestionarlo adecuadamente. La capacidad de gestionar adecuadamente un elevado nivel de riesgo puede ser un factor diferenciador en la medida en que [JONES05A] [UNE71504.08]:

- La Organización puede operar en circunstancias en las que otras organizaciones no podrían operar con suficiente seguridad. Con frecuencia, la asunción de un mayor nivel de riesgo lleva asociada un mayor retorno de la inversión, que podría denominarse una “prima de riesgo”.

- El mejor control del riesgo permite a la Organización disponer de información de mejor calidad para la toma de decisiones. Por ejemplo, la capacidad de valorar el nivel de riesgo puede permitir determinar si la “prima de riesgo” es proporcionada y justifica la asunción de un riesgo adicional.
- El mejor control del riesgo también permite detectar de forma precoz las desviaciones, proporcionando un mayor tiempo de reacción para la toma de medidas correctoras. Por ejemplo, la detección precoz del mal funcionamiento de un determinado procedimiento de soporte (o de un cambio en el entorno que pueda afectar a un proceso) puede permitir la introducción de controles adicionales, de modo que las deficiencias se corrijan antes de que el impacto sea significativo.
- Por último, un mejor control del riesgo, en la medida en que pueda comunicarse a todos los grupos de interés (accionistas, personal, clientes, proveedores, supervisores, etc.) puede dar ventajas competitivas significativas (mayor acceso a la financiación, facilidad para retener el talento, facilidad para lograr y fidelizar clientes, etc.). Existen diversos mecanismos para la comunicación de este mayor nivel de control a todos los grupos de interés:
 - Publicación de memorias de gestión donde conste el compromiso de la Organización con la gestión del riesgo y el enfoque general empleado en su gestión. Por ejemplo, estas memorias forman parte de las memorias anuales de actividad que publican todas las empresas cotizadas.

- Obtención de certificaciones, por las que un tercero independiente y autorizado para ello da fe de la calidad de algún aspecto determinado de la gestión. Entre las certificaciones más frecuentes pueden citarse ISO 9001 (Sistema de gestión de la calidad), ISO 14001 (Sistema de gestión medioambiental), ISO 27001 (Sistema de gestión de seguridad de la información) [ISO27001.05], ISO 18001-OHSAS (Sistema de gestión de prevención de riesgos laborales), ISO 28001 (Sistema de gestión de seguridad en la cadena de suministro), AICPA Webtrust (Gestión de seguridad para entidades de certificación, utilizado frecuentemente en el ámbito del comercio electrónico) [AICPA00] [AICPA08], etc.
- Menor desviación en el cumplimiento de los objetivos planteados.
- Menor ocurrencia de defectos de control que puedan reflejarse en los medios de comunicación, ya sean sectoriales o generales.

Esta doble faceta del riesgo como amenaza y como oportunidad se refleja en la existencia de dos términos afines utilizados para denominar la cantidad de riesgo que gestionan las organizaciones [JONES05A] [UNE71504.08]:

- Se denomina tolerancia al riesgo a la cantidad de riesgo que una Organización es capaz de gestionar.
- Se denomina apetito de riesgo a la cantidad de riesgo que una Organización está dispuesta a gestionar para lograr los objetivos establecidos.

2. OBJETIVOS

Existen múltiples motivos para que la Organización haya decidido elaborar un análisis de riesgos de Seguridad de la Información. Entre los más importantes cabe citar los siguientes:

2.1. Racionalizar la inversión en seguridad de la información.

Todas las medidas de seguridad de la información tienen un coste asociado a su implantación y a su mantenimiento. Esto es lo que se conoce como el coste de la seguridad. [MAGE06]

Estos costes, a su vez, pueden ser directos o indirectos, y en ocasiones difíciles de acotar con precisión. [MAGE06] [JONES05A]

Por ejemplo, la implantación de un sistema de control de acceso a los sistemas de información mediante tarjetas criptográficas, puede involucrar, entre otros, los siguientes costes:

- Costes directos:
 - Adaptación de la infraestructura tecnológica y las aplicaciones informáticas para la utilización de las tarjetas.
 - Desarrollo, implantación y mantenimiento de la CA (Autoridad de Certificación) correspondiente (hardware, software, políticas, claves, etc.)
 - Especificación formal de los permisos de cada perfil de usuario a definir, tanto a nivel de aplicaciones como a nivel de permisos dentro de cada aplicación.
 - Producción y distribución de las tarjetas, incluyendo los procedimientos para la autenticación de los usuarios correspondiente a la RA (Autoridad de Registro).

- Instalación de lectores de tarjetas en los equipos que no dispongan de ellos.
- Costes indirectos:
 - Incremento de la actividad de los servicios de soporte por incidencias con los lectores de tarjetas o con las propias tarjetas.
 - Necesidad de emitir tarjetas temporales para el caso en que un usuario no disponga de la tarjeta en un momento dado.
 - Tiempo de usuario perdido durante la resolución de las incidencias relacionadas con las tarjetas.
 - Incremento en el uso de la red por parte de las aplicaciones, que ya no dependen de sí mismas para autenticar a los usuarios.
 - Espacio de almacenamiento del stock de tarjetas.
 - Gestión segura de las claves criptográficas maestras: almacenamiento seguro y segregado, asignación de la función de custodia de claves al personal, necesidad de disponer de personal suplente.
 - Medidas de control interno necesarias para garantizar el nivel de seguridad de la PKI (supervisión, auditorías, etc.)

Asimismo, la falta de medidas de seguridad también tiene un coste asociado para las Organizaciones, en forma de incidentes de seguridad que producen pérdidas. Esto es lo que se conoce el coste de la inseguridad. [MAGE06]

Los costes de la inseguridad también pueden ser directos o indirectos, y también pueden ser difíciles de acotar con precisión. [MAGE06]

Por ejemplo, el extravío de un soporte con información de pedidos de clientes puede suponer, entre otros, los siguientes costes:

- Costes directos:
 - Reemplazo del soporte extraviado (generalmente supondrá un coste despreciable).

- Reemplazo de la información extraviada, bien sea a partir de datos disponibles en la Organización o contactando nuevamente con los clientes.
- Costes indirectos:
 - Costes legales, por incumplimiento de leyes como la Ley de Protección de Datos o los acuerdos de confidencialidad con los clientes.
 - Costes reputacionales, debidos a la pérdida de confianza de los clientes, o del público en general si la noticia tiene una difusión amplia.
 - Costes comerciales, debidos al retraso en el servicio de los pedidos.
 - Costes de gestión, debidos al personal que debe dedicarse a recopilar de nuevo la información perdida y a proceder con el nuevo procedimiento de gestión de los pedidos.

Un objetivo de cualquier Organización es minimizar el coste total, tomado como la suma del coste de la seguridad y el coste de la inseguridad. [MAGE06]

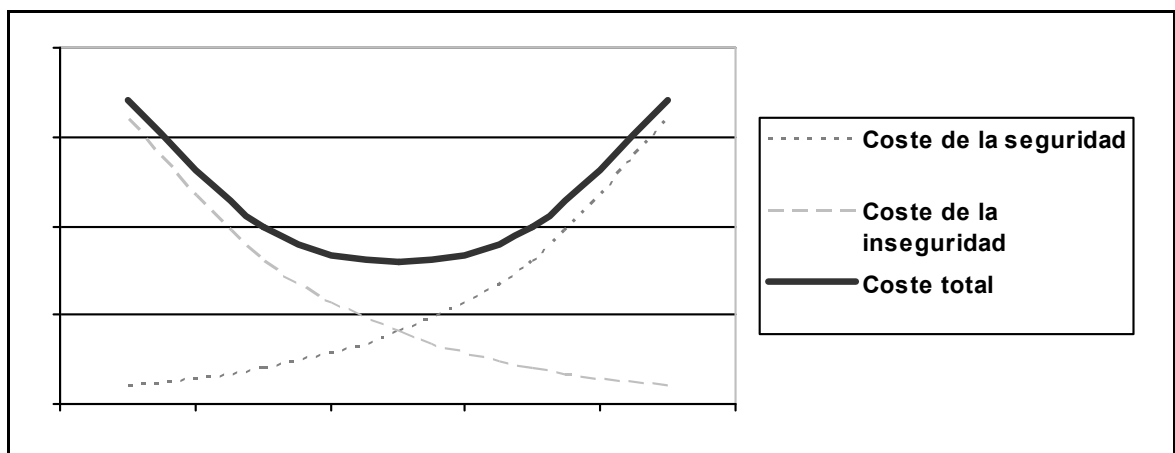


Figura 1: Coste de la seguridad y de la inseguridad

El análisis de riesgos permite cuantificar cuál es el coste de la inseguridad (riesgo) que asume una Organización en un momento determinado, y cómo evoluciona este coste en función de las medidas de seguridad que se implementen. De esta forma el análisis de riesgos permite determinar cuándo una determinada medida de seguridad va a suponer una reducción del riesgo menor que su propio coste, y, por tanto, no es aconsejable su implantación desde un punto de vista económico. [MAGE06]

Es importante destacar que no se considera posible la reducción del riesgo a 0. El objetivo del análisis y la gestión de riesgos no es la eliminación completa del riesgo, sino su reducción a unos niveles tolerables por la Organización en función de su apetito al riesgo. [MAGE06] [JONES05A]

2.2. Formalizar la toma de decisiones

El abanico de medidas de seguridad que la Organización puede considerar para proteger su información es muy amplio. Existen diversos marcos de referencia y códigos de buenas prácticas (por ejemplo ISO/IEC 27002 [ISO27002.05], COBIT [ISACA07], ITIL-ISO/IEC 20000 [ITIL06] [ISO20000-2.05], NIST SP 800-53 [NIST800-53.04], etc.) que contienen centenares de medidas de seguridad que se pueden considerar.

El presupuesto de Seguridad de la Información es limitado para plantear la implantación completa de cualquiera de los marcos de referencia o códigos de buenas prácticas hasta el máximo nivel de cumplimiento.

Además, es virtualmente imposible la implantación simultánea de un número tan elevado de controles con los recursos disponibles en la Organización.

Por este motivo, los responsables de Seguridad de la Información necesitan mecanismos que les faciliten priorizar las medidas a implantar y que les permitan justificar las decisiones tomadas en ese sentido.

El análisis de riesgos permite determinar cuáles son los principales riesgos de Seguridad de la Información que afronta la Organización, teniendo en cuenta las medidas de seguridad ya implantadas. Con esta información, el Responsable de Seguridad puede determinar cuáles son las medidas que reducen en mayor medida este riesgo, y con ello, cuáles debe priorizar.

La formalización implica que el análisis debe aportar dos características fundamentales:

- Objetividad, en la medida en que diferentes personas, aplicando el mismo procedimiento sobre los mismos datos, deberían obtener resultados idénticos.
- Valoración, de modo que todos los riesgos y las medidas de seguridad potencialmente aplicables para mitigarlos quedan priorizadas utilizando una escala que puede ser numérica (en el caso del análisis cuantitativo) o literal (en el caso del análisis cualitativo).

2.3. Cumplir con las normativas aplicables

Existen algunos requerimientos normativos y regulatorios que implícita o explícitamente reconocen la necesidad de llevar a cabo un análisis de riesgos para adecuar las medidas de seguridad a las circunstancias específicas de la Organización. En España cabe destacar:

- Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y sus desarrollos reglamentarios
- Real Decreto 263/1996, de 16 de Febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.

El análisis de riesgos es considerado una pieza fundamental para la Seguridad de la Información por diversos estándares y códigos de buenas prácticas. Algunos ejemplos de estándares y códigos de buenas prácticas que prescriben la realización de análisis de riesgos son:

- Directrices de la OCDE para la seguridad de sistemas y redes de información [OCDE02]
- ISO/IEC 27001:2005 Tecnología de Información – Técnicas de seguridad – Sistemas de Gestión de Seguridad de la Información – Requerimientos [ISO27001.05]
- ISO/IEC 27002:2005 Tecnología de Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información [ISO27002.05]
- BS 25999:2006 Gestión de continuidad de negocio [BS25999-1.06] [BS25999-2.07]
- ITIL – Information Technology Infrastructure Library [ITIL06]
- ISO/IEC 20000 Tecnología de información – Gestión del servicio [ISO20000-1.05] [ISO20000-2.05]
- COBIT – Control OBjectives for Information and related Technology [ISACA07]
- Criterios de Seguridad, Normalización y Conservación de las aplicaciones utilizadas para el ejercicio de potestades
- NIST SP 800-53 Controles de seguridad recomendados para los sistemas de información federales [NIST800-53.04]
- PCI DSS Payment Card Industry Data Security Standards [PCI08]

Adicionalmente, diversas regulaciones establecen la necesidad de implantar un modelo de análisis de riesgos a nivel corporativo dentro del que la Seguridad de la Información debería ser una parte constituyente. Algunas de estas regulaciones son:

- Códigos de buen gobierno corporativo, en España, el Informe Olivencia, el Informe Aldama y el Código Unificado de Buen Gobierno.
- Dentro del sector bancario, Basilea II [BIS04], y especialmente el Pilar I de cálculo de los requisitos mínimos de capital regulatorio, que toma como uno de sus parámetros el cálculo del riesgo operacional, y el Pilar II de supervisión de la gestión de los fondos propios, en la medida en que establece la creación de un sistema de control interno.
- Dentro del sector asegurador, Solvencia II, especialmente el Pilar II referente al proceso de supervisión, que establece la creación de un sistema de control interno.
- En el ámbito norteamericano, pero que afecta a las filiales relevantes de empresas cotizadas, la Ley Sarbanes Oxley establece la obligación de crear un sistema de control interno basado en el marco de referencia de COSO [COSO92]. En el ámbito de los sistemas de información, el marco de referencia utilizado con mayor frecuencia en conjunción con COSO es COBIT [ISACA07], ya citado en el apartado anterior. Existen unos desarrollos legislativos equivalentes en Japón (conocidos coloquialmente como J-SOX) y en la Comunidad Europea (Octava directiva, conocida coloquialmente como EuroSOX), cuya repercusión ha sido menor.

En el anexo II de este documento se incluyen algunos extractos de las principales referencias al análisis de riesgos recogidas de leyes, reglamentos, normas, códigos de buenas prácticas y marcos de control, aplicables o de uso extendido en el ámbito español.

3. PLANTEAMIENTO DEL PROBLEMA

Se pretende realizar un análisis de riesgos de seguridad de la información que permita a la Organización:

- Definir formalmente los requerimientos de Seguridad de la Información en función de sus necesidades, y con ello dimensionar adecuadamente la inversión y la estructura necesaria para soportar la Seguridad de la Información. [ISO27001.05] [ISO27002.05]
- Definir un Programa de Seguridad de la Información formal basado en estándares internacionales. [ISO27005.08] [NIST800-18.98]
- Establecer un Sistema de Gestión de Seguridad de la Información (SGSI) conforme al estándar ISO/IEC 27001:2005, con el objetivo de hacer sostenibles en el tiempo todas las iniciativas en materia de Seguridad de la Información. [ISO27001.05]
- Certificar el SGSI desarrollado para demostrar ante la propia Organización y ante cualquier tercero interesado el compromiso y la dedicación a la Seguridad de la Información por parte de la Organización. [ISO27001.05]
- Desarrollar una metodología de análisis de riesgos que conjugue la compatibilidad con las metodologías estándar existentes en la actualidad con las necesidades específicas de la Organización en la materia.
- Desarrollar una herramienta que facilite la realización del análisis de riesgos y su posterior mantenimiento.

4. ESTADO DE LA CUESTIÓN

A continuación se describen brevemente los principales modelos y metodologías de análisis de riesgos estándar.

Se describen por separado los modelos y las metodologías definidos para el análisis de riesgos de seguridad de la información, los modelos y metodologías definidos para el análisis de riesgos corporativos y los modelos y metodologías definidos para propósitos específicos.

4.1. Análisis de riesgos de seguridad de la información

4.1.1. Conceptos generales

A pesar de que existe un elevado número de metodologías de análisis de riesgos de seguridad de la información, que se describen posteriormente en este documento, existe un modelo y unos principios básicos comunes a todas ellas que se describen a continuación. [GLAM04] [VORST05] [ENISA06] [ISC2.04] [HARRIS06] [ISACA06] [ISACA08]

La base sobre la que se apoyan las metodologías actuales de análisis de riesgo es el cálculo de probabilidades, según la secuencia que se describe a continuación.

4.1.1.1. Elementos del modelo

Las metodologías de análisis de riesgos de seguridad de la información parten de la necesidad de identificar formalmente los elementos a proteger. Estos elementos se recogen en un inventario de activos de información, considerando como tales aquellos elementos que tienen valor para la Organización. [MAGE06]

Los activos deben valorarse en función de un conjunto de requerimientos de seguridad. Estos requerimientos varían entre las diferentes metodologías, si bien existe consenso sobre tres de ellas: confidencialidad, integridad y disponibilidad. Esto significa que para cada activo de información debe valorarse de forma independiente el coste que tendría para la Organización una pérdida total de su confidencialidad, de su integridad y de su disponibilidad, así como de los otros requerimientos de seguridad que se consideren en cada caso. [MAGE06]

Una vez identificados los activos, deben identificarse las amenazas que pueden causar pérdidas sobre estos activos, teniendo en cuenta los diferentes requerimientos de seguridad. Algunas metodologías especifican un elemento intermedio, las vulnerabilidades, consideradas como las debilidades que hacen que un determinado activo pueda ser vulnerable a una determinada amenaza. [ALBER01]

Identificadas las amenazas, debe identificarse las salvaguardas que permiten proteger a los activos de las diferentes amenazas. [CRAMM03]

La cuantificación de los distintos elementos que forman parte del modelo de análisis de riesgos se aborda en los siguientes apartados.

4.1.1.2. Pérdida esperada (Single Loss Expectancy – SLE)

Considerando un único activo de información (A), un único requerimiento de seguridad (R) y una única amenaza (T) se puede estimar la pérdida económica esperada en caso de que la amenaza se realice. [ISC2.04] [JONES05A]

Generalmente, la pérdida esperada no se representa en términos absolutos, sino como un porcentaje de degradación referido al valor total del activo para el requerimiento considerado. De esta forma, se puede considerar:

$$SLE(A, R, T) = \text{Valor (A, R)} \times \text{Degradación(A, R, T)}$$

Dado que la valoración se realiza generalmente respecto a diferentes requerimientos de seguridad (confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad, etc.), la pérdida total debida a la realización de una amenaza sobre un activo se calculará como la suma de las pérdidas en cada requerimiento:

$$SLE(A, T) = \sum_R SLE(A, R, T) = \sum_R \text{Valor}(A, R) \times \text{Degradación}(A, R, T)$$

Dado que existen diversos activos a los que puede afectar la amenaza considerada, la pérdida esperada total es la suma de la pérdida provocada en cada uno de los activos:

$$SLE(T) = \sum_A SLE(A, T) = \sum_A \sum_R \text{Valor}(A, R) \times \text{Degradación}(A, R, T)$$

4.1.1.3. Pérdida anual esperada (Annual Loss Expectancy – ALE)

Una vez conocida la pérdida provocada por la realización de cada amenaza, en caso de que ocurra, se debe considerar la probabilidad de que la amenaza se realice efectivamente en el periodo de un año. La pérdida anual esperada provocada por una amenaza puede definirse, por tanto, como [ISC2.04] [JONES05A]:

$$ALE(T) = P(T) \times SLE(T) = P(T) \times \sum_A \sum_R \text{Valor}(A, R) \times \text{Degradación}(A, R, T)$$

La pérdida anual esperada teniendo en cuenta todas las amenazas puede definirse, por tanto, como:

$$\begin{aligned} ALE &= \sum_T P(T) \times SLE(T) = \\ &= \sum_T \left(P(T) \times \sum_A \sum_R \text{Valor}(A, R) \times \text{Degradación}(A, R, T) \right) \end{aligned}$$

Debido a que existen amenazas para las que se espera más de una ocurrencia anual, el concepto de probabilidad se sustituye por el concepto de frecuencia (Annual Rate of Occurrence – ARO). Por ello, la definición de pérdida anual esperada queda ligeramente modificada como:

$$\begin{aligned} ALE &= \sum_T ARO(T) \times SLE(T) \\ &= \sum_T \left(ARO(T) \times \sum_A \sum_R Valor(A, R) \times Degradación(A, R, T) \right) \end{aligned}$$

El concepto de riesgo intrínseco se asocia habitualmente a la pérdida anual estimada, y se representa de forma equivalente como:

$$\begin{aligned} \text{Riesgo intrínseco} &= \text{Frecuencia} \times \text{Impacto} = \\ &= \text{Frecuencia} \times \text{Valor} \times \text{Degradación} = ALE \end{aligned}$$

4.1.1.4. Cálculo del efecto de las salvaguardas

Las salvaguardas (S) implantadas permiten reducir la frecuencia de ocurrencia de las amenazas o la degradación causada por ellas en caso de realizarse [ISC2.04] [MAGE06].

Teniendo en cuenta la reducción de la frecuencia, se puede considerar P(S) la probabilidad de que una salvaguarda sea eficaz en la prevención de la ocurrencia de una amenaza determinada. Por tanto, puede considerarse que:

$$P(A/S_i) = P(A) \times (1 - P(S_i))$$

Dado el conjunto de salvaguardas implantadas, la probabilidad de ocurrencia puede calcularse como:

$$P(A/S) = P(A) \times \prod_S (1 - P(S))$$

Siendo P(S) la probabilidad de que la salvaguarda S sea eficaz mitigando la amenaza A.

Considerando el concepto de frecuencia en lugar del de probabilidad, la frecuencia anual de ocurrencia se puede calcular como:

$$ARO' = ARO \times \prod_S (1 - P(S))$$

De forma análoga, se puede calcular la degradación una vez aplicadas las salvaguardas:

$$\text{Degradación}(A, R, T)' = \text{Degradación}(A, R, T) \times \prod_S (1 - I(S))$$

Donde $I(S)$ es la reducción del impacto provocado por la acción de la salvaguarda S .

Por tanto, el cálculo del riesgo residual puede definirse como:

$$ALE = \sum_T \left(ARO(T) \times \prod_S (1 - P(S)) \times \sum_A \sum_R \text{Valor}(A, R) \times \text{Degradación}(A, R, T) \times \prod_S (1 - I(S)) \right)$$

Debido al elevado coste computacional de estos cálculos, algunas metodologías simplifican el cálculo definiendo un porcentaje fijo de reducción de la probabilidad y de la degradación para cada salvaguarda implantada. De esta forma:

$$ARO'' = ARO \times \sum_i \Delta P_i$$

$$\text{Degradación}(A, R, T)' = \text{Degradación}(A, R, T) \times \sum_i \Delta I_i$$

4.1.1.5. Relaciones entre los activos

Los activos de información tienen relaciones de dependencia que afectan adicionalmente al cálculo de los riesgos. Para simplificar la notación, no se tendrán en cuenta en este apartado los distintos requerimientos considerados en el análisis de riesgos [MAGE06].

Dados dos activos A y B, de forma que el activo A depende del activo B, el valor del activo B (para cada uno de los requerimientos de seguridad considerados), a efectos del análisis de riesgos, puede incrementarse con el valor del activo A, debido a que la realización de una amenaza sobre el activo B no sólo provocará la degradación correspondiente del activo B, sino también una degradación proporcional en el activo A. Esto se conoce como Valor acumulado.

$$\text{Valor acumulado (B)} = \text{Valor (B)} + \text{Valor (A)}$$

Considerando adicionalmente que la dependencia entre los activos puede no ser total, sino estar expresada en forma de un porcentaje, queda:

$$\text{Valor acumulado (B)} = \text{Valor (B)} + \text{Valor (A)} \times \text{Dependencia (A, B)}$$

En caso de realizarse una amenaza T sobre el activo B, las pérdidas podrían estimarse como el impacto sobre B más el impacto sobre A soportado por B:

$$\text{SLE}'(\text{B}) = \text{SLE (B)} + \text{SLE (A)}$$

$$\begin{aligned} \text{SLE}'(\text{B}) = & \text{Valor (B)} \times \text{Impacto (B, T)} + \\ & + \text{Dependencia (A, B)} \times \text{Valor (A)} \times \text{Impacto (B, T)} \end{aligned}$$

$$\text{SLE}'(\text{B}) = (\text{Valor (B)} + \text{Dependencia (A, B)} \times \text{Valor (A)}) \times \text{Impacto (B, T)}$$

El riesgo total de B puede estimarse como la suma entre el riesgo propio de B más el riesgo de A soportado por B:

$$\begin{aligned} \text{Riesgo (B)} = & (\text{Valor (B)} + \text{Dependencia (A, B)} \times \text{Valor (A)}) \times \\ & \times \text{Impacto (B, T)} \times P(\text{B, T}) \end{aligned}$$

De forma análoga, dado el mismo caso de dos activos A y B, siendo A dependiente de B en cierto porcentaje, y dada una determinada amenaza T, el efecto de la realización de la amenaza sobre el activo A debe tener en cuenta también la dependencia del activo B. De esta forma, se puede considerar el cálculo del riesgo total sobre A como el riesgo intrínseco más el riesgo repercutido por B:

$$\text{Riesgo}(A) = \text{Riesgo}(A) + \text{Riesgo Repercutido}(B)$$

$$\begin{aligned} \text{Riesgo}(A) = & P(A, T) \times \text{Valor}(A) \times \text{Impacto}(A, T) + \\ & + \text{Dependencia}(A, B) \times P(B, T) \times \text{Valor}(A) \times \text{Impacto}(B, T) \end{aligned}$$

$$\begin{aligned} \text{Riesgo}(A) = & \text{Valor}(A) \times (P(A, T) \times \text{Impacto}(A, T) + \\ & + \text{Dependencia}(A, B) \times P(B, T) \times \text{Impacto}(B, T)) \end{aligned}$$

El cálculo de los distintos parámetros acumulados o repercutidos cobra interés especialmente en la obtención de resultados parciales del análisis, teniendo en cuenta sólo un determinado activo o una determinada amenaza.

4.1.1.6. Métodos cualitativos

Los conceptos desarrollados hasta ahora muestran los principios básicos para un análisis de riesgos cuantitativo, basado en el cálculo de pérdidas en términos monetarios.

La valoración de los diferentes requerimientos de seguridad puede realizarse de forma cuantitativa o cualitativa [ISC2.04] [MAGE06]:

- La **valoración cuantitativa** supone establecer un valor numérico para cada uno de los requerimientos de seguridad. Este valor se calcula en términos de las pérdidas esperadas en caso de incumplimiento de dicho requerimiento. Los principales conceptos de pérdidas a tener en cuenta en una valoración cuantitativa incluyen los siguientes:
 - Coste de reposición de los activos y recursos de información perdidos: adquisición, instalación, recuperación, etc.

- Coste de mano de obra invertida en recuperar y/o reponer los activos y recursos de información.
- Lucro cesante debido a la pérdida de ingresos provocada por la parada o degradación del funcionamiento de los diferentes procesos afectados.
- Capacidad de operar, debido a la pérdida de confianza de los clientes y proveedores, que se traduce en una pérdida de actividad o en peores condiciones económicas.
- Sanciones y penalizaciones por incumplimiento de la ley u obligaciones contractuales.
- Daño a otros activos, propios o ajenos
- Daño a personas.
- Daños medioambientales.
- Daños reputacionales: percepción del mercado, pérdida de clientes, dificultad para acceder al crédito, coste de las campañas de marketing necesarias para recuperar la reputación perdida, etc.
- Valor de los secretos desvelados: secreto industrial, secreto comercial, etc.
- La **valoración cualitativa** supone asignar un valor de una escala definida para cada uno de los requerimientos de seguridad. Este valor se calcula en base a un conjunto de características que define cada una de las categorías de la escala, basadas en las descritas para la valoración cuantitativa.

La valoración cuantitativa es más precisa, pero supone un mayor esfuerzo y dificultad, por la necesidad de valorar los distintos conceptos de pérdida en términos generalmente económicos.

Debido a la dificultad y el coste de realizar un análisis cuantitativo, muchas metodologías de análisis de riesgos han desarrollado enfoques cuantitativos, que permiten ubicar el riesgo en una escala de órdenes de magnitud. Este análisis se conoce como análisis cualitativo.

Los principios del análisis cualitativo son los mismos que los del análisis cuantitativo, sustituyendo los cálculos aritméticos por la aplicación de tablas.

De esta forma, considerando que el valor de los activos y la degradación causada por una determinada amenaza están valorados en una escala de tres niveles (Alto, Medio, Bajo), y dado que:

$$\text{Impacto} = \text{Valor} \times \text{Degradación}$$

Se puede estimar el orden de magnitud del impacto utilizando la siguiente tabla:

Impacto			Degradación		
			Baja	Media	Alta
Valor		Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto

Tabla 1: Cálculo cualitativo del impacto

De forma análoga al impacto, el riesgo puede definirse como:

$$\text{Riesgo} = \text{Frecuencia} \times \text{Impacto}$$

Y puede calcularse con la siguiente tabla:

Riesgo		Impacto		
		Bajo	Medio	Alto
Probabilidad	Baja	Bajo	Bajo	Medio
	Media	Bajo	Medio	Alto
	Alta	Medio	Alto	Alto

Tabla 2: Cálculo cualitativo del riesgo

Por último, el cálculo del riesgo residual puede definirse como:

Riesgo residual = Riesgo intrínseco - riesgo mitigado por las salvaguardas

Y puede calcularse con la siguiente tabla:

Riesgo residual		Riesgo intrínseco		
		Bajo	Medio	Alto
Salvaguardas	Bajas	Bajo	Bajo	Medio
	Medias	Bajo	Medio	Alto
	Altas	Medio	Alto	Alto

Tabla 3: Cálculo cualitativo del riesgo residual

La elaboración de las tablas puede variar en función de las diferentes metodologías o necesidades de cada análisis. A continuación se muestran dos ejemplos de tablas utilizando las funciones máximo, mínimo y media:

Mínimo		Parámetro 2		
		Bajo	Medio	Alto
Parámetro 1	Bajo	Bajo	Bajo	Bajo
	Medio	Bajo	Medio	Medio
	Alto	Bajo	Medio	Alto

Tabla 4: Cálculo cualitativo mediante la función mínimo

Máximo			Parámetro 2		
			Bajo	Medio	Alto
Parámetro 1		Bajo	Bajo	Medio	Alto
		Medio	Medio	Medio	Alto
		Alto	Alto	Alto	Alto

Tabla 5: Cálculo cualitativo mediante la función máximo

Media			Parámetro 2		
			Bajo	Medio	Alto
Parámetro 1		Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto

Tabla 6: Cálculo cualitativo mediante la función media

Es posible convertir valores en diferentes escalas, por ejemplo, a continuación se toman dos parámetros en una escala de tres niveles y se obtiene un resultado en una escala de cinco niveles:

Media			Parámetro 2		
			Bajo	Medio	Alto
Parámetro 1		Bajo	Muy baja	Baja	Media
		Medio	Baja	Media	Alta
		Alto	Media	Alta	Muy alta

Tabla 7: Cálculo cualitativo utilizando dos escalas

A continuación se muestra el paso inverso al caso anterior: la conversión de dos escalas de cinco niveles a una escala de tres niveles:

Media		Parámetro 2				
		Muy bajo	Bajo	Medio	Alto	Muy Alto
Parámetro 1	Muy bajo	Baja	Baja	Baja	Media	Media
	Bajo	Baja	Baja	Media	Media	Media
	Medio	Baja	Media	Media	Media	Alta
	Alto	Media	Media	Media	Alta	Alta
	Muy alto	Media	Media	Alta	Alta	Alta

Tabla 8: Cálculo cualitativo utilizando dos escalas

4.1.1.7. Métodos mixtos

Debido a que los métodos cuantitativos y cualitativos tienen ventajas e inconvenientes, existen alternativas para combinar ambos métodos de forma que se obtengan las mayores ventajas de cada uno. Esos métodos que presentan algunas características de los métodos cuantitativos y otras características de los métodos cualitativos se denominan métodos mixtos [ISC2.04].

4.1.1.8. Ejemplo

Para ilustrar los conceptos expuestos en los apartados anteriores, a continuación se incluye un ejemplo simplificado de un análisis de riesgos cuantitativo.

Sea un proceso comercial de una organización en el que se han identificado dos activos de información: clientes y clientes potenciales.

La información de clientes está soportada por la aplicación comercial, y la información de clientes potenciales por la aplicación de marketing. Ambas aplicaciones residen en un mismo servidor, que, por tanto, también soporta ambos activos de información. Todos estos elementos se conocerán como recursos de información.

Existe un estándar de seguridad que protege todos los sistemas de información, y la aplicación comercial, por considerarse más relevante, tiene medidas de seguridad adicionales.

Se considera que existen sólo dos amenazas: incendio y acceso no autorizado a las aplicaciones.

Se desea analizar sólo dos requerimientos de seguridad: Confidencialidad y Disponibilidad.

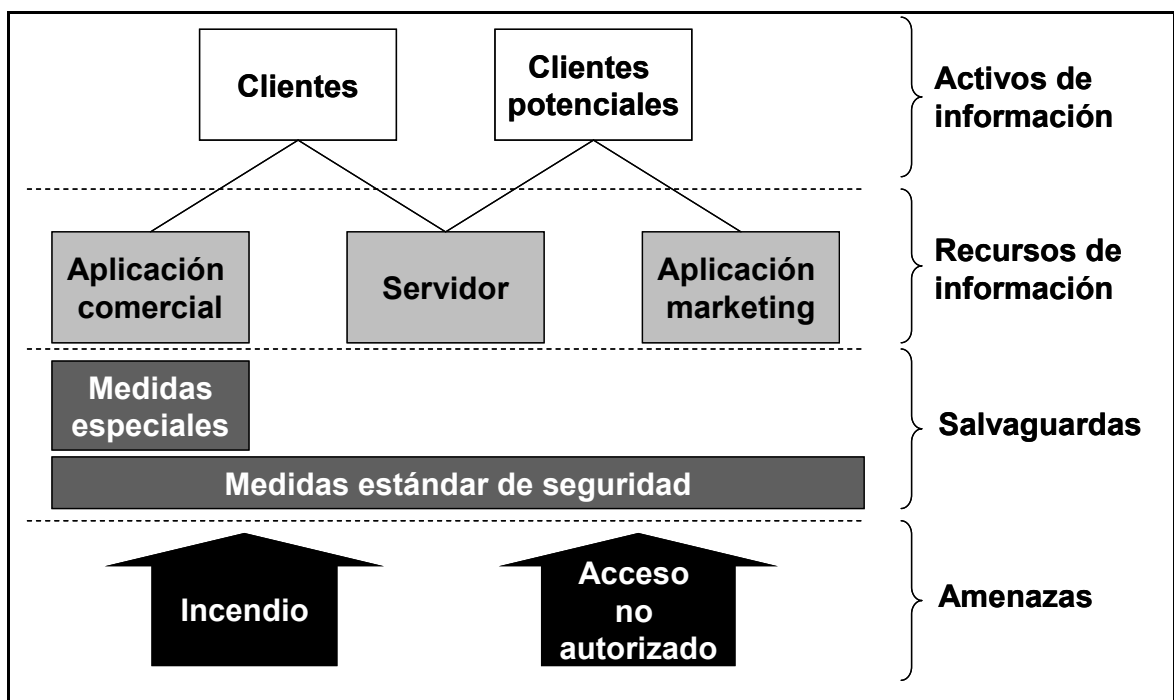


Figura 2: Ejemplo análisis de riesgos

En primer lugar, es necesario conocer el valor de todos los elementos, para lo cual se entrevista a los responsables comerciales de la Organización, y se obtienen los siguientes resultados:

Activo	Requerimiento	Valor	Justificación
Información de clientes	Confidencialidad	10.000	Sanciones y el deterioro de relaciones con clientes
	Disponibilidad	100.000	Lucro cesante, al perderse el perfil comercial de los clientes.
Información de clientes potenciales	Confidencialidad	2.000	Sanciones
	Disponibilidad	1.000	Obtención de bases de datos comerciales y consolidación de información de comerciales

Tabla 9: Planteamiento del caso práctico de análisis de riesgos – Listado de activos

El valor de las aplicaciones y del servidor como tales, se considera despreciable en comparación con el valor de los activos de información que soportan, por lo que se considera que su valor es cero. Sin embargo, esos elementos tienen un valor soportado debido al valor de los activos que soportan:

Recurso	Requerimiento	Valor (€)	Justificación
Aplicación comercial	Confidencialidad	10.000	Información de clientes
	Disponibilidad	100.000	Información de clientes
Aplicación de marketing	Confidencialidad	2.000	Información de clientes potenciales
	Disponibilidad	1.000	Información de clientes potenciales
Servidor	Confidencialidad	12.000	Información de clientes + Información de clientes potenciales
	Disponibilidad	101.000	Información de clientes + Información de clientes potenciales

Tabla 10: Planteamiento del caso práctico de análisis de riesgos - Listado de recursos

Una vez valorados los activos, se necesita conocer y valorar sus amenazas. La valoración de las amenazas, obtenido de entrevistas con los responsables es la siguiente:

Amenaza	Frecuencia	Degradación			
		Aplicaciones		Servidores	
		Confidenc.	Disponib.	Confidenc.	Disponib.
Incendio	0,1	0 %	0 %	0 %	100 %
Acceso no autorizado	5	50 %	0 %	0 %	0 %

Tabla 11: Caso práctico de análisis de riesgos: cálculo de la degradación

La información como concepto no tiene amenazas, si no es a través de los sistemas que la almacenan y/o procesan. El impacto de las amenazas sobre la información se calcula como la suma de las amenazas repercutidas por los recursos que la soportan.

Con la valoración de los activos y los recursos, y atendiendo a la degradación que causan en ellos las amenazas, es posible calcular la pérdida esperada (SLE – Single Loss Expectancy) en caso de que se realice alguna de las amenazas:

Activo / Recurso	SLE			
	Incendio		Acceso no autorizado	
	Confidenc.	Disponib.	Confidenc.	Disponib.
	Valor x Degradación	Valor x Degradación	Valor x Degradación	Valor x Degradación
Clientes	$10.000 \times (0\% + 0\%) = 0$	$100.000 \times (0\% + 50\%) = 50.000$	$10.000 \times (100\% + 0\%) = 10.000$	$100.000 \times (0\% + 0\%) = 0$
Clientes potenciales	$2.000 \times (0\% + 0\%) = 0$	$1.000 \times (0\% + 50\%) = 500$	$2.000 \times (100\% + 0\%) = 2.000$	$1.000 \times (0\% + 0\%) = 0$
Aplicación comercial	$10.000 \times 0\% = 0$	$100.000 \times 0\% = 0$	$10.000 \times 100\% = 10.000$	$100.000 \times 0\% = 0$
Aplicación marketing	$2.000 \times 0\% = 0$	$1.000 \times 0\% = 500$	$2.000 \times 100\% = 2.000$	$1.000 \times 0\% = 0$
Servidor	$12.000 \times 0\% = 0$	$101.000 \times 50\% = 50.500$	$12.000 \times 0\% = 0$	$101.000 \times 0\% = 0$
TOTAL	0	$50.000 + 500 = 50.500$	$10.000 + 2.000 = 2.000$	0
		$0 + 50.500 = 50.500$		$2.000 + 0 = 2.000$

Tabla 12: Caso práctico de análisis de riesgos - Cálculo de la pérdida esperada

La suma de las pérdidas estimadas debe realizarse teniendo en cuenta sólo los activos (riesgo repercutido) o los recursos (riesgo soportado), para evitar que se duplique el resultado obtenido.

Una vez calculada la pérdida esperada en caso de que se realice cada amenaza se puede calcular la pérdida anual esperada, teniendo en cuenta la frecuencia con la que se realiza cada amenaza:

Activo / Recurso	ALE = Riesgo intrínseco			
	Incendio		Acceso no autorizado	
	Confidenc.	Disponibilidad	Confidenc.	Disponibilidad
	Frecuencia x SLE	Frecuencia x SLE	Frecuencia x SLE	Frecuencia x SLE
Clientes	$0,1 \times 0 = 0$	$0,1 \times 50.000 = 5.000$	$5 \times 10.000 = 50.000$	$5 \times 0 = 0$
Clientes potenciales	$0,1 \times 0 = 0$	$0,1 \times 500 = 50$	$5 \times 2.000 = 10.000$	$5 \times 0 = 0$
Aplicación comercial	$0,1 \times 0 = 0$	$0,1 \times 0 = 0$	$5 \times 10.000 = 50.000$	$5 \times 0 = 0$
Aplicación marketing	$0,1 \times 0 = 0$	$0,1 \times 500 = 50$	$5 \times 2.000 = 10.000$	$5 \times 0 = 0$
Servidor	$0,1 \times 0 = 0$	$0,1 \times 50.500 = 5.050$	$5 \times 0 = 0$	$5 \times 0 = 0$
TOTAL	0	$50.00 + 50 = 50.50$	$50.000 + 10.000 = 60.000$	0
		$0 + 50.500 = 50.500$		$2.000 + 0 = 2.000$

Tabla 13: Caso práctico de análisis de riesgos - Cálculo de la pérdida anual esperada

Por tanto, si no existieran salvaguardas, la Organización sufriría unas pérdidas estimadas de 52.500 € anuales debidas a incidentes de seguridad de la información.

Para valorar el efecto de las salvaguardas es necesario estimar su eficacia, teniendo en cuenta diversos factores. En este ejemplo se supone que:

- Las salvaguardas estándar implantadas reducen un 90% la probabilidad de que se realicen las amenazas.

- Las salvaguardas estándar implantadas reducen un 80% la degradación en caso de que se realicen las amenazas.
- Las salvaguardas adicionales sobre la aplicación comercial elevan la reducción de la probabilidad de que se produzca un acceso no autorizado hasta el 95%.
- Las salvaguardas adicionales sobre la aplicación comercial elevan la reducción de la degradación en caso de acceso no autorizado hasta el 85%.

Teniendo en cuenta las salvaguardas, es posible calcular el riesgo efectivo:

Activo / Recurso	ALE' = Riesgo efectivo			
	Incendio		Acceso no autorizado	
	Confidenc.	Disponibilidad	Confidenc.	Disponibilidad
	Frecuencia' x SLE'	Frecuencia' x SLE'	Frecuencia' x SLE'	Frecuencia' x SLE'
Cientes	$0,1 \times 10\% \times 0 \times 20\% = 0$	$0,1 \times 10\% \times 50.000 \times 20\% = 100$	$5 \times 5\% \times 10.000 \times 15\% = 375$	$5 \times 5\% \times 0 \times 15\% = 0$
Cientes potenciales	$0,1 \times 10\% \times 0 \times 20\% = 0$	$0,1 \times 10\% \times 500 \times 20\% = 1$	$5 \times 10\% \times 2.000 \times 20\% = 200$	$5 \times 10\% \times 0 \times 20\% = 0$
Aplicación comercial	$0,1 \times 10\% \times 0 \times 20\% = 0$	$0,1 \times 10\% \times 0 \times 20\% = 0$	$5 \times 5\% \times 10.000 \times 15\% = 375$	$5 \times 5\% \times 0 \times 15\% = 0$
Aplicación marketing	$0,1 \times 10\% \times 0 \times 20\% = 0$	$0,1 \times 10\% \times 500 \times 20\% = 0$	$5 \times 10\% \times 2.000 \times 20\% = 200$	$5 \times 10\% \times 0 \times 20\% = 0$
Servidor	$0,1 \times 10\% \times 0 \times 20\% = 0$	$0,1 \times 10\% \times 50.500 \times 20\% = 101$	$5 \times 10\% \times 0 \times 20\% = 0$	$5 \times 10\% \times 0 \times 20\% = 0$
TOTAL	0	$100 + 1 = 101$	$375 + 200 = 575$	0
		$0 + 101 = 101$		$575 + 0 = 575$

Tabla 14: Caso práctico de análisis de riesgos - Cálculo del riesgo efectivo

Por tanto, las pérdidas anuales esperadas teniendo en cuenta las salvaguardas implantadas son 676 €.

Del análisis de la tabla se pueden obtener conclusiones sobre los recursos y/o las amenazas que requieren medidas adicionales de protección para reducir el riesgo, en caso de que sea esa la estrategia de la Organización.

Se ha obtenido una reducción de las pérdidas anuales esperadas de 52.500-676=51.824 €. Si el coste anual de mantenimiento de las salvaguardas implantadas es superior, conviene analizar la conveniencia de mantenerlas.

4.1.2. ISO TR 13335:1997 Tecnología de la información – Guías para la gestión de la seguridad de las TI

No se trata de un estándar internacional, sino de un informe técnico (TR).

Los objetivos por los que este informe técnico fue concebido fueron:

- Definir y describir los conceptos asociados con la gestión de la seguridad de las Tecnologías de la Información.
- Identificar las relaciones entre la gestión de la seguridad de las Tecnologías de la Información y la gestión de las propias Tecnologías de la Información.
- Presentar varios modelos útiles para la gestión de la seguridad de las Tecnologías de la Información.
- Proporcionar una guía general sobre la gestión de la seguridad de las Tecnologías de la Información.

El documento se articula en las siguientes cinco partes:

- Parte 1: Conceptos y modelos para la seguridad de las Tecnologías de la Información. (Publicada en 2004) [ISO13335-1.04]
- Parte 2: Planificación y gestión de la seguridad de las Tecnologías de la Información. (Publicada en 1997, ha quedado obsoleta por la publicación de la última versión de la parte 1) [ISO13335-2.97]
- Parte 3: Técnicas para la gestión de la seguridad de las Tecnologías de la Información. (Publicada en 1998, ha quedado obsoleta por la publicación de la norma ISO/IEC 27005:2008) [ISO13335-3.98]

- Parte 4: Selección de salvaguardas. (Publicada en 2000, ha quedado obsoleta por la publicación de la norma ISO/IEC 27005:2008) [ISO13335-4.00]
- Parte 5: Salvaguardas para conexiones externas. (Publicada en 2001, ha quedado obsoleta por la publicación de la norma ISO/IEC 18028-1:2006) [ISO13335-5.01]

El modelo de procesos propuesto por el informe técnico ISO/IEC 13335 para la gestión de la Seguridad de la Información se resume en el siguiente gráfico:

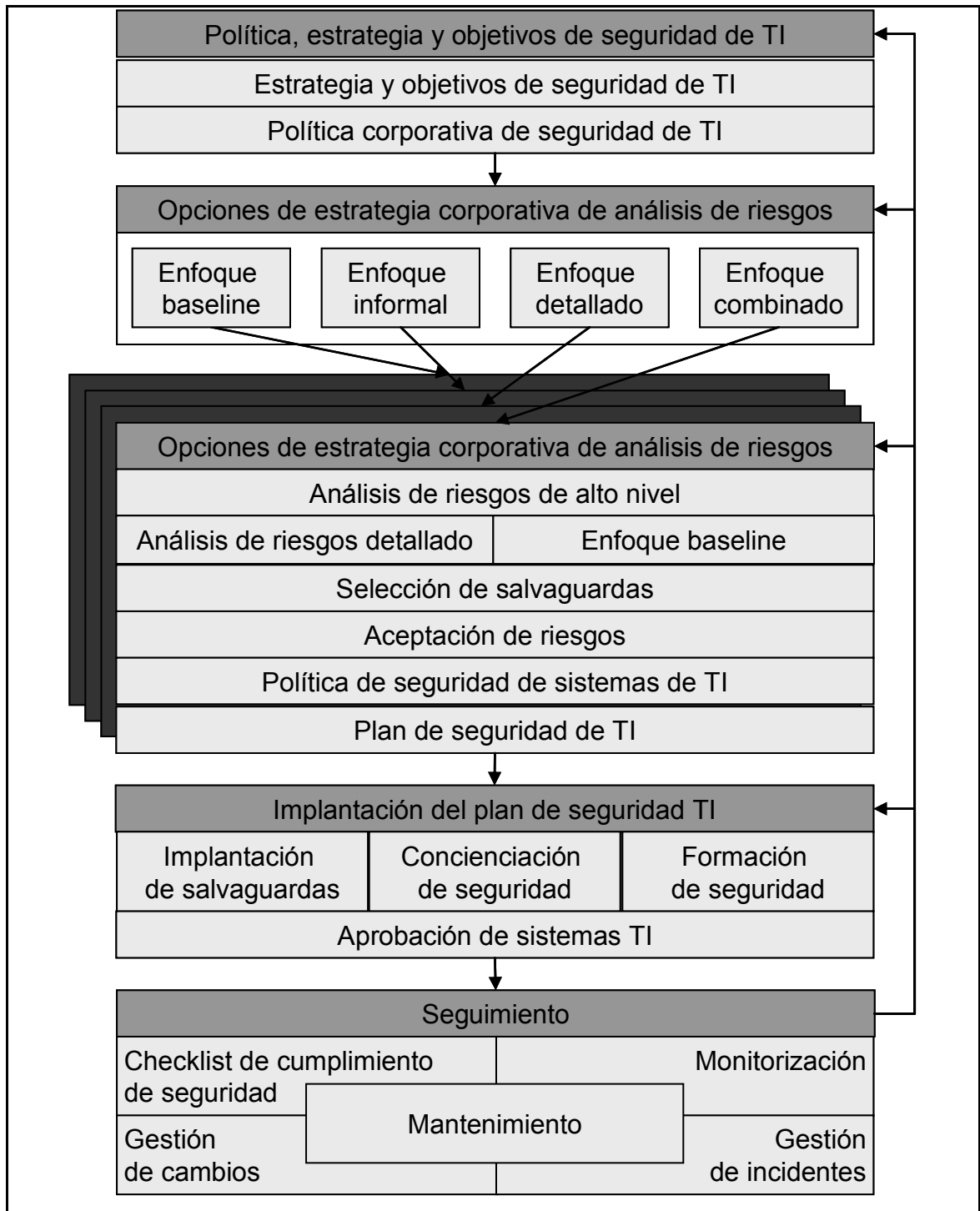


Figura 3: Procesos de gestión de seguridad de la información de ISO/IEC 13335

Como parte de los procesos de gestión de seguridad de la información se incluye el proceso de análisis detallado de riesgos, que se describe en el siguiente gráfico:

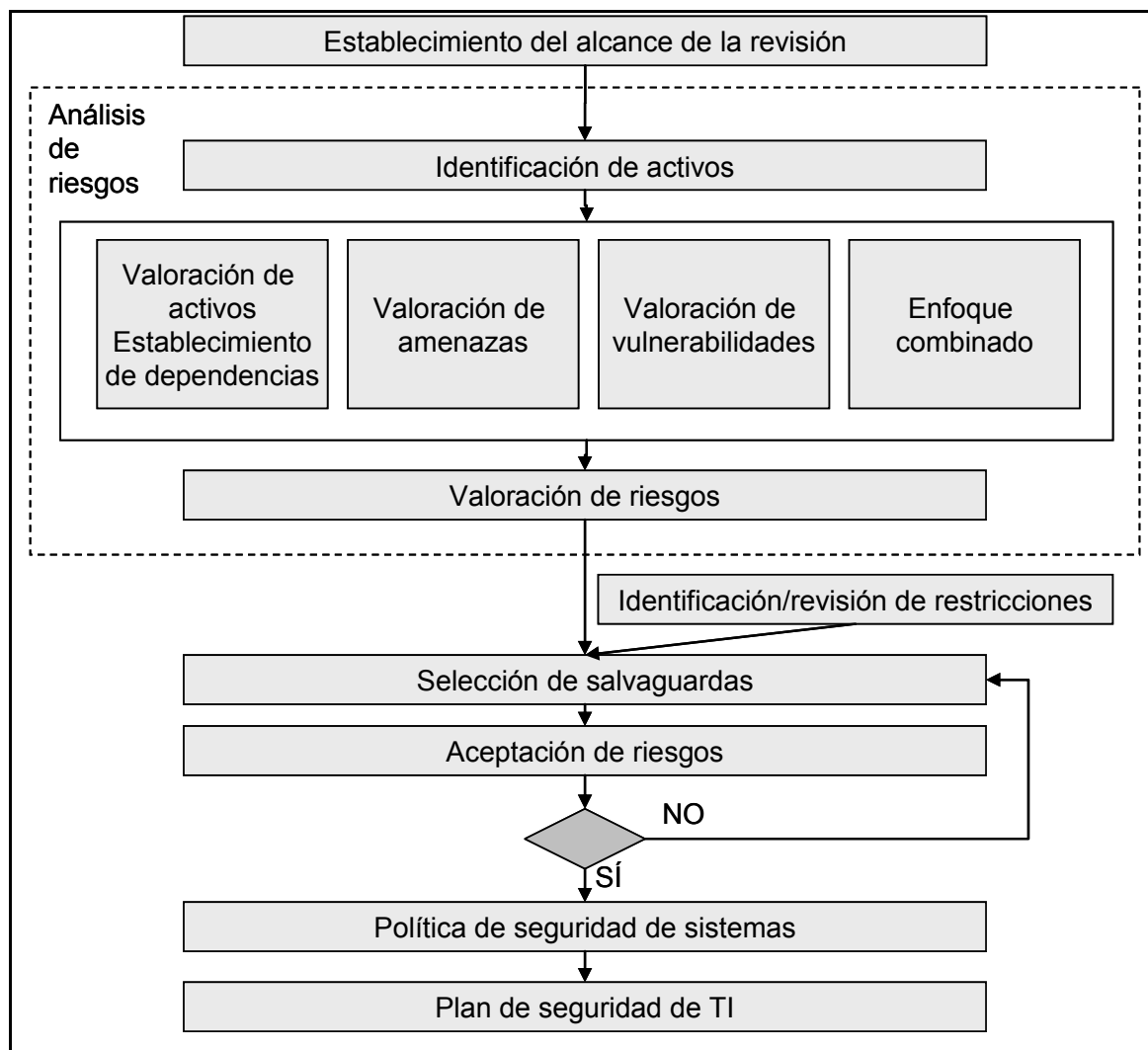


Figura 4: Proceso de análisis detallado de riesgos de ISO/IEC 13335

4.1.3. ISO/IEC 27005:2008 Tecnologías de la información – Técnicas de seguridad – Gestión del riesgo de seguridad de la información

La norma ISO/IEC 27005:2008 forma parte de la familia ISO 27000 dedicada a la seguridad de la información. Sirve de complemento a las dos primeras normas de la familia (ISO/IEC 27001:2005 [ISO27001.05] e ISO/IEC 27002:2005 [ISO27002.05]), que definen la necesidad de elaborar un análisis de riesgos pero no especifican directrices para ello.

Está basada en los informes técnicos ISO/IEC TR 13335-3:1998 [ISO13335-3.98] e ISO/IEC TR 13335-4:2000 [ISO13335-4.00], descritos en el apartado anterior, que quedaron obsoletos desde su publicación. También está basada en la norma BS 7799-3:2006 [BS7799-3.06].

El proceso de gestión de riesgos se describe en las siguientes 6 cláusulas [ISO27005.08]:

- **Cláusula 7 Establecimiento del contexto**, en la que se definen los objetivos, el alcance y la organización para todo el proceso.
- **Cláusula 8 Valoración de riesgos**, en la que se obtiene toda la información necesaria para conocer, valorar y priorizar los riesgos. Se divide en tres apartados:
 - Identificación de riesgos, que consiste en determinar qué puede provocar pérdidas a la Organización.
 - Estimación de riesgos, que consiste en utilizar métodos cuantitativos o cualitativos para obtener una cuantificación de los riesgos identificados, teniendo en cuenta los activos, las amenazas y las salvaguardas.
 - Evaluación de riesgos, que consiste en comparar los riesgos estimados con los criterios de evaluación y de aceptación de riesgos definidos en el establecimiento del contexto.

- **Cláusula 9 Tratamiento de riesgos**, en la que se define la estrategia para tratar cada uno de los riesgos valorados: reducción, aceptación, evitación o transferencia.
- **Cláusula 10 Aceptación de riesgos**, en la que se determinan los riesgos que se decide aceptar, y la justificación correspondiente a cada riesgo aceptado.
- **Cláusula 11 Comunicación de riesgos**, en la que todos los grupos de interés intercambian información sobre los riesgos.
- **Cláusula 12 Monitorización y revisión de riesgos**, en la que el análisis de riesgos se actualiza con todos los cambios internos o externos que afectan a la valoración de los riesgos.

El proceso de gestión de riesgos definido por la norma ISO/IEC 27005:2008 puede resumirse en el siguiente gráfico:

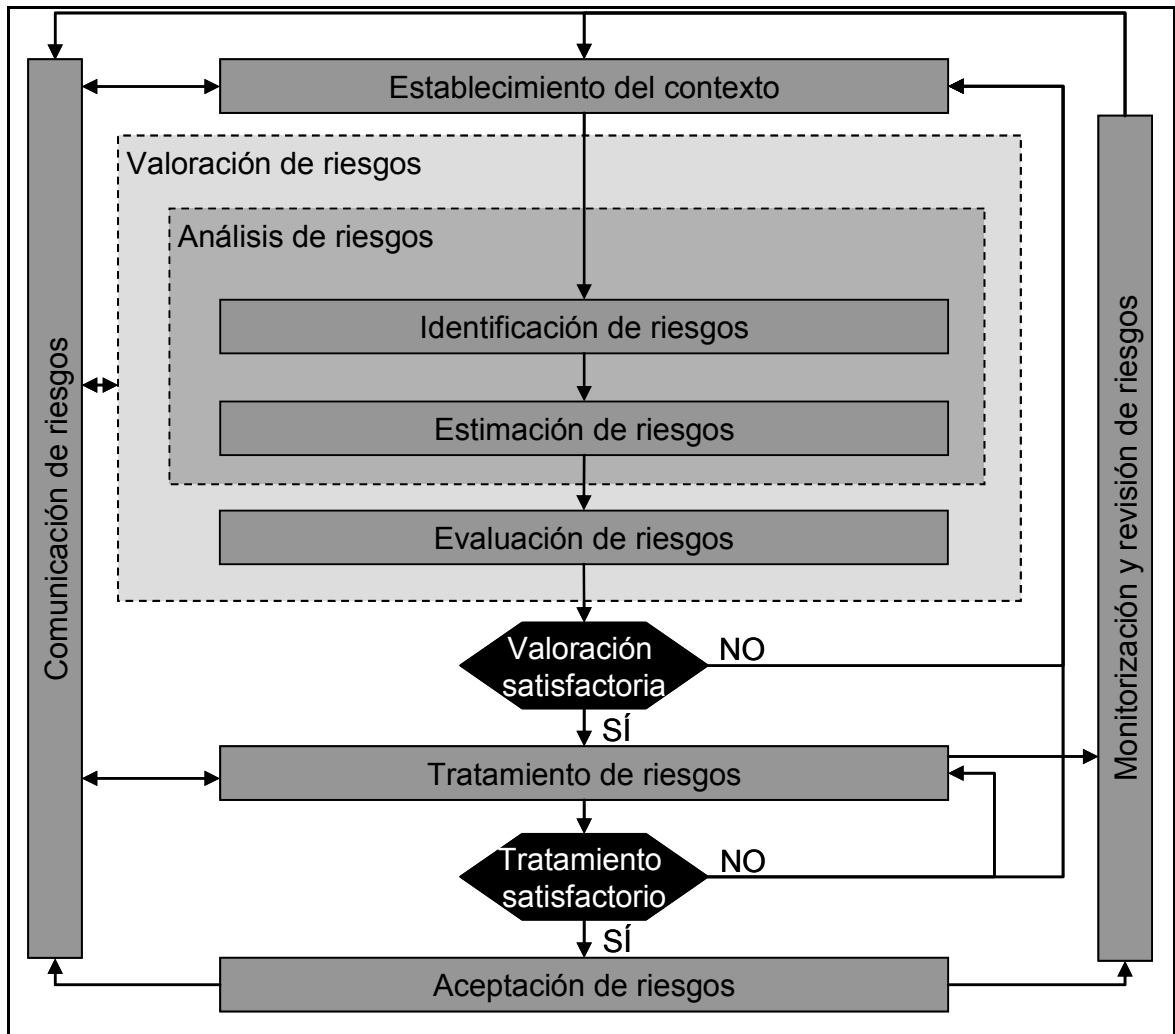


Figura 5: Proceso de gestión de riesgos de seguridad de la información de ISO/IEC 27005:2008

En línea con el estándar ISO/IEC 27001:2005, el proceso de gestión de riesgos se considera iterativo, siguiendo el ciclo de Deming:

Ciclo de Deming	Proceso de gestión de riesgos de seguridad de la información
Planificar	Establecimiento del contexto Valoración de riesgos Desarrollo del plan de tratamiento de riesgos Aceptación de riesgos
Hacer	Implantación del plan de tratamiento de riesgos
Verificar	Monitorización y revisión continua de riesgos
Actuar	Mantenimiento y mejora del proceso de gestión de riesgos de seguridad de la información

Tabla 15: Ciclo de Deming aplicado a la gestión de riesgos de seguridad de la información

4.1.4. UNE 71504:2008 Metodología de análisis y gestión de riesgos para los sistemas de información

Desarrollada por el comité técnico AEN/CTN 71 Tecnología de la información, de AENOR [UNE71504.08].

El proceso de gestión de riesgos que define consta de las siguientes fases principales:

- Método de análisis
 - Tareas preparatorias
 - Caracterización de activos
 - Identificación de los activos relevantes
 - Identificación de relaciones entre los activos
 - Valoración de los activos
 - Caracterización de las amenazas
 - Identificación de las amenazas relevantes
 - Valoración de la vulnerabilidad de los activos ante las amenazas
 - Cálculo del riesgo intrínseco

- Caracterización de las salvaguardas
 - Determinación de las salvaguardas adecuadas
 - Valoración de las salvaguardas
 - Cálculo del riesgo efectivo
- Evaluación de riesgos
- Tratamiento de riesgos
 - Definición del plan de seguridad
 - Aprobación del plan de seguridad
- Administración de la gestión de riesgos

La metodología se puede resumir gráficamente de la siguiente forma:

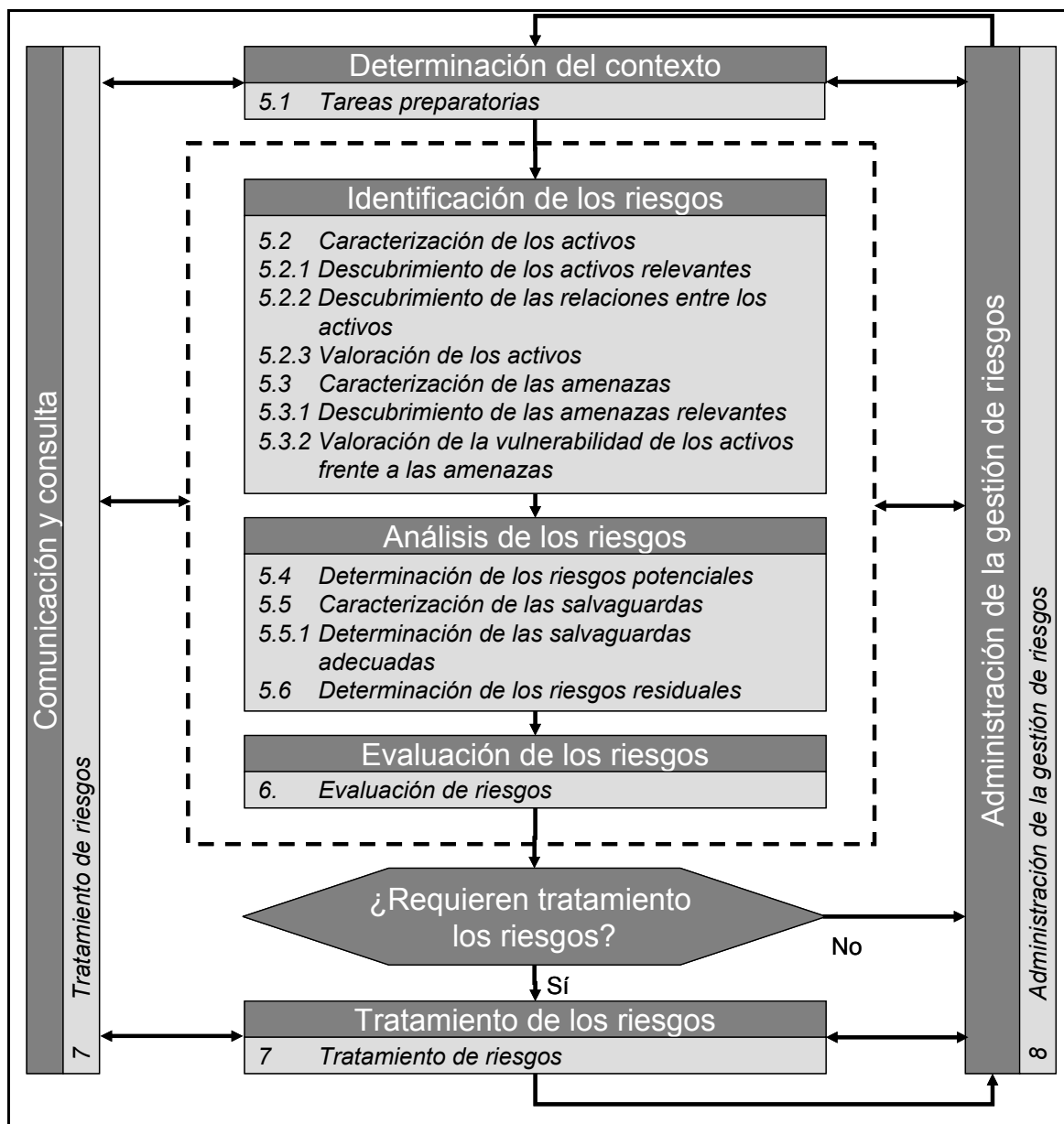


Figura 6: Modelo UNE 71504

4.1.5. BS 7799-3:2006 Sistemas de Gestión de Seguridad de la Información – Parte 3: Guías para la gestión de riesgos de seguridad de la información

Se definió para soportar la implantación de Sistemas de Gestión de Seguridad de la Información basados en el estándar ISO/IEC 27001:2005 [BS7799-3.06] [ISO27001.05].

Los principales procesos de análisis de riesgos que define son:

- Análisis de riesgos:
 - Identificación de activos
 - Identificación de requerimientos legales y de negocio relevantes para los activos identificados.
 - Valoración de los activos teniendo en cuenta los requerimientos identificados y el impacto resultante de la pérdida de confidencialidad, integridad o disponibilidad.
 - Identificación de amenazas y vulnerabilidades relevantes para los activos identificados.
 - Valoración de la posibilidad de que ocurran las amenazas y vulnerabilidades.
- Evaluación de riesgos:
 - Cálculo de riesgos
 - Evaluación de los riesgos teniendo en cuenta una escala de riesgos.
- Tratamiento de riesgos y decisiones de la dirección
 - Determinación de la estrategia de gestión de los riesgos:
 - Reducir
 - Aceptar
 - Transferir
 - Evitar
 - Evaluación del riesgo residual
 - Definición del plan de tratamiento de riesgos

- Actividades de gestión continuo del riesgo:
 - Mantenimiento y monitorización.
 - Revisiones de la dirección.
 - Revisiones y reevaluaciones de riesgos.
 - Auditorías.
 - Controles de documentación.
 - Acciones correctivas y preventivas.
 - Reporting y comunicaciones

Los procesos propuestos para la gestión del riesgo definen un ciclo iterativo que se puede comprobar en el siguiente diagrama:

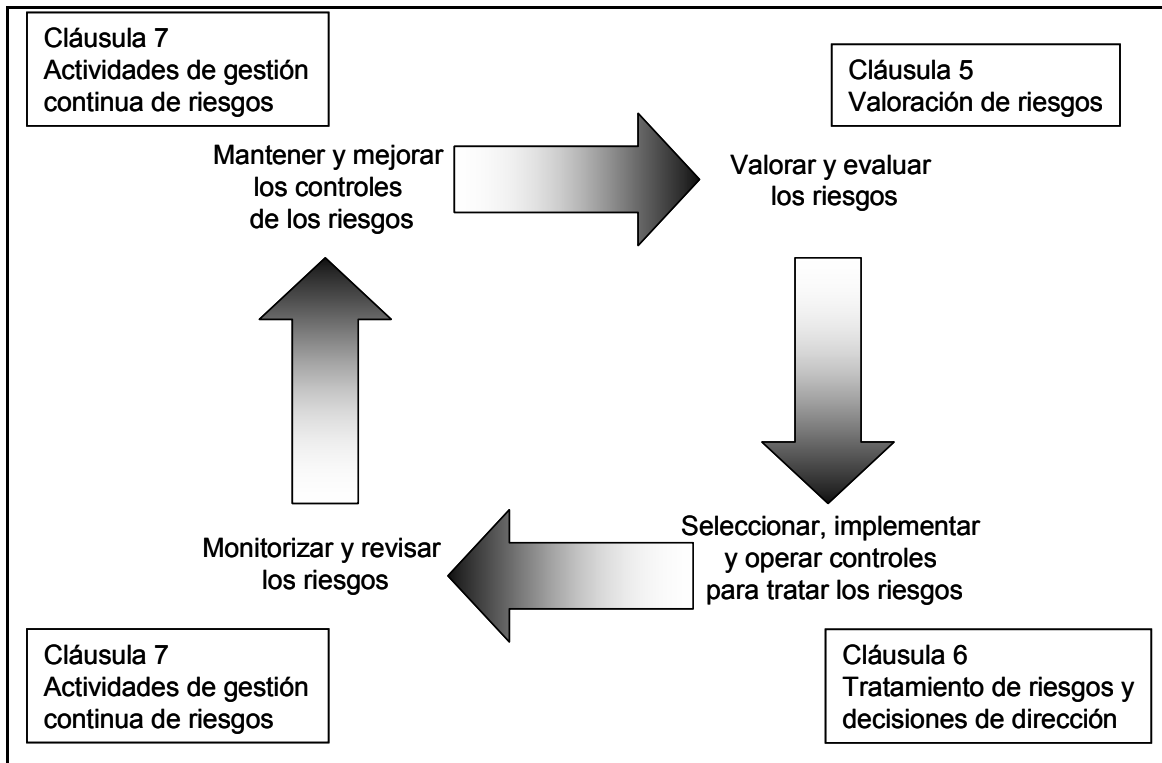


Figura 7: Modelo de procesos de gestión de riesgos de BS 7799-3

4.1.6. AS/NZS 4360:2004 Gestión de riesgos

En el momento de la publicación de las normas ISO/IEC 27001:2005 [ISO27001.05] e ISO/IEC 27002:2005 [ISO27002.05] la norma AS/NZS 4360:2004 [AS4360.04] era la única norma internacional publicada para la realización de análisis de riesgos de seguridad de la información (si no se considera el informe técnico ISO/IEC TR 13335 [ISO13335-3.98] [ISO13335-4.00], que no tenía rango de norma, y los diversos modelos y metodologías existentes que no estaban respaldados por organizaciones de estandarización y normalización), y por ello, hasta la publicación de las normas BS 7799-3:2006 [BS7799-3.06] e ISO/IEC 27005:2008 [ISO27005.08] fue la norma dominante a nivel internacional soportando la implantación de Sistemas de Gestión de Seguridad de la Información.

El proceso de gestión de riesgos propuesto por la norma AS/NZS 4360:2004 puede resumirse en el siguiente esquema [AS4360.04]:

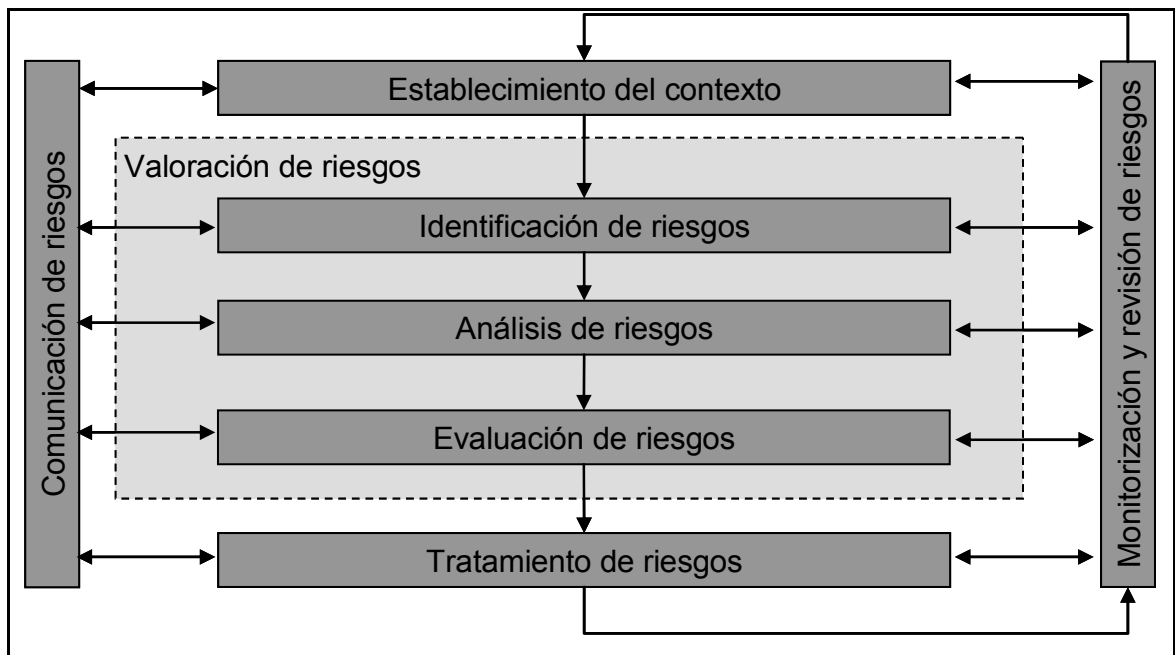


Figura 8: Proceso de gestión de riesgos de AS/NZS 4360:2004

Los principales aspectos considerados por la norma AS/NZS 4360:2004 son:

- Establecimiento del contexto:
 - Definición de objetivos
 - Identificación de grupos de interés
 - Definición de criterios para el análisis de riesgos
 - Definición de elementos clave
- Identificación de riesgos
 - ¿Qué puede ocurrir?
 - ¿Cómo puede ocurrir?
- Análisis de los riesgos
 - Revisar controles
 - Posibilidades
 - Consecuencias
 - Nivel de riesgo
- Evaluación de los riesgos
 - Evaluar los riesgos
 - Priorizar los riesgos
- Tratamiento de los riesgos
 - Identificar opciones (reducción, aceptación, traspaso, evitación)
 - Seleccionar las mejores estrategias
 - Desarrollar planes de tratamiento de riesgos
 - Implementar los planes

4.1.7. MAGERIT – Metodología de Análisis y Gestión de Riesgos de IT

La metodología MAGERIT fue desarrollada por el Consejo Superior de Administración Electrónica, y publicada por el Ministerio de Administraciones Públicas [MAGE06].

La primera versión se publicó en 1997 y la versión vigente en la actualidad es la versión 2.0, publicada en 2006.

Se trata de una metodología abierta, de uso muy extendido en el ámbito español, y de uso obligatorio por parte de la Administración Pública Española.

Dispone de una herramienta de soporte, PILAR II (Proceso Informático-Lógico para el Análisis y la gestión de Riesgos), de uso gratuito para la Administración Pública española y comercial para organizaciones privadas.

La metodología consta de tres volúmenes:

- **Volumen I – Método**, es el volumen principal en el que se explica detalladamente la metodología.
- **Volumen II – Catálogo de elementos**, complementa el volumen principal proporcionando diversos inventarios de utilidad en la aplicación de la metodología. Los inventarios que incluye son:
 - Tipos de activos
 - Dimensiones y criterios de valoración
 - Amenazas
 - Salvaguardas
- **Volumen III – Guía de técnicas**, complementa el volumen principal proporcionando una introducción de algunas de técnicas a utilizar en las distintas fases del análisis de riesgos. Las técnicas que recoge son:
 - Técnicas específicas para el análisis de riesgos:
 - Análisis mediante tablas
 - Análisis algorítmico
 - Árboles de ataque
 - Técnicas generales
 - Análisis coste-beneficio
 - Diagramas de flujo de datos (DFD)
 - Diagramas de procesos
 - Técnicas gráficas
 - Planificación de proyectos
 - Sesiones de trabajo: entrevistas, reuniones y presentaciones

- Valoración Delphi

La metodología MAGERIT se puede resumir gráficamente de la siguiente forma:

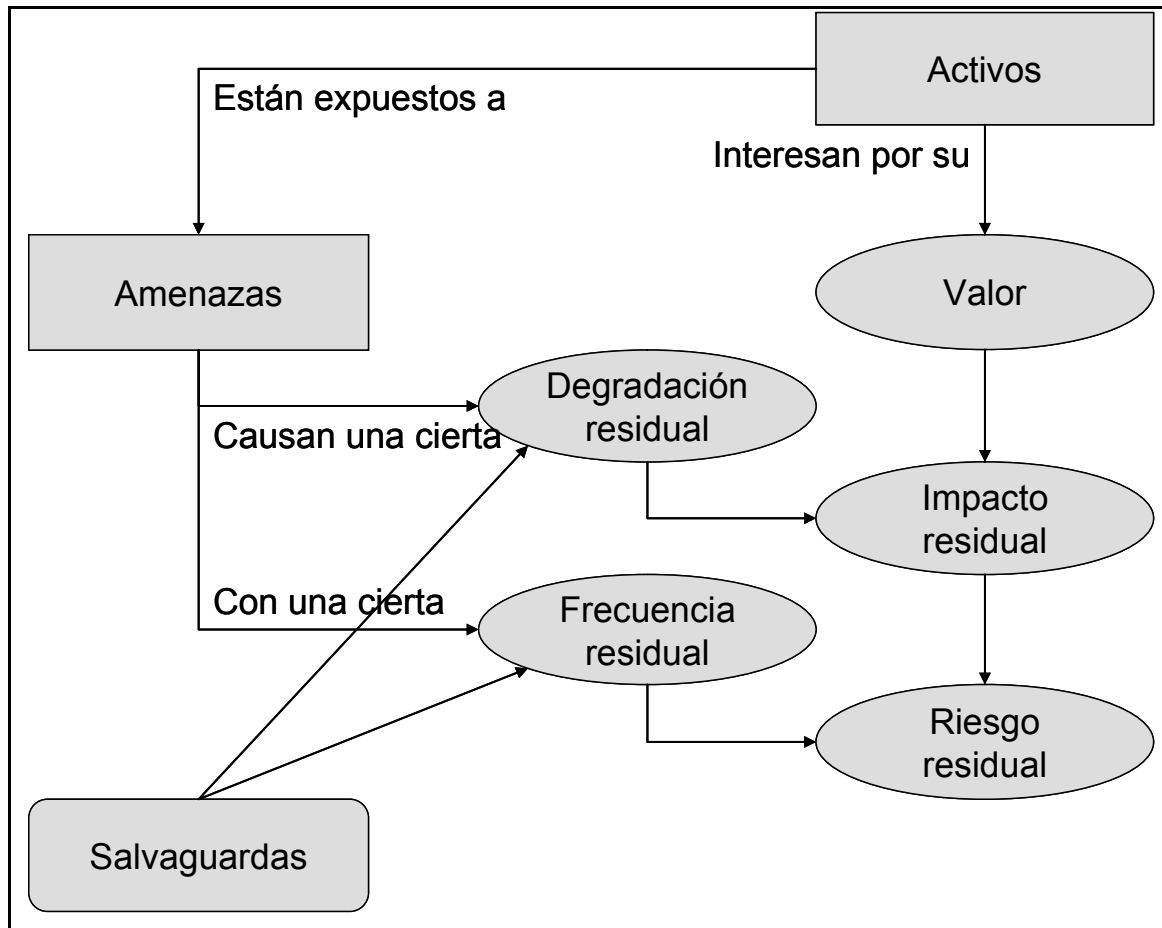


Figura 9: Modelo MAGERIT

4.1.8. OCTAVE – Operationally Critical Threat, Asset and Vulnerability Evaluation

OCTAVE es un modelo para la creación de metodologías de análisis de riesgos desarrollado por la Universidad de Carnegie Mellon.[ALBER01]

El núcleo central de OCTAVE es un conjunto de criterios (principios, atributos y resultados) a partir de los cuales se pueden desarrollar diversas metodologías.

Cualquier metodología que aplique los criterios puede considerarse compatible con el modelo OCTAVE. Las tres metodologías publicadas a la fecha de este documento por el Software Engineering Institute (SEI) de la Universidad de Carnegie Mellon son:

- **OCTAVE.** La metodología original, definida para grandes organizaciones. [ALBER01] [ALBER03A] [ALBER03B]
- **OCTAVE-S.** Metodología definida para pequeñas organizaciones. [ALBER05]
- **OCTAVE Allegro.** Metodología definida para analizar riesgos con un mayor enfoque en los activos de información, en oposición al enfoque en los recursos de información. [ALBER07]

Los criterios que forman el núcleo de OCTAVE son:

- Principios de los que se derivan atributos:
 - La metodología debe ser auto-dirigida
 - RA.1 Equipo de análisis
 - RA.2 Capacidades del equipo de análisis
 - Las medidas deben ser adaptables a las necesidades
 - RA.3 Catálogo de prácticas
 - RA.4 Perfil genérico de amenazas
 - RA.5 Catálogo de vulnerabilidades
 - El proceso debe ser definido
 - RA.6 Actividades de evaluación definidas
 - RA.7 Documentación de los resultados de la evaluación
 - RA.8 Alcance de la evaluación
 - El proceso debe ser continuo
 - RA.9 Próximos pasos
 - RA.3 Catálogo de prácticas
 - El proceso debe seguirse con visión de futuro
 - RA.10 Enfoque en riesgos

- El proceso debe centrarse en un reducido número de riesgos críticos
 - RA.8 Alcance de la evaluación
 - RA.11 Actividades enfocadas
- Gestión integrada:
 - RA.12 Aspectos organizativos y tecnológicos
 - RA.13 Participación de negocio y de áreas tecnológicas
 - RA.14 Participación de la alta dirección
- Comunicación abierta
 - RA.15 Enfoque colaborativo
- Perspectiva global
 - RA.12 Aspectos organizativos y tecnológicos
 - RA.13 Participación de negocio y de áreas tecnológicas
- Equipo de trabajo
 - RA.1 Equipo de análisis
 - RA.2 Capacidades del equipo de análisis
 - RA.13 Participación de negocio y de áreas tecnológicas
 - RA.15 Enfoque colaborativo
- Resultados de las distintas fases:
 - Fase 1: Visión organizativa
 - RO1.1 Activos críticos
 - RO1.2 Requerimientos de seguridad para los activos críticos
 - RO1.3 Amenazas sobre los activos críticos
 - RO1.4 Prácticas de seguridad actuales
 - RO1.5 Vulnerabilidades organizativas actuales
 - Fase 2: Visión tecnológica
 - RO2.1 Componentes clave
 - RO2.2 Vulnerabilidades tecnológicas actuales
 - Fase 3: Estrategia y desarrollo del plan
 - RO3.1 Riesgos sobre activos críticos
 - RO3.2 Medidas contra los riesgos
 - RO3.3 Estrategia de protección

- RO3.4 Planes de mitigación del riesgo

Las fases del proceso OCTAVE pueden resumirse en el siguiente gráfico:

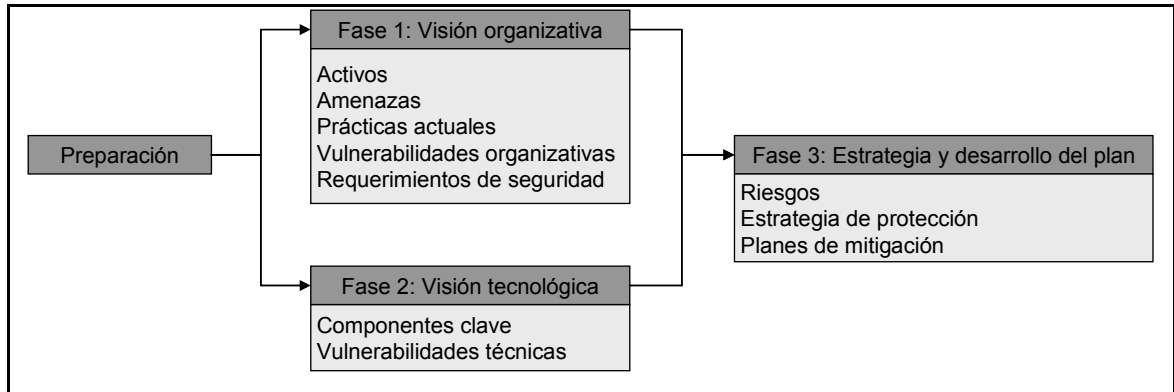


Figura 10: Fases del proceso OCTAVE

Para cada metodología se define un conjunto de procesos diferente adaptado a las necesidades particulares, siempre cumpliendo todos los criterios. Los procesos de cada una de las metodologías son:

- OCTAVE
 - Fase 1: Visión organizativa
 - Identificar conocimiento de la alta dirección
 - Identificar conocimiento de la dirección de áreas operativas
 - Identificar conocimiento del personal de áreas operativas y de TI
 - Crear perfiles de amenazas
 - Fase 2: Visión tecnológica
 - Identificar componentes clave
 - Evaluar componentes seleccionados
 - Fase 3: Estrategia y desarrollo del plan
 - Analizar los riesgos
 - Diseñar la estrategia de protección

- OCTAVE-S
 - Fase 1: Visión organizativa
 - Identificar información organizativa
 - Crear perfiles de amenazas
 - Fase 2: Visión tecnológica
 - Examinar la infraestructura tecnológica relacionada con los activos críticos
 - Fase 3: Estrategia y desarrollo del plan
 - Analizar los riesgos
 - Diseñar la estrategia de protección y planes de mitigación
- OCTAVE Allegro
 - Fase 1: Establecer dirección
 - Establecer criterios de valoración de riesgos
 - Fase 2: Perfilar activos
 - Desarrollar perfiles de activos de información
 - Identificar recursos de información
 - Fase 3: Identificar amenazas
 - Identificar áreas de interés para el análisis
 - Identificar escenarios de amenazas
 - Fase 4: Identificar y mitigar riesgos
 - Identificar riesgos
 - Analizar riesgos
 - Seleccionar enfoque de mitigación

4.1.9. CRAMM – CCTA Risk Analysis and Management Method

CRAMM es una metodología de análisis de riesgos desarrollada en Reino Unido por la Agencia Central de Cómputo y Telecomunicaciones (CCTA). Comenzó a desarrollarse en la década de 1980 y actualmente está en su versión 5.1. Es el método de análisis de riesgos preferente en Organismos de la Administración Pública británica [CRAMM03].

Pese a tratarse de una iniciativa del Sector Público, el mantenimiento y la gestión de la metodología lo realiza una empresa privada de consultoría, Insight Consulting, actualmente integrada en Siemens.

El modelo de análisis y gestión de riesgos de CRAMM puede resumirse en el siguiente gráfico:

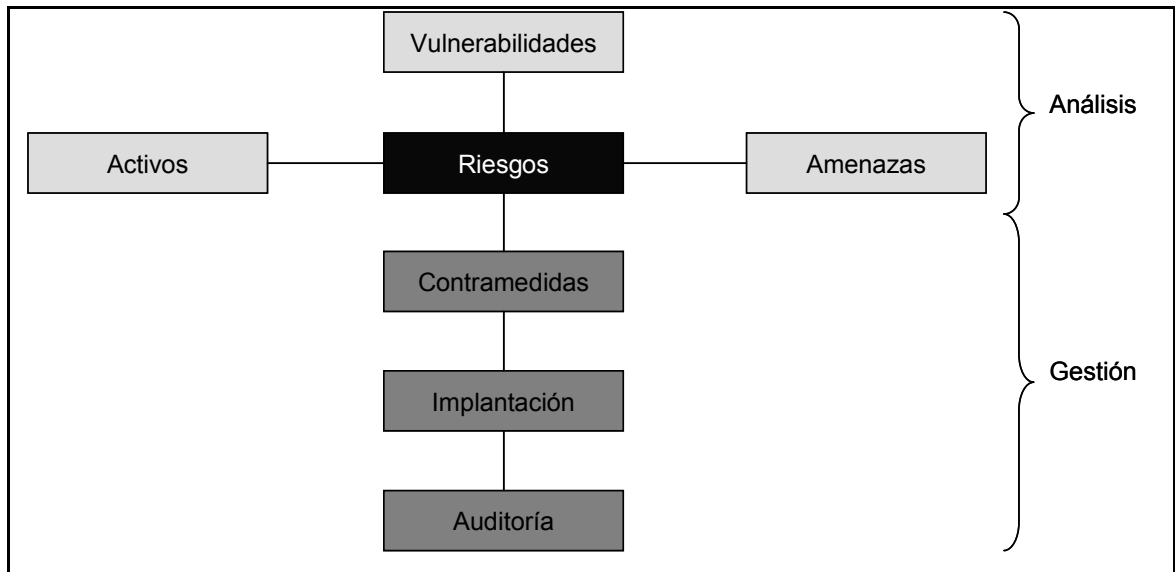


Figura 11: Modelo de análisis y gestión de riesgos de CRAMM

Uno de los aspectos principales de CRAMM es el soporte que proporciona la herramienta informática que la soporta, con una base de datos de:

- Más de 400 tipos de activos
- Más de 25 tipos de impacto
- 38 tipos de amenaza
- 7 tipos de medida del riesgo
- Más de 3.500 salvaguardas.

Actualmente CRAMM soporta tres tipos de revisiones:

- CRAMM Express
- CRAMM Expert
- BS7799

Adicionalmente existen variantes para la gestión de riesgos en proyectos de desarrollo, con una interfaz al ciclo de vida estándar utilizado por la Administración Pública británica: SSADM (Structured System Analysis and Design Method).

La metodología CRAMM define tres fases para la realización del análisis de riesgos:

- Fase 1: Establecimiento de objetivos de seguridad:
 - Definir el alcance del estudio.
 - Definir el valor de la información entrevistando a los usuarios sobre los impactos potenciales para el negocio que podrían producirse por la indisponibilidad, destrucción, divulgación o modificación.
 - Identificar y evaluar los activos físicos que forman parte del sistema.
 - Identificar y evaluar los activos de software que forman parte del sistema.
- Fase 2: Evaluación de riesgos:
 - Identificar y valorar el tipo y nivel de las amenazas que pueden afectar al sistema.
 - Valorar las vulnerabilidades de los sistemas ante las amenazas identificadas.
 - Combinar las valoraciones de amenazas y vulnerabilidades para calcular la medida de los riesgos.
- Fase 3: Identificación y selección de contramedidas.

Los principales productos de la metodología CRAMM son:

- Documento de inicio del proyecto
- Informes de análisis de riesgos

- Informes de gestión de riesgos, basados en una base de datos de más de 3.500 salvaguardas técnicas y organizativas.
- Plan de implantación

Las principales actividades del proceso de análisis y gestión de riesgos de CRAMM se resumen en el siguiente gráfico:

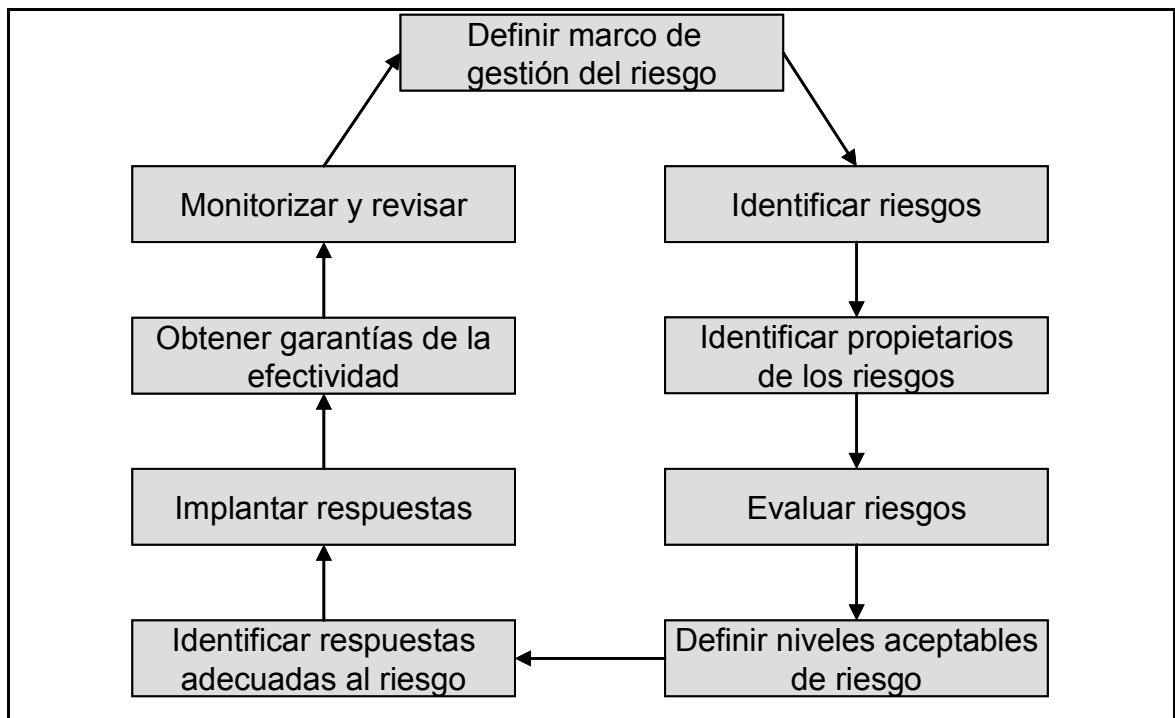


Figura 12: Principales actividades de análisis y gestión de riesgos de CRAMM

4.1.10. NIST SP 800-30 Guía de gestión de riesgos para sistemas de tecnología de la información

El NIST (National Institute of Standards and Technology) ha dedicado una serie de publicaciones especiales, la SP 800 a la seguridad de la información. Esta serie incluye una metodología para el análisis y gestión de riesgos de seguridad de la información, alineada y complementaria con el resto de documentos de la serie.

El proceso de análisis de riesgos definido en la metodología NIST SP 800-30 puede resumirse en el siguiente gráfico [NIST800-30.02]:

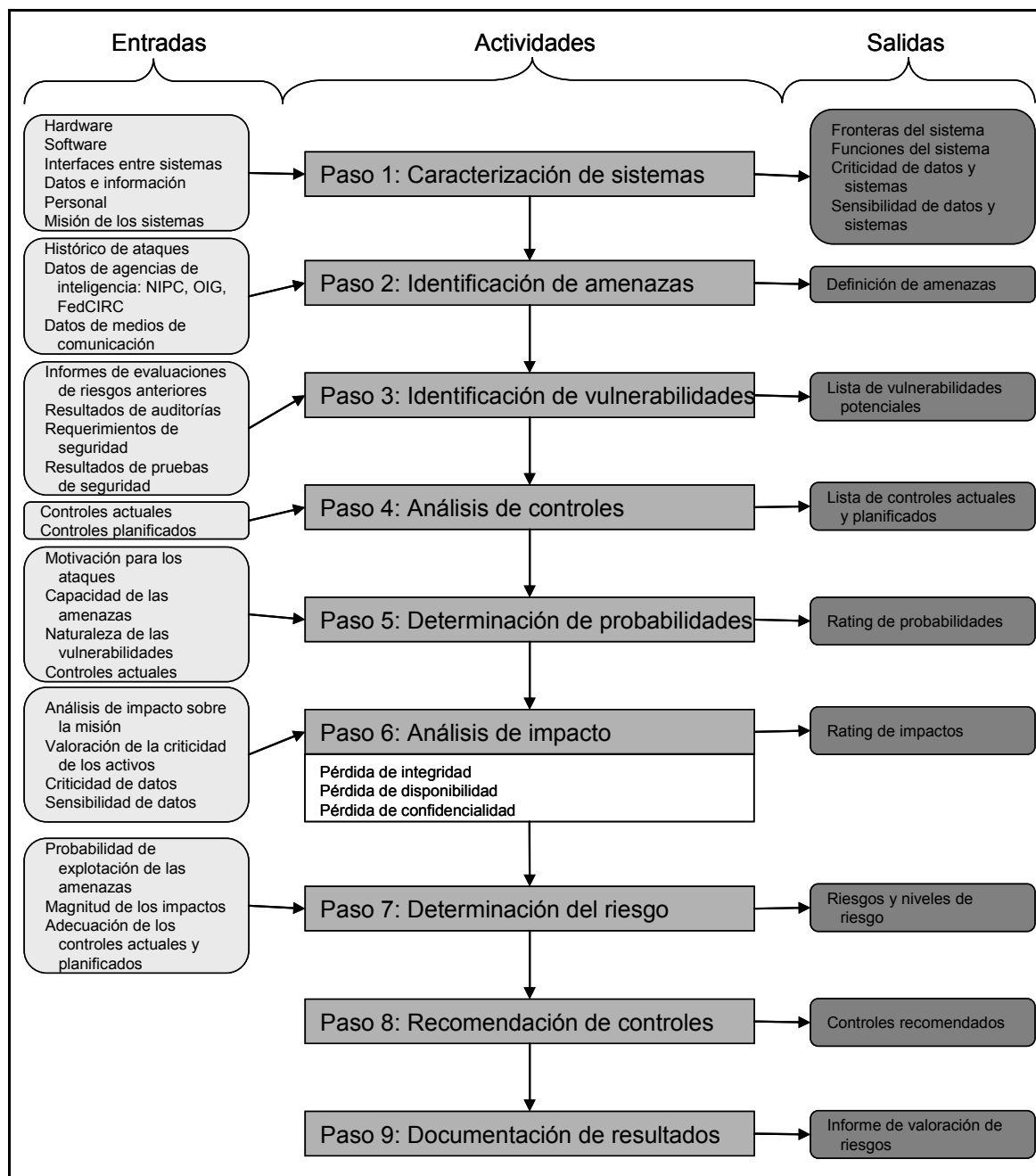


Figura 13: Proceso de análisis de riesgos de NIST SP 800-30

El proceso de gestión de riesgos definido en la metodología NIST SP 800-30 puede resumirse en el siguiente gráfico:

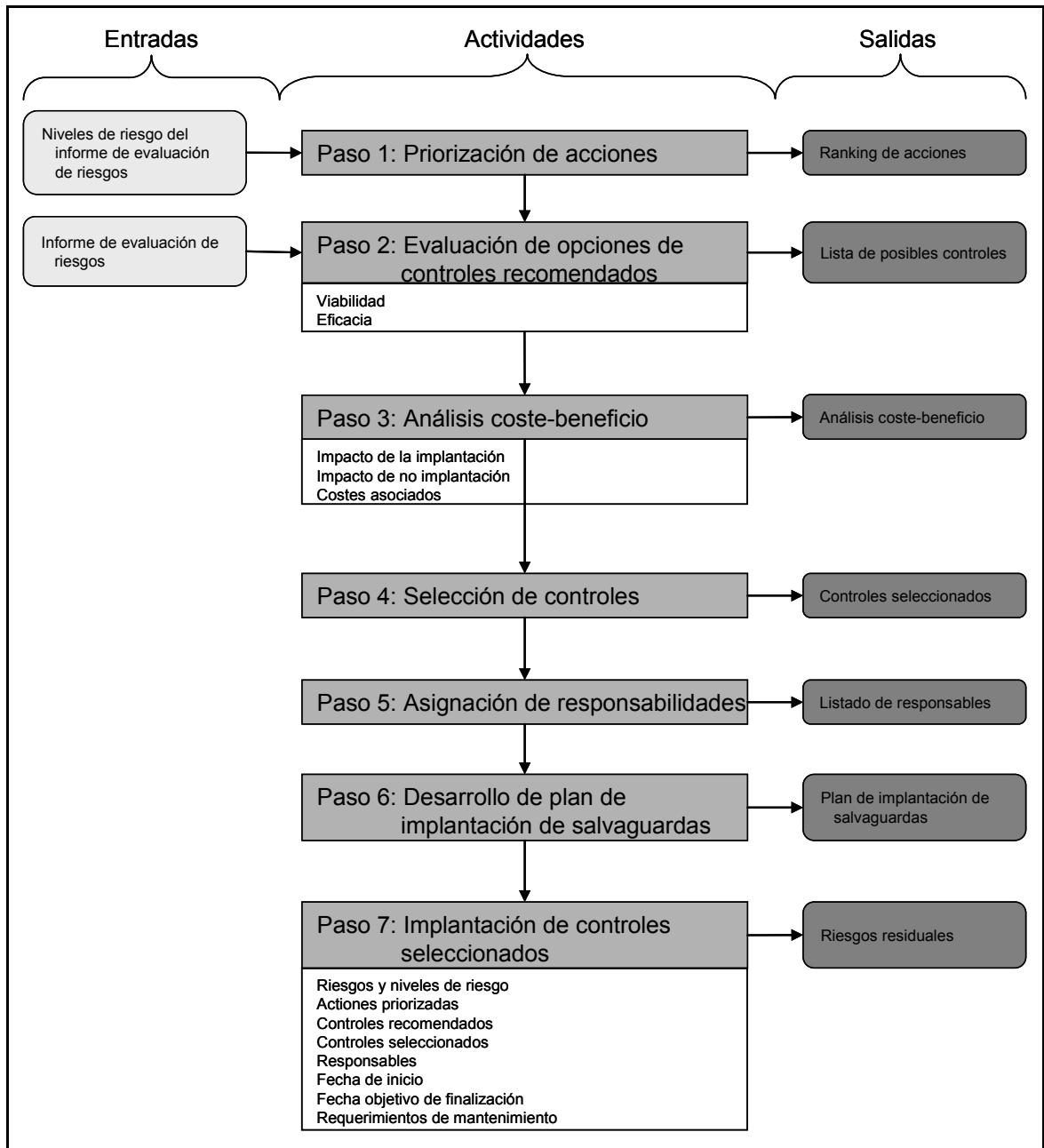


Figura 14: Proceso de gestión de riesgos de NIST SP 800-30

4.1.11. IRAM – Information Risk Analysis Methodologies

El ISF es una organización sin ánimo de lucro de ámbito internacional que desarrolla de forma colaborativa recomendaciones y herramientas de seguridad para sus miembros. Entre las principales preocupaciones del ISF se encuentra el análisis y la gestión de riesgos, y por ello ha desarrollado y publicado diversas metodologías y modelos de análisis de riesgos a lo largo del tiempo [ISF06]:

- SPRINT (Simplified Process for Risk Identification): Análisis de riesgos para una aplicación informática importante pero no crítica.
- SARA (Simple to Apply Risk Analysis): Análisis de riesgos para una aplicación informática crítica.
- FIRM (Fundamental Information Risk Management): Evaluar riesgos en un entorno heterogéneo dentro de un ciclo regular de monitorización.

La metodología actual de análisis y gestión de riesgos del ISF es IRAM, y está alineada con el resto de proyectos del ISF, y en particular con:

- Estudio bienal de amenazas de seguridad (ISF Information Security Status Survey)
- Manual de buenas prácticas de seguridad de la información (The Standard of Good Practice for Information Security), que incluye un inventario de más de 3.200 salvaguardas. [ISF07]

IRAM consta de tres fases principales:

- Fase 1: Análisis de impacto sobre el negocio (BIA).
 - Soportada por la herramienta BIA Assistant.
- Fase 2: Evaluación de amenazas y vulnerabilidades.
 - Soportada por la herramienta T&VA Assistant.
- Fase 3: Selección de controles.
 - Soportada por la herramienta CS Assistant.

Las tres herramientas han sido migradas del entorno microinformático original a un entorno web en una nueva herramienta integrada: IRAM Risk Analyst Workbench.

4.1.12. CORAS – CONstruct a platform for Risk Analysis of Security critical systems

Desarrollado a partir de 2001 por SINTEF, un grupo de investigación noruego financiado por organizaciones del sector público y privado. Se desarrolló en el marco del Proyecto CORAS (IST-2000-25031) financiado por la Unión Europea [STOL01] [STOL02A] [STOL02B] [STOL06] [STOL07A] [STOL07B] [HOGG07A].

El método CORAS proporciona:

- Una metodología de análisis de riesgos basado en la elaboración de modelos, que consta de siete pasos, basados fundamentalmente en entrevistas con los expertos.
- Un lenguaje gráfico basado en UML (Unified Modelling Language) para la definición de los modelos (activos, amenazas, riesgos y salvaguardas), y guías para su utilización a lo largo del proceso. El lenguaje se ha definido como un perfil UML.
- Un editor gráfico para soportar la elaboración de los modelos, basado en Microsoft Visio.
- Una biblioteca de casos reutilizables.
- Una herramienta de gestión de casos, que permite su gestión y reutilización.
- Representación textual basada en XML (eXtensible Mark-up Language) del lenguaje gráfico.
- Un formato estándar de informe para facilitar la comunicación de distintas partes en el proceso de análisis de riesgos.

Los siete pasos del método CORAS pueden representarse gráficamente de la siguiente forma:

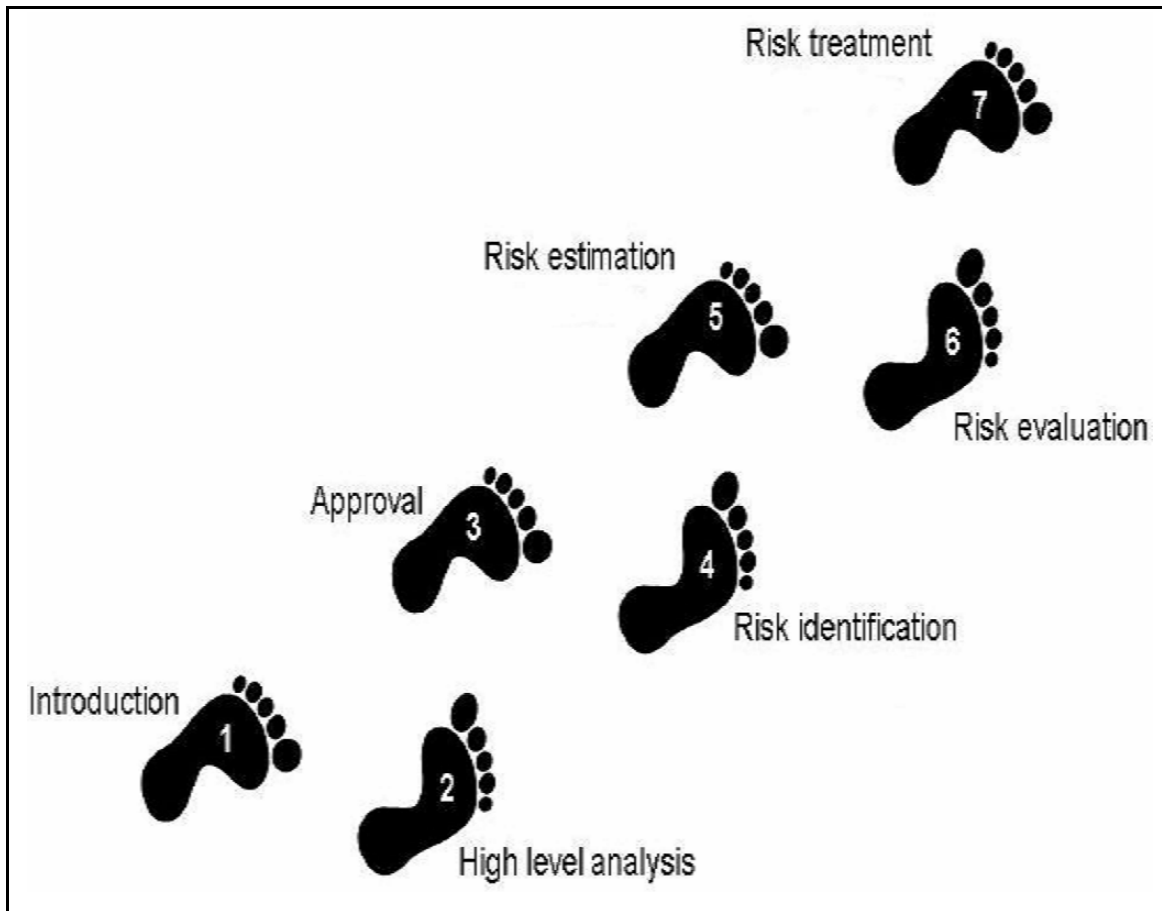


Figura 15: Los siete pasos de la metodología CORAS

Los siete pasos del método CORAS son:

- **Paso 1, Presentación:** Reunión inicial, para presentar los objetivos y el alcance del análisis y recabar información inicial.
- **Paso 2, Análisis de alto nivel:** Entrevistas para verificar la comprensión de la información obtenida y la documentación analizada. Se identifican amenazas, vulnerabilidades, escenarios e incidentes.
- **Paso 3, Aprobación:** Descripción detallada de los objetivos, alcance y consideraciones, para su aprobación por parte del destinatario del análisis de riesgos.

- **Paso 4, Identificación de riesgos:** Identificación detallada de amenazas, vulnerabilidades, escenarios e incidentes.
- **Paso 5, Estimación de riesgo:** Estimación de probabilidades e impactos de los incidentes identificados en el paso anterior.
- **Paso 6, Evaluación de riesgo:** Emisión del informe de riesgos, para su ajuste fino y correcciones.
- **Paso 7, Tratamiento del riesgo:** Identificación de las salvaguardas necesarias, y realización de análisis coste/beneficio.

4.1.13. SOMAP – Security Officers Management and Analysis Project

El Security Officers Management and Analysis Project (SOMAP) es una organización sin ánimo de lucro cuyo objetivo es desarrollar proyectos Open Source relacionados con la gestión de la seguridad de la información [SOMAP06] [SOMAP07].

Actualmente, SOMAP tiene en marcha cuatro proyectos:

- Open Governance, Risk & Compliance Maturity Management Methodology (OGRCM3) se centra en desarrollar una metodología para la medición y la gestión de riesgos. Está publicada la versión 1.0, que considera un proceso cíclico de cuatro fases:
 - Alcance de cumplimiento
 - Gestión y categorización de activos
 - Medición y documentación del cumplimiento
 - Evaluación y reporting
- Open Risk Model Repository (ORIMOR) se centra en desarrollar una base de datos que soporte el marco de referencia y la herramienta. Dispone de un repositorio de:
 - Tipos de activos y dependencias entre ellos
 - Vulnerabilidades
 - Salvaguardas
 - Relación entre activos, vulnerabilidades y salvaguardas.

- Relación entre vulnerabilidades y salvaguardas
- Cuestionarios

Está prevista la publicación periódica de informes con el contenido de la base de datos para su uso independiente de la herramienta de gestión (ver ORICO)

Algunas características relevantes de la herramienta son:

- Uso de identificadores UUID (Universally Unique Identifier) según los estándares ISO/IEC 11578:1996 y DCE 1.1, para facilitar las actualizaciones y migraciones y el soporte multilenguaje.
- La base de datos presente ser multilenguaje, considerando inicialmente el inglés y el alemán.
- Uso de Open Source Vulnerability DataBase (OSVDB) para mantener actualizada permanentemente la base de datos.
- Open Risk & Compliance Framework and Tool (ORICO) se centra en desarrollar un marco de referencia y una herramienta de soporte del modelo. Actualmente se han publicado versiones beta, pero aún no se ha publicado ninguna versión estable.

El modelo de datos actual de ORIMOR es el siguiente:

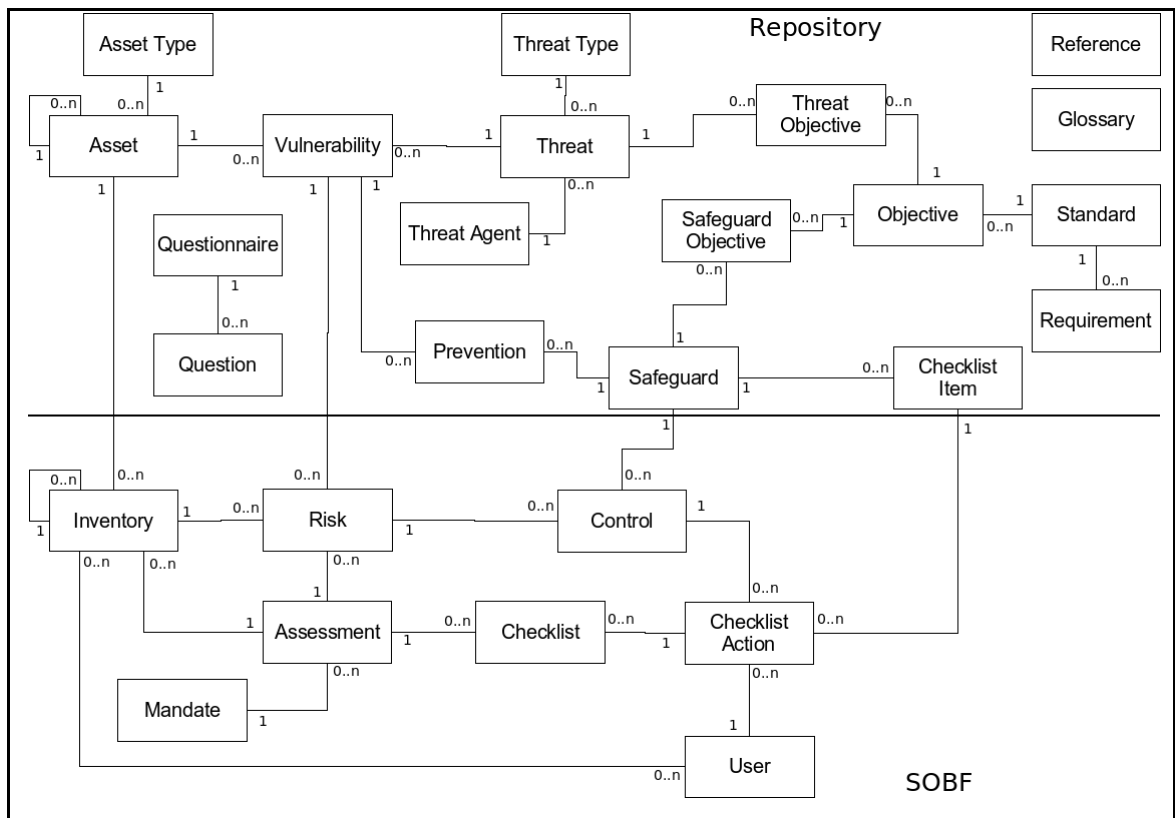


Figura 16: Modelo de datos de SOMAP (ORIMOR)

4.1.14. FAIR – Factor Analysis of Information Risk

Desarrollada por Risk Management Insight (RMI) para mejorar la utilización de los modelos actuales para la realización de análisis de riesgos [JONES05A] [JONES05B] [JONES08A] [JONES08B].

La metodología se centra en aprovechar la experiencia del análisis de riesgos en otros ámbitos empresariales y en mejorar el modelo utilizado en el análisis de riesgos de seguridad de la información, aumentando la precisión en el uso de los conceptos y el detalle en el análisis de los escenarios planteados.

La metodología incide en la naturaleza probabilística del análisis de riesgos y, con ello, la imposibilidad de obtener resultados con el nivel de precisión que se maneja en otros ámbitos de la tecnología.

El modelo consta de los siguientes elementos principales:

- Una taxonomía de factores para el cálculo de riesgos de información.
- Un método para la medición de los factores que forman parte de la taxonomía.
- Un modelo de simulación para la aplicación de la taxonomía y el método de medición.
- Una herramienta informática para la realización de los cálculos asociados al modelo.

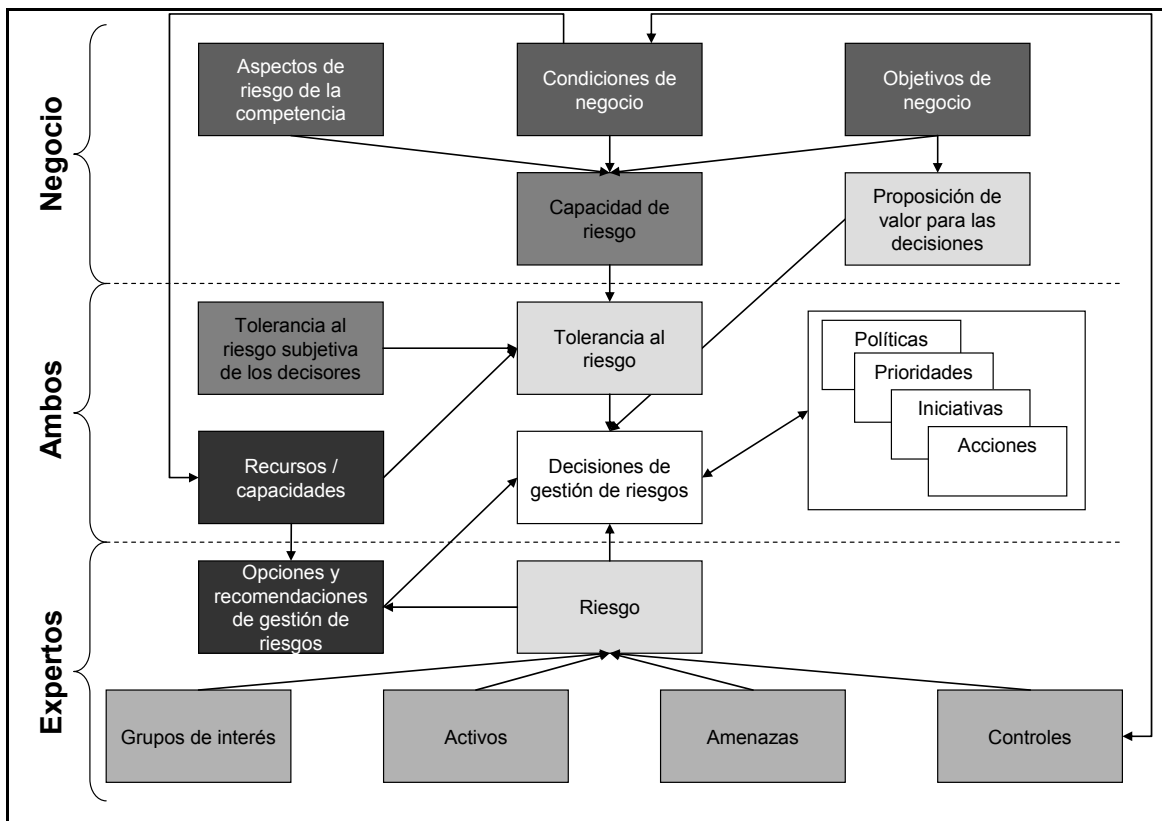


Figura 17: Modelo de decisiones de gestión de riesgos de FAIR

Los principales aspectos en los que incide el modelo son:

- Necesidad de poner en contexto todos los elementos que forman parte del análisis. No es posible valorar la participación en el riesgo de un elemento determinado dentro de un escenario sin tener en cuenta el contexto en el que se produce su participación.
- Valoración de los beneficios que puede obtener la organización un determinado nivel de riesgo.
- Valoración del efecto acumulativo de los riesgos, por el que el riesgo de un conjunto determinado de riesgos concurrentes puede ser superior a la suma de los riesgos individuales (Efecto avalancha).
- Una taxonomía detallada de los factores que influyen en la valoración del riesgo, que se detalla a continuación:

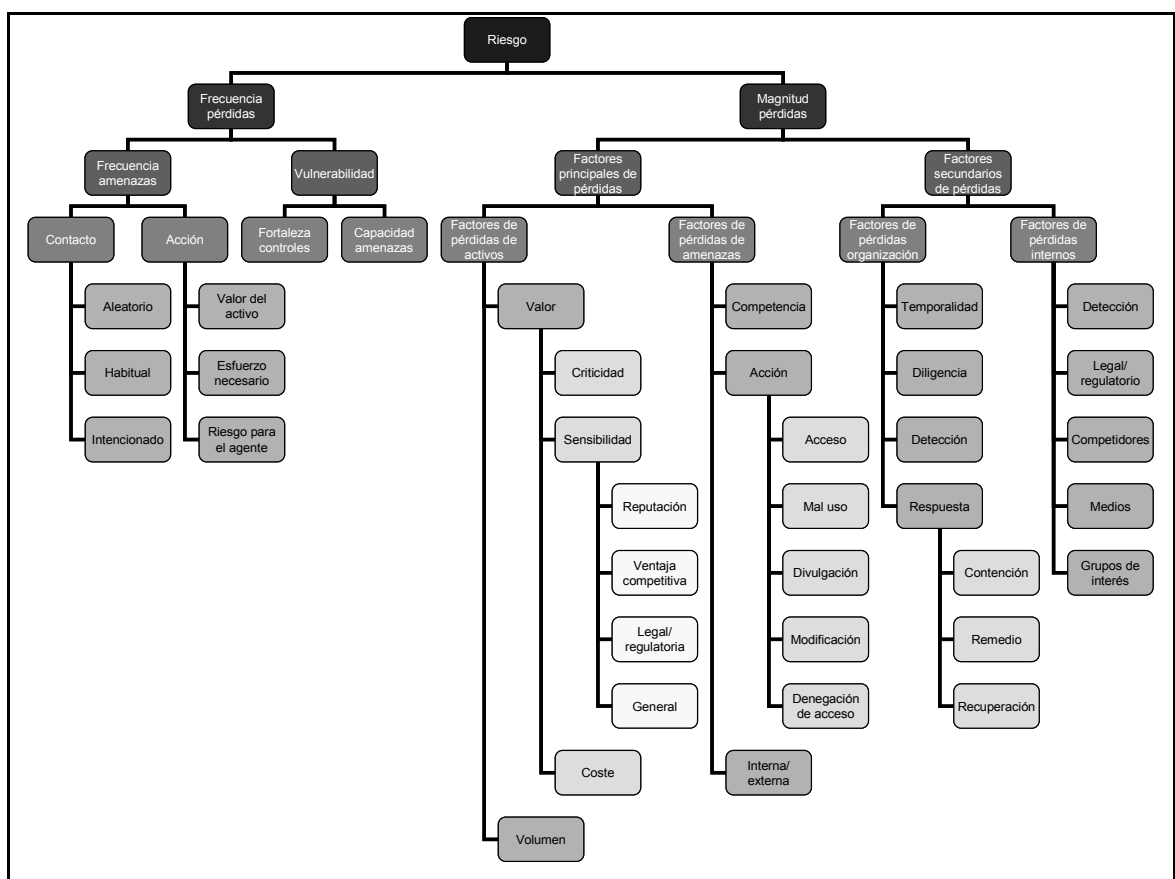


Figura 18: Taxonomía de factores de los riesgos de información de FAIR

4.1.15. Otras metodologías

Adicionalmente a las metodologías descritas, existen otras que no se han analizado en detalle porque se han considerado de menor relevancia en el ámbito español o actual. Algunas de las metodologías descartadas por estos motivos han sido las siguientes:

- FRAP/FRAAP (Facilitated Risk Analysis –and Assessment - Process), metodología simplificada para el análisis de riesgos cualitativo basada en la realización de ejercicios de brainstorming por parte de un grupo de participantes de distintos perfiles complementarios. Su principal característica es la rapidez con la que puede aplicarse. Desarrollada por Peltier Associates.
- PARA (Practical Application of Risk Analysis)
- Austrian IT Security Handbook (sólo disponible en alemán)
- Dutch A&K Analysis (sólo disponible en holandés)
- Ebios (Expression des Besoins et Identification des Objectifs de Sécurité), publicada por la Administración Pública francesa. Incorpora una herramienta de soporte.
- IT-Grundschutz (IT Baseline Protection Manual), publicada por la Administración Pública alemana. Soportado por la herramienta GSTool.
- Mehari publicada por el Club Francés de Seguridad de la Información. Sustituye a una metodología anterior (Marion). Dispone de una herramienta de soporte (Risicare).
- ARiES (Aerospace Risk Evaluation System)
- STIR (Simple Technique for Illustrating Risk)
- CORA (Cost-Of-Risk Analysis)
- ISRAM (Information Security Risk Analysis Method)

4.1.16. Metodologías comerciales

Adicionalmente a las metodologías ya citadas, existe un elevado número de metodologías propietarias soportadas por productos comerciales. Estas metodologías no se han considerado en la realización de este estudio.

Algunas de las metodologías comerciales más relevantes son:

- Acuity Stream
- Amenaza IT Threat Tree Modeling System
- Callio
- Casis
- COBRA (Consultative Objective & Bi-functional Risk Analysis)
- Countermeasures
- GxSGSI
- ISAMM (Information Security Assessment & Monitoring Method)
- MIGRA (Metodologia Integrata per la Gestione del Rischio Aziendale)
- Modulo Risk Manager
- Proteus
- Ra2
- Real ISMS
- ResolverBallot y Resolver Risk
- RiskPAC
- Riskwatch
- RM Studio
- SBA
- Security Risk Management Toolkit
- The Buddy System

4.1.17. Tablas comparativas

Nombre	Origen			
	Descripción	Organización	País	Año ¹
ISO TR 13335:1997	Tecnología de la información – Guías para la gestión de la seguridad de las TI	ISO –International Organization for Standardization	Internacional (Suiza)	1997
ISO 27005:2008	Tecnologías de la información – Técnicas de seguridad – Gestión del riesgo de seguridad de la información	ISO –International Organization for Standardization	Internacional (Suiza)	2008
UNE 71504:2008	Metodología de análisis y gestión de riesgos para los sistemas de información	AENOR – Asociación Española de Normalización y Certificación	España	2008
BS 7799-3:2006	Sistemas de Gestión de Seguridad de la Información – Parte 3: Guías para la gestión de riesgos de seguridad de la información	BSI – British Standards Institution	Reino Unido	2006
AS/NZS 4360:2004	Gestión de riesgos	AS/NZS – Australian Standards / New Zealand Standards	Australia / Nueva Zelanda	2004
MAGERIT	Metodología de Análisis y GEstion de Riesgos de IT	Ministerio de Administraciones Públicas ²	España	2006

¹ Se considera la fecha de publicación de la versión más reciente.

² A través del CSAE, Consejo Superior de Administración Electrónica.

Nombre	Origen			
	Descripción	Organización	País	Año ¹
OCTAVE	Operationally Critical Threat, Asset and Vulnerability Evaluation	Universidad de Carnegie Mellon ¹	Estados Unidos	2001 - 2007
CRAMM	CCTA Risk Analysis and Management Method	CCTA - Central Computing and Telecommunications Agency ²³	Reino Unido	2003
NIST SP 800 – 30	Guía de gestión de riesgos para sistemas de tecnología de información	NIST - National Institute of Standards and Technology	Estados Unidos	2002
IRAM	Information Risk Analysis Methodologies	ISF – Information Security Forum	Internacional (Reino Unido)	2006
CORAS	CONstruct a platform for Risk Analysis of Security critical systems	SINTEF y otros.	Europeo (Noruega)	2001-2007
SOMAP	Security Officers Management & Analysis Project	SOMAP.org	Internacional (Suiza)	Beta ⁴
FAIR	Factor Analysis of Information Risk	Risk Management Insight	Estados Unidos	2005

Tabla 16: Comparativa de metodologías de análisis de riesgos - Responsables

¹ A través del SEI (Software Engineering Institute), dentro del programa CERT (Computer Emergency Response Team).

² Desde 2001 integrada en la OCG (Office of Government Commerce).

³ El mantenimiento lo realiza Insight Consulting, empresa integrada en Siemens.

⁴ Algunos subproyectos no han finalizado la primera versión a la fecha de cierre de este documento.

Nombre	Alcance considerado	
	Análisis de riesgos	Gestión de riesgos
ISO TR 13335:1997	●	●
ISO 27005:2008	●	●
UNE 71504:2008	●	●
BS 7799-3:2006	●	●
AS/NZS 4360:2004	●	●
MAGERIT	●	●
OCTAVE	●	●
CRAMM	●	●
NIST SP 800 – 30	●	●
IRAM	●	●
CORAS	●	●
SOMAP	●	●
FAIR	●	●

Tabla 17: Comparativa de metodologías de análisis de riesgos - Alcance considerado

Leyenda: ● Completo ◐ Amplio ◑ Satisfactorio ◒ Pobre ○ No tiene








































Nombre	Tipo de análisis		
	Cuantitativo	Cualitativo	Mixto
ISO TR 13335:1997			
ISO 27005:2008			
UNE 71504:2008			
BS 7799-3:2006			
AS/NZS 4360:2004			
MAGERIT			
OCTAVE			
CRAMM			
NIST SP 800 – 30			
IRAM			
CORAS			
SOMAP			
FAIR			 ¹

Tabla 18: Comparativa de metodologías de análisis de riesgos - Tipo de análisis

Leyenda:  Completo  Amplio  Satisfactorio  Pobre  No tiene

¹ Considera los métodos mixtos una variante de los métodos cuantitativos, con una reducción en la precisión.

Nombre	Tipo de riesgo		
	Intrínseco	Efectivo	Residual
ISO TR 13335:1997	○	●	◐ ¹
ISO 27005:2008	○	●	◐ ¹
UNE 71504:2008	●	●	◐ ¹
BS 7799-3:2006	○	●	◐ ¹
AS/NZS 4360:2004	○	●	◐ ¹
MAGERIT	●	●	○
OCTAVE	○	●	◐ ¹
CRAMM	●	●	○
NIST SP 800 – 30	○	●	◐
IRAM	●	●	◐ ¹
CORAS	○	●	◑
SOMAP	○	●	◐ ¹
FAIR	○	●	○

Tabla 19: Comparativa de metodologías de análisis de riesgos - Tipo de riesgo

Leyenda: ● Completo ◑ Amplio ◐ Satisfactorio ◑ Pobre ○ No tiene

¹ Proceso iterativo, una vez implantadas las salvaguardas

Nombre	Elementos del modelo						
	Procesos	Activos	Recursos	Dependencias	Vulnerabilidades	Amenazas	Salvaguardas
ISO TR 13335:1997	○	◐	●	◐	●	●	●
ISO 27005:2008	○	●	●	●	●	●	●
UNE 71504:2008	○	●	○	●	○	●	●
BS 7799-3:2006	●	●	●	●	●	●	●
AS/NZS 4360:2004	●	●	●	●	●	●	●
MAGERIT	○	●	○	●	○	●	●
OCTAVE	●	●	●	●	●	●	●
CRAMM	○	●	○	●	●	●	●
NIST SP 800 – 30	○	○	●	○	●	●	●
IRAM	○	●	○	●	●	●	●
CORAS	○	◐	◐	○	◐	●	●
SOMAP	○	○	●	●	●	●	●
FAIR	○	◐ ¹	●	○	●	● ²	●

Tabla 20: Comparativa de metodologías de análisis de riesgos - Elementos del modelo

Leyenda: ● Completo ◐ Amplio ◑ Satisfactorio ◒ Pobre ○ No tiene

¹ Tiene en cuenta un nuevo elemento, los factores de pérdida, para representar aquellos elementos del escenario que, sin ser activos o amenazas, influyen en la magnitud de las pérdidas esperadas.

² No sólo considera las amenazas, sino también incluye una taxonomía de los agentes que provocan las amenazas, ya sea de forma intencionada o accidental.

Nombre	Objetivos de seguridad					
	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Otros
ISO TR 13335:1997	●	●	●	●	●	Fiabilidad
ISO 27005:2008	●	●	●	●	●	Fiabilidad
UNE 71504:2008	●	●	●	◐	◐	◐
BS 7799-3:2006	●	●	●	○	○	○
AS/NZS 4360:2004	●	●	●	○	○	○
MAGERIT	●	●	●	●	●	○
OCTAVE	●	●	●	○	○	○
CRAMM	●	●	●	○	○	○
NIST SP 800 – 30	●	●	●	○	○	○
IRAM	●	●	●	○	○	○
CORAS ¹	◐	◐	◐	◐	◐	◐
SOMAP	●	●	●	●	●	Audita- bilidad
FAIR	●	●	●	○	○	Mal uso Divulgación

Tabla 21: Comparativa de metodologías de análisis de riesgos – Objetivos de seguridad

Leyenda: ● Completo ◐ Amplio ◑ Satisfactorio ◒ Pobre ○ No tiene

¹ Se basa en escenarios definidos por el usuario, y no define objetivos de seguridad concretos.

Nombre	Inventarios				
	Tipos de recursos	Vulnerabilidades	Amenazas	Salvaguardas	Otros
ISO TR 13335:1997	○	●	●	●	Criterios de valoración de activos. Baselines de seguridad
ISO 27005:2008	●	●	●	●	Criterios de valoración de activos. Restricciones para la reducción del riesgo
UNE 71504:2008	○	○	○	○	Factores clave de éxito y de fracaso. Roles y funciones
BS 7799-3:2006	●	●	●	●	Requerimientos legales o de negocio. Procesos de negocio. Roles y funciones.
AS/NZS 4360:2004	○	○	◐	◐	Amenazas genéricas. Criterios de valoración de activos
MAGERIT	●	○	●	◐ ¹	○
OCTAVE	●	● ²	● ³	●	○
CRAMM	●	●	●	●	○
NIST SP 800 – 30	●	●	●	●	○
IRAM	○	● ⁴	● ⁴	● ⁵	○

¹ La metodología define únicamente una taxonomía de salvaguardas. La herramienta PILAR que soporta la metodología incluye un inventario detallado de más de 3.200 salvaguardas.

² Utilizando herramientas externas para la identificación de vulnerabilidades tecnológicas.

³ Mediante perfiles de riesgos.

⁴ A través del estudio bienal de amenazas de seguridad TI (ISF Information Security Status Survey).

⁵ •A través del Manual de buenas prácticas de seguridad de la información (The Standard of Good Practice for Information Security), que incluye un inventario de más de 3.200 salvaguardas.













Nombre	Inventarios				
	Tipos de recursos	Vulnerabilidades	Amenazas	Salvaguardas	Otros
CORAS ¹					Incidentes
SOMAP ²					Dependencias entre tipos de recurso Relaciones activo-amenaza Relaciones amenaza-salvaguarda Relaciones entre el modelo de salvaguardas y modelos externos.
FAIR					Tipos de pérdidas

Tabla 22: Comparativa de metodologías de análisis de riesgos - Inventarios

Leyenda:  Completo  Amplio  Satisfactorio  Pobre  No tiene

¹ No incluye inventarios, pero sí un conjunto de ejemplos de los que se pueden obtener elementos.

² Una vez finalizados los proyectos que están en curso

Nombre	Ayudas a la implantación					
	Herra- mienta	Plan de proyecto	Técnicas	Roles	Compa- rativas	Otros
ISO TR 13335:1997	○	◐	◑	○	○	○
ISO 27005:2008	○	◐	○	◐	○	○
UNE 71504:2008	○	●	○	●	○	○
BS 7799-3:2006	○	◐	○	◐	○	○
AS/NZS 4360:2004	○	◐	○	◐	○	○
MAGERIT	● ¹²	●	●	●	● ³	○
OCTAVE	○	●	●	●	○	Cuestionarios
CRAMM	● ¹	◐	○	●	● ⁴	Cuestionarios
NIST SP 800 – 30	○	○	○	●	○	○
IRAM	● ⁵	○	○	○	○	Soporte del ISF
CORAS	●	●	○	◐	○	Ejemplos
SOMAP ⁶	●	○	○	○	● ⁷	○
FAIR	●	●	○	○	○	○

Tabla 23: Comparativa de metodologías de análisis de riesgos - Ayudas a la implantación

Leyenda: ● Completo ◐ Amplio ◑ Satisfactorio ◒ Pobre ○ No tiene

¹ Herramienta comercial

² Gratuita para su uso por parte de la Administración Pública española.

³ Con LOPD, CNSC e ISO 27002

⁴ Con ISO 27002 y estándares técnicos de Unix y Windows

⁵ Disponible sólo para miembros del ISF

⁶ Una vez finalizados los proyectos que están en curso

⁷ Inicialmente está prevista con ISO 27001, ISO 27002, ISO 27005, COP y German Grundschrift

4.2. Otros tipos de análisis de riesgos

Una vez descritos los principales modelos y metodologías de análisis de riesgos de seguridad de la información, cabe citar brevemente otros tipos análisis de riesgos que se realizan en otros entornos empresariales.

Estos tipos de análisis de riesgos presentan características comunes con el análisis de riesgos de seguridad de la información y, en ocasiones, deben considerarse como iniciativas integradas.

4.2.1. Enterprise Risk Management (ERM)

El Gobierno Corporativo y el Control Interno son disciplinas que han experimentado un extraordinario desarrollo a partir de la década de 1990, y tienen como objetivo la detección y mitigación de los riesgos que amenazan la consecución de los objetivos corporativos [COSO92] [COSO04].

Existen Códigos de Buen Gobierno Corporativo y legislación relevante publicados en prácticamente todos los países, siendo los siguientes los más representativos o que tienen mayor influencia en el ámbito español:

- España: Informe Olivencia (1998), Informe Aldama (2003), Código Unificado de Buen Gobierno (2006)
- OCDE: Principios de Gobierno Corporativo de la OCDE (1999, 2004) [OCDE04] y Guía sobre Gobierno Corporativo de la Empresas propiedad del Estado (2005)
- Comunidad Europea. Informe Winter (2002)
- Reino Unido: Informe Cadbury (1992), Informe Greenbury (1995), Código Hampel (1998), Informe Turnbull (1999), Código Combinado sobre Gobierno Corporativo (2003 y 2006)
- Francia: Informes Viénot (1995 y 1999)
- Alemania: Informe Baums (2001) Código Cromme (2000 a 2006)
- Holanda: Informe Peters (1997), Código Tabaksblat (2003)

- Bélgica: Código Lippens (2004), Código Buysse (2005)
- Estados Unidos: Ley Sarbanes-Oxley (2002)

Dos de los pilares básicos de gran parte de estos códigos son el Control Interno y la Gestión de Riesgos Corporativos.

Las principales referencias en materia de Control Interno y Gestión de Riesgos Corporativos son las publicadas en Estados Unidos por COSO (Committee of Sponsoring Organizations of the Treadway Commission), principalmente:

- Internal Control – Integrated Framework (1992) [COSO92]
- Enterprise Risk Management – Integrated Framework (2004) [COSO04]

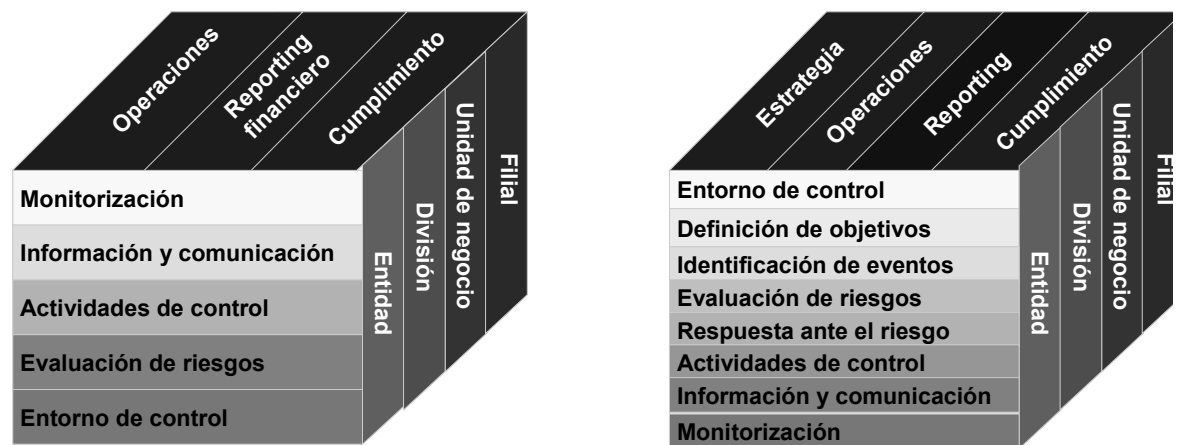


Figura 19: Modelos de Control Interno y de Gestión de Riesgos Corporativos (ERM) de COSO

4.2.2. Strategic Risk Management (SRM)

Definido en 2005 por J. Slyworsky y J. Drzik of Mercer, es un método sistemático para gestionar el riesgo estratégico de una Organización y obtener de ello una ventaja competitiva sobre la competencia.

El modelo distingue siete dominios de riesgo estratégico:

- Industria
- Tecnología
- Marca
- Competencia
- Clientes
- Proyectos
- Estancamiento

4.2.3. Evaluación de riesgo financiero

Existe gran cantidad de métodos que soportan la toma de decisiones sobre inversiones financieras que tienen en cuenta el riesgo incurrido por la inversión.

El objetivo de RAR (Rentabilidad Ajustada al Riesgo, RAROC – Risk Adjusted Return On Capital) consiste en evaluar la rentabilidad de un conjunto de inversiones reales o potenciales teniendo en cuenta la cuantificación de los riesgos que tienen asociados.

El objetivo de VaR (Value at Risk) es determinar, mediante análisis estadísticos basados en históricos y la aplicación de modelos, la pérdida máxima, en circunstancias normales de mercado, que puede sufrir una cartera en un periodo de tiempo determinado.

4.2.4. Basilea II y Solvencia II

Tanto las Entidades Financieras como las Entidades Aseguradoras están obligadas a disponer de un capital disponible (Reservas y provisiones) para cubrir contingencias (impago de deudas, fluctuación de mercados, obligaciones de pago, etc.).

El mantenimiento de dicho capital disponible supone para las Entidades un importante coste de oportunidad, por lo que es importante calcular el capital mínimo necesario.

El Banco de Pagos Internacionales de Basilea (BIS – Bank for International Settlements) ha definido, en el Acuerdo de Basilea II [BIS04], varios métodos para el cálculo de capital mínimo regulatorio para las Entidades Financieras en función del riesgo asumido por la Entidad. El Acuerdo de Basilea II se apoya en tres pilares:

- Pilar I: Requerimientos mínimos de capital, en función del riesgo de tipo de interés, riesgo de crédito y riesgo operativo
- Pilar II: El proceso de supervisión
- Pilar III: Disciplina de mercado

El modelo de Solvencia II está en desarrollo por la Comunidad Europea. Se trata de una transposición del modelo de Basilea II para el Sector Asegurador.

4.2.5. Análisis de riesgos de auditoría

Los procesos de auditoría, ya sea tecnológica o de procesos, requieren la identificación de los principales riesgos que afectan a los procesos o unidades auditados.

Generalmente, el análisis de riesgos que se realiza en auditoría se basa en la documentación de los procesos auditados en flujogramas, y la identificación en ellos de los riesgos mediante el uso de algún marco de referencia.

Una vez identificados, los riesgos se valoran y priorizan, para obtener un mapa o matriz de riesgos.

4.2.6. Análisis de riesgos de proyectos

Los principales riesgos a los que se ve sometido un proyecto son:

- Incumplimiento de objetivos.
- Coste superior al presupuestado.
- Retrasos en la finalización.

Existen distintas metodologías para la gestión de riesgos, entre las que destacan PRINCE2 (PProjects IN Controlled Environments) [PRINCE05] [PRINCE06] [P3M3.06] y PMBOK (Project Management Base Of Knowledge) [PMI00] que especifican los mecanismos necesarios para identificar y mitigar estos riesgos en el contexto de la ejecución de los proyectos.

4.2.7. Análisis de vulnerabilidades

Todos los sistemas de información, ya sean estándar o desarrollos a medida, están sujetos a la aparición de defectos que impacten sobre la seguridad.

El proceso de gestión de vulnerabilidades permite detectar las nuevas vulnerabilidades descubiertas y establecer las medidas necesarias para evitar que la explotación de dichas vulnerabilidades provoque pérdidas para la Organización.

El proceso de gestión de vulnerabilidades se basa en obtención de información, ya sea por parte de los fabricantes, por parte de organizaciones independientes o por información no estructurada recibida en el mercado, de las nuevas vulnerabilidades detectadas, las formas de explotarlas y las medidas preventivas, correctivas, detectivas o paliativas que pueden aplicarse.

4.2.8. Riesgos laborales

Las Empresas tienen diversas obligaciones en relación al mantenimiento de la salud de sus empleados, que se han reflejado en diversas normas y legislaciones de prevención de riesgos laborales.

Las normas más relevantes en materia de riesgos laborales están basadas en la norma BS 8800:2004 y han sido definidas por un grupo de organizaciones normalizadoras y publicadas por BSI dentro de la familia BSI OHSAS 18000 (OHSAS – Occupational Health and Safety Assessment Series).

Las normas publicadas hasta la fecha son las siguientes:

- BSI OHSAS 18001:2007 Occupational Health and Safety Assessment Series - Specifications for OH&S Management Systems.
- BSI OHSAS 18002:2008 Occupational Health and Safety Assessment Series - Guidance for OH&S Management Systems.

4.2.9. Protección de infraestructuras críticas

En los últimos años, la preocupación de los Estados por la ocurrencia de hechos catastróficos ya sean naturales, accidentales o provocados que impidan el funcionamiento normal de grandes regiones ha llevado al desarrollo de planes de protección de infraestructuras críticas.

Se consideran infraestructuras críticas aquellos activos y servicios necesarios para el funcionamiento normal de una comunidad. La Comunidad Europea, en su Comunicación de la Comisión al Consejo y al Parlamento Europeo - Protección de las infraestructuras críticas en la lucha contra el terrorismo (COM (2004) 702) considera críticas las siguientes infraestructuras:

- Centrales y redes de energía;
- Tecnologías de la información y las comunicaciones;
- Finanzas (por ejemplo, banca, valores e inversiones);
- Sector sanitario;
- Alimentación;
- Agua (embalses, almacenamiento, tratamiento y redes);
- Transportes (aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, sistemas de control del tráfico);
- Producción, almacenamiento y transporte de mercancías peligrosas (materiales químicos, biológicos, radiológicos y nucleares);
- Administración (servicios básicos, instalaciones, redes de información, activos, y principales lugares y monumentos nacionales).

Esta preocupación y las actividades que ha originado han provocado la creación de multitud de metodologías de análisis de riesgos especializadas.

La principal característica de estas metodologías consiste en la visión global de los activos o servicios que analizan, puesto que este análisis no se centra en los procesos de una Organización determinada, sino que afectan a sectores completos de actividad.

Algunas de las principales metodologías de análisis de riesgos

- ACAMS (Automated Critical Asset Management System)
- CAPRA (Critical Asset & Portfolio Risk Analysis)
- CARVER (Criticality, Accesibility, Recoverability, Vulnerability, Effect, Recognizability)
- CARVER2web (Criticality, Accesibility, Recoverability, Vulnerability, Espyability, Redundancy)
- HLS-CAM (Homeland Security-Comprehensive Assessment tool)
- MSHARRPP+V (Mission, Symbolism, History, Accessibility, Recognizability, Recoverability, Population, Proximity + Vulnerability)
- PairPM (Pairwise Program Management)
- PSRAT (Port Security Risk Assessment tool)
- RAMCAP (Risk Analysis and Management for Critical Asset Protection)
- Sandia Labs RAM (Risk Assessment Methodologies) Series:
 - RAM-D (Dams)
 - RAM-C (Communities)
 - RAM-W (Water)
 - RAM-WSM (Small Water Utilities, Large Water Utilites)
 - RAM-T (High Voltage Electric Transmission Lines, Oil lines, linear activities)
 - RAM-CF (Chemical Facilites)
 - RAM-FE (Fossil Energy)
 - RAMPART (Property Analysis and Ranking Tool)

- RAM - SEA (Security Evaluation Assessment), para emplazamientos militares.
 - RAM-SS (School Security)
 - RAM-VAM, para prisiones.
- Security Engineering
- VSAT Water and Wastewater (Vulnerability Self Assessment Tool)

5. PLAN DE PROYECTO

5.1. Fases del proyecto

El desarrollo de este proyecto se ha organizado en cuatro fases que se describen en el siguiente gráfico junto con las principales actividades de cada una:



Figura 20: Fases del proyecto

El objetivo de cada una de las fases se describe a continuación:

- FASE I: Definición de la metodología

Definición de la metodología a emplear durante el proyecto, partiendo de las metodologías estándar de análisis de riesgos, combinándolas y adaptándolas a los requerimientos específicos de la Organización.

- FASE II: Desarrollo de la herramienta

Desarrollo de una herramienta informática que soporte la realización de análisis de riesgos utilizando la metodología desarrollada.

- FASE III: Análisis de riesgos

Empleo de la metodología y la herramienta para la realización de un análisis de riesgos que soporte la implantación de un SGSI en la Organización.

- FASE IV: Gestión de riesgos

Desarrollo de un plan de acción en base a la estrategia de gestión de riesgos definida por la Organización y los resultados del análisis de riesgos realizado.

En los siguientes apartados se puede encontrar una descripción más detallada de las tareas realizadas correspondientes a cada fase y actividad.

5.2. Planificación del proyecto

La planificación general del proyecto queda resumida en el siguiente diagrama Gantt:

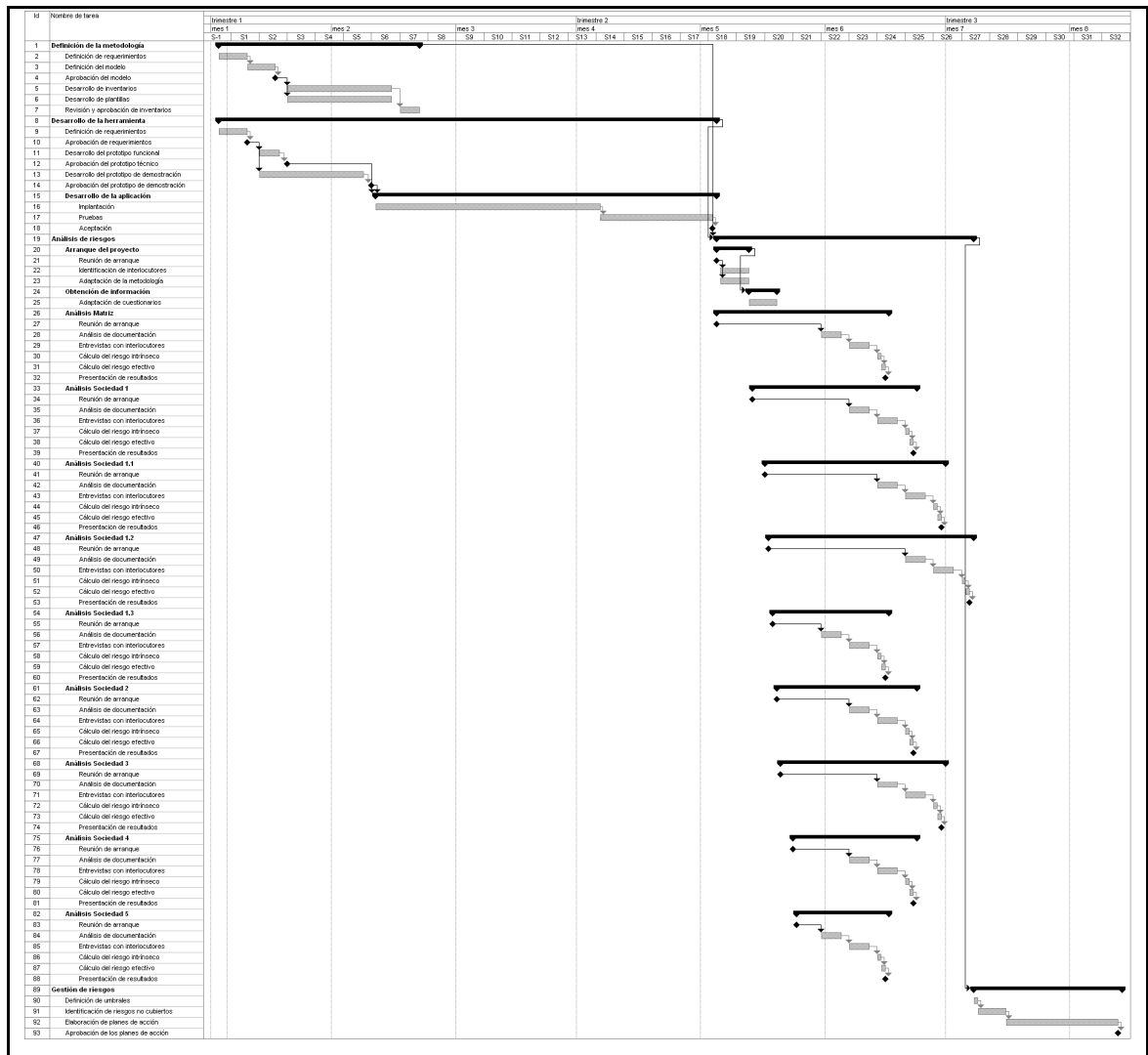


Figura 21: Planificación del proyecto

5.3. Equipo de trabajo

El equipo de trabajo definido para la ejecución de cada una de las fases del proyecto fue el siguiente:

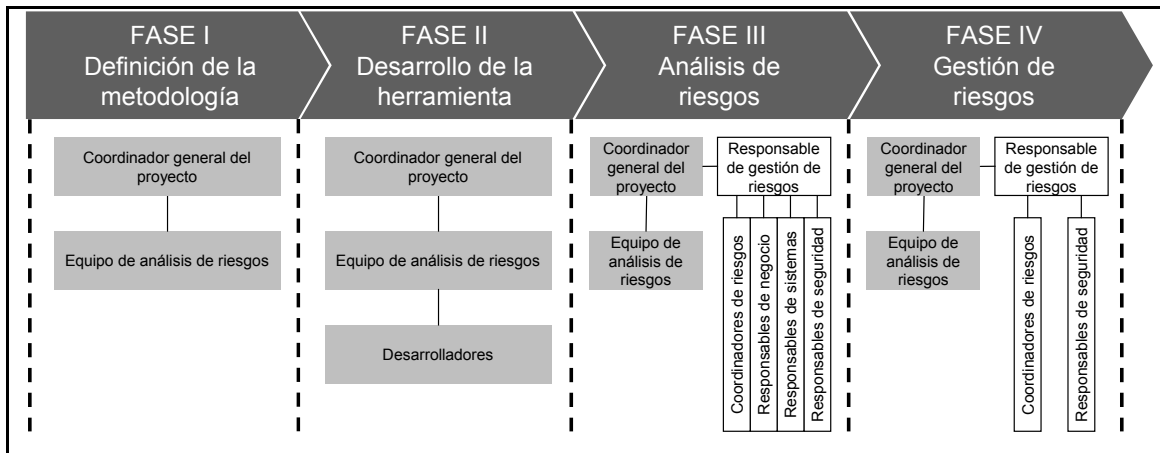


Figura 22: Organización del equipo de trabajo

La asignación de tareas a los diferentes miembros del equipo de trabajo se describe a continuación:

- **Coordinador general del proyecto.** Asumió las siguientes funciones:
 - Liderar los distintos equipos de trabajo, asignando funciones y responsabilidades.
 - Planificar y coordinar las actividades de los distintos equipos de trabajo.
 - Proporcionar el soporte técnico y metodológico necesario para ejecutar las distintas tareas.
 - Proporcionar la formación necesaria a los distintos equipos de trabajo.
 - Supervisar la calidad de los diferentes resultados obtenidos en la ejecución de las distintas tareas.
 - Realizar un seguimiento de cumplimiento de plazos y objetivos.

- **Responsable de gestión de riesgos de la Organización.** Asumió las siguientes funciones:
 - Liderar el proyecto en la Organización, proponiendo y patrocinando el proyecto ante la Dirección, proporcionando información sobre el avance del proyecto y presentando los resultados intermedios y finales.
 - Definir el alcance del proyecto en la Organización.
 - Aprobar los ajustes en la metodología para la realización del análisis de riesgos.
 - Coordinar el proyecto con las distintas Sociedades de la Organización consideradas dentro del alcance.
 - Realizar el seguimiento del equipo de trabajo, verificando el cumplimiento de los distintos hitos y la calidad de los resultados obtenidos.
- **Equipo de análisis de riesgos.** Asumió las siguientes funciones:
 - Ajustar la metodología a las necesidades del proyecto.
 - Definir los requerimientos para la herramienta de soporte a la metodología.
 - Preparar los cuestionarios adaptados a la metodología y a las necesidades de la Organización.
 - Analizar la documentación recibida de las distintas áreas de la Organización.
 - Mantener entrevistas con los intervinientes para obtener la información necesaria para el análisis de riesgos. En las reuniones la función del equipo de análisis de riesgos es ayudar en la aplicación de la metodología y en la unificación de criterios. La identificación y valoración de activos, recursos y salvaguardas deben ser realizadas por los respectivos responsables.
 - Realizar la valoración de los riesgos utilizando la herramienta desarrollada en la fase anterior.

- **Coordinadores de riesgos de cada Sociedad.** Asumieron las siguientes funciones:
 - Recopilar la documentación relevante para el proyecto.
 - Definir los procesos de la Sociedad a considerar en el análisis.
 - Establecer un calendario de reuniones con el personal de la Sociedad relevante para el proyecto.
 - Revisar los resultados obtenidos en el análisis de riesgos de la Sociedad.
- **Responsables de negocio:** Asumieron las siguientes funciones:
 - Proporcionar documentación sobre los procesos bajo su responsabilidad.
 - Completar y aclarar la documentación proporcionada.
 - Definir los procesos de la Sociedad a considerar en el análisis.
 - Identificar y valorar los activos de información relevantes para sus procesos.
 - Identificar los recursos que soportan los activos de información identificados.
- **Responsables de Sistemas de Información:** Asumieron las siguientes funciones:
 - Proporcionar documentación sobre los recursos de información bajo su responsabilidad.
 - Completar y aclarar la documentación proporcionada.
 - Identificar recursos de información relevantes y asociarlos a los activos de información correspondientes.
- **Responsables de Seguridad de la Información:** Asumieron las siguientes funciones:
 - Proporcionar documentación sobre las salvaguardas implantadas en la Sociedad.
 - Completar y aclarar la documentación proporcionada.
 - Identificar y valorar las salvaguardas implantadas en la Sociedad.

- **Desarrolladores.** Asumieron las siguientes funciones:
 - Desarrollar la herramienta informática a partir de las especificaciones proporcionadas por el equipo de análisis de riesgos.

6. FASE I: DEFINICIÓN DE LA METODOLOGÍA

6.1. Definición de requerimientos

Teniendo en cuenta las distintas metodologías disponibles para hacer el análisis de riesgos, se decidió desarrollar una metodología adaptada específicamente a las necesidades de la Organización.

Las características deseables en la metodología a desarrollar son los siguientes:

- Basada en estándares, para aprovechar conocimiento y herramientas y permitir la realización de comparaciones con otras organizaciones.
- Sencillez y facilidad de uso, tanto en el momento de la primera implantación como en el mantenimiento.
- Enfocada a los procesos de negocio y de soporte de la Organización.
- Modular y adaptable, que pueda adaptarse a diferentes entornos.
- Objetiva, los resultados no deben depender de quién aplique la metodología ni de cómo lo haga.

Dadas las características deseables para la metodología, se han desarrollado unos principios para su desarrollo:

- Metodología mixta, con entrada de datos cualitativa, para facilitar la comunicación entre las distintas partes que deben participar en el análisis y métodos de cálculo cuantitativos para aprovechar la mayor eficiencia computacional y mayor precisión en los resultados.
- Utilización de los principios básicos comunes a las principales metodologías de análisis de riesgos estándar. Utilización de principios, estándares y metodologías estándar en los aspectos que se deban tratar y no cubran las metodologías estándar de análisis de riesgos.
- Eliminación de los elementos que aporten menor valor en la consecución de los objetivos, en aras de mayor facilidad de uso y claridad.

- Que disponga de diversos inventarios de tipos de activos, amenazas y salvaguardas, de modo que se pueda utilizar con sencillez y que se pueda adaptar fácilmente a distintas necesidades y objetivos del análisis.
- Que disponga de una herramienta de soporte específica que facilite la entrada de datos y la realización de los cálculos.
- Que disponga de todos los elementos habituales que permiten dotar de objetividad al proceso: acuerdo entre varios expertos, definición de baremos objetivos de valoración y proporcionar ejemplos con valores de referencia reales.

6.2. Desarrollo del modelo

6.2.1. Modelo de la metodología

Para definir la presente metodología se ha considerado el modelo que forma la base de todas las metodologías estándar de análisis de riesgos, y se han seleccionado las diferentes alternativas disponibles para la definición del modelo teniendo en cuenta los principios descritos.

El modelo general de la metodología está resumido en el siguiente diagrama:

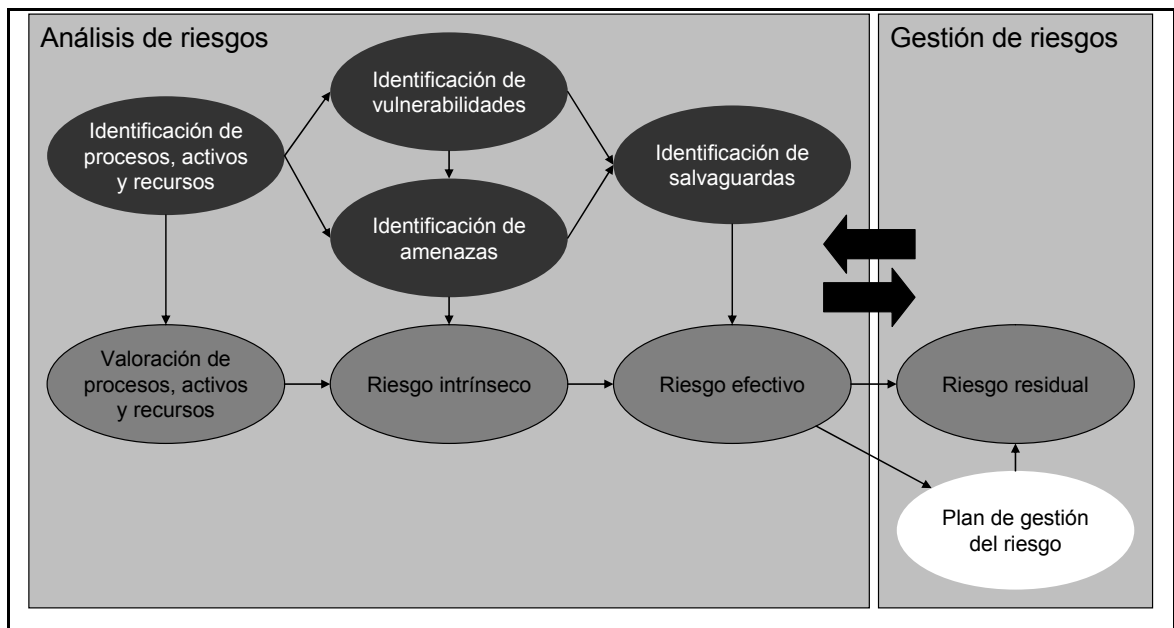


Figura 23: Modelo general de la metodología de análisis de riesgos

En primer lugar, el modelo diferencia dos fases diferenciadas:

- **Análisis de riesgos**, que comprende la obtención de información referente a procesos, activos, recursos, vulnerabilidades, amenazas y salvaguardas.
- **Gestión de riesgos**, que comprende la definición de la estrategia a seguir para ajustar el nivel de riesgo a los requerimientos de la Organización.

En este modelo se distinguen por colores tres tipos de elementos:

- Inventario de activos, vulnerabilidades, amenazas y salvaguardas.
- Valoración de activos, vulnerabilidades, amenazas y salvaguardas para la obtención del riesgo intrínseco, efectivo y residual.
- Plan de gestión del riesgo.

Por último, el modelo especifica que el análisis de riesgos debe considerarse un ciclo por el que, tras la gestión del riesgo se sitúa una nueva iteración del análisis de riesgos que permite obtener la evolución de los procesos, activos, recursos, vulnerabilidades, amenazas y salvaguardas y de esta forma reajustar permanentemente el nivel de riesgo a los requerimientos de la Organización.

6.2.2. Fases de la metodología

6.2.2.1. Valoración de procesos de negocio

Los procesos de la Organización suponen el elemento de mayor valor del modelo, puesto que son los que permiten a la Organización cumplir sus objetivos de negocio.

Los procesos de la Organización pueden dividirse en:

- **Procesos de negocio** o productivos, que son los definidos para cumplir el cometido y los objetivos de la Organización.
- **Procesos de soporte** o de apoyo, que son los procesos cuyo objetivo consiste en asegurar el funcionamiento de los procesos de negocio.

La metodología requiere la identificación de los diferentes procesos de negocio y de soporte, por diferentes motivos:

- Poner en contexto el resto de elementos a valorar: activos, recursos, amenazas, salvaguardas, etc.
- Definir la importancia relativa de los distintos elementos del sistema.
- Descartar de forma precoz los procesos que no disponen ni requieren de información relevante, y que, por tanto, pueden obviarse durante el análisis de riesgo, reduciéndose en consonancia el esfuerzo necesario para la realización del análisis sin afectar a la calidad del resultado final.

Las tareas a realizar en relación con los procesos de negocio son:

- Inventariar los procesos dentro del alcance del análisis de riesgo.
- Documentar brevemente los objetivos de cada uno de los procesos de negocio, para facilitar la interpretación posterior del análisis realizado.
- Identificar las relaciones existentes entre los distintos procesos: dependencia, secuencia, etc.
- Realizar un análisis informal de riesgos de seguridad de la información a alto nivel, que permita descartar aquellos procesos que no resulten de interés para las fases posteriores.

6.2.2.2. Valoración de activos de información

Una vez identificados los procesos críticos para el negocio, se debe identificar los activos de información relevantes involucrados en cada uno de ellos.

Se considera **activo de información** a toda aquella información que tiene valor para la Organización en la medida en que le permite el cumplimiento de sus objetivos. En oposición, los **recursos de la información** tienen un valor intrínseco generalmente despreciable para la Organización, y son necesarios en la medida en que permiten el manejo de los activos de información.

Los activos de información son intangibles, esto es, la tarea no consiste en identificar aplicaciones ficheros o bases de datos sino la información que se utiliza en el proceso desde un punto de vista conceptual.

Para facilitar un método sistemático para la identificación de los activos de información existen dos enfoques que pueden utilizarse independiente o conjuntamente:

- Enfoque **top-down** (de arriba abajo), que consiste en inferir los activos de información relacionados con los procesos a partir de la descripción de los procesos.

- Enfoque **bottom-up** (de abajo arriba), que consiste en identificar las principales aplicaciones, ficheros y bases de datos utilizados por el proceso y conceptualizar la información que almacenan y procesan. En este enfoque no se debe olvidar la importancia de la información no automatizada que pueda ser relevante para el análisis y que en función del alcance definido, puede formar parte del alcance del análisis de riesgos.

Para cada activo de información identificado se debe registrar, al menos, la siguiente información:

- Nombre del activo de información.
- Descripción del contenido del activo de información.
- Descripción del uso que se da a esta información en el contexto del proceso considerado y de otros procesos que puedan estar relacionados.
- Recursos de información que se utilizan para procesar y almacenar el activo de información.

Una vez inventariados los activos de información es necesario identificar y documentar el valor que su seguridad representa para la Organización. Para ello, se asignará un conjunto de valores a cada activo teniendo en cuenta los diferentes requerimientos de seguridad que se consideren relevantes teniendo en cuenta el alcance y el objetivo definido para el análisis de riesgos.

El valor que tienen los activos de información para la Organización en el ámbito de la seguridad puede medirse desde diversos puntos de vista. Estos puntos de vista se denominan, en el marco de esta metodología, requerimientos de seguridad.

La valoración se deberá realizar mediante una ponderación de las pérdidas ocasionadas para la Organización en caso de que se pierda, debido a la realización de una amenaza, cada uno de los requerimientos de seguridad definidos para los diferentes activos de información.

En aras de la adaptabilidad, la metodología no define un conjunto de requerimientos de seguridad cerrado a utilizar, que deberá definirse para cada análisis, si bien, a título orientativo, se proponen los siguientes requerimientos de seguridad que pueden valorarse al definir los requerimientos a considerar, procedentes de diversas metodologías:

- Confidencialidad (generalmente aceptado)
- Integridad (generalmente aceptado)
- Disponibilidad (generalmente aceptado)
- Trazabilidad - Responsabilidad – Auditabilidad (ISO 13335-1 [ISO13335-1.04], MAGERIT [MAGE06], SOMAP [SOMAP07])
- Autenticidad - No repudio (ISO 13335-1 [ISO13335-1.04], MAGERIT [MAGE06])
- Fiabilidad (ISO 13335-1 [13335-1.04], COBIT [ISACA07])
- Efectividad (COBIT [ISACA07])
- Eficiencia (COBIT [ISACA07])
- Cumplimiento (COBIT [ISACA07])
- Mal uso (FAIR [JONES05A])
- Divulgación (FAIR [JONES05A])

La valoración de la disponibilidad requiere considerar el impacto en función de distintos tiempos de indisponibilidad. Para simplificar el modelo y homogeneizar el tratamiento de los diferentes requerimientos de seguridad sólo se considera el impacto en caso de indisponibilidad indefinida, por tanto, en caso de superarse el Tiempo Objetivo de Recuperación (RTO - Recovery Time Objective) o el Punto Objetivo de Recuperación (RPO – Recovery Point Objective) [MAGE06].

Conviene destacar que los distintos requerimientos de seguridad no son totalmente independientes entre sí, existiendo algunos requerimientos para los que se espera una elevada correlación. Algunos ejemplos de estas correlaciones son:

- Un requerimiento elevado de confidencialidad se espera que generalmente lleve asociado un elevado requerimiento de trazabilidad, debido a la necesidad de identificar accesos no autorizados a la información.
- Un requerimiento elevado de integridad se espera que generalmente lleve asociado un elevado requerimiento de trazabilidad, debido a la necesidad de identificar modificaciones no autorizadas de la información.
- Un requerimiento elevado de disponibilidad se espera que generalmente lleve asociado un elevado requerimiento de integridad, debido a que el impacto entre no disponer de información para la ejecución de un proceso y que la información disponible no sea fiable, será generalmente similar.
- Un requerimiento elevado de confidencialidad se espera que generalmente lleve asociado un elevado requerimiento de autenticidad de usuarios, por la necesidad de garantizar la identidad de las personas que acceden a la información.
- Un requerimiento elevado de integridad se espera que generalmente lleve asociado un elevado requerimiento de autenticidad de usuarios, por la necesidad de garantizar la identidad de las personas que modifican la información.
- Un requerimiento elevado de integridad se espera que generalmente lleve asociado un elevado requerimiento de autenticidad de datos, debido a que el impacto de utilizar datos no fiables y utilizar datos no auténticos será, en muchos casos, similar.

La metodología a emplear en este proyecto utiliza una valoración de activos cualitativa, si bien a cada valor de la escala se le asigna un valor cuantitativo fijo. Esto permite utilizar los métodos de cálculo del riesgo cuantitativos, que aportan mayor precisión que los cualitativos. La escala cualitativa deberá determinarse en función del entorno, si bien no deberá ser lineal, sino exponencial, para facilitar la diferenciación de los riesgos más importantes [JONES05A].

La metodología no define una escala determinada a utilizar en la valoración, recomendándose utilizar escalas de entre 3 y 10 valores, en función de las necesidades de cada análisis de riesgos. La escala por defecto tiene 5 niveles y está recogida en el anexo III de este documento.

6.2.2.3. Valoración de recursos de información

Se considera **recurso de información** a cualquier elemento que se emplea en el manejo de activos de información.

Para facilitar la identificación de los recursos de información se considera necesario disponer de un inventario de tipos de activos de información, que se ha elaborado en base al inventario de la metodología MAGERIT [MAG06], y se puede encontrar en el anexo IV. Este inventario puede modificarse para adaptarlo a las necesidades específicas de cada análisis de riesgos.

Todos los recursos de información que se identifiquen deben asignarse a una de las categorías definidas para facilitar el análisis posterior.

Debido a que los recursos de información no tienen valor por sí mismos (o se considera que, en general, éste será despreciable), sino sólo en la medida en que permiten el manejo de los activos de información, que sí que tienen un valor intrínseco para la Organización, los recursos de información no se valoran.

Un tipo especial de recurso de información corresponde a las salvaguardas de seguridad. Las salvaguardas de seguridad, como cualquier otro recurso de información están sometidas a amenazas y, por tanto, deben identificarse, sus riesgos deben evaluarse y deben establecerse las medidas de protección necesarias.

6.2.2.4. Dependencias entre activos y recursos de información

Cada activo de información está soportado por uno o más recursos de información. No pueden existir activos de información sin recursos que permitan su manejo [MAGE06].

Cada recurso de información soporta uno o más activos de información. No pueden existir recursos de información cuya existencia no esté justificada por el soporte a uno o varios activos de información.

La identificación de las relaciones de dependencia entre activos y recursos de información es clave en la aplicación de la metodología, puesto que la asignación de valor a los recursos de información no se realiza directamente, sino a través de los activos de información que soportan, y, de forma inversa, los activos de información, al ser conceptuales, no tienen amenazas sino a través de los recursos de información que los procesan.

Para simplificar el modelo se considera que, en caso de existir, la dependencia que los activos tienen de los recursos asociados es total.

Debido a que se desprecia el valor intrínseco de los recursos de información y a que las dependencias son totales, la creación de una jerarquía de dependencias entre recursos de información no aporta información adicional. Por ello, no se consideran dependencias entre los diferentes recursos de información, sino que todos los recursos soportan directamente sus activos.

6.2.2.5. Valoración de vulnerabilidades

La metodología no considera explícitamente el concepto de vulnerabilidad. Este concepto queda reflejado en el hecho de que no todas las amenazas son aplicables a todos los recursos. Por tanto, la consideración de que una amenaza pueda afectar a un recurso supone la posibilidad de que el activo pueda tener vulnerabilidades ante esa amenaza [MAGE06].

6.2.2.6. Valoración de amenazas

Una amenaza es cualquier causa potencial, ya sea intencional o fortuita, de un daño a un recurso de información, y, por extensión, a los activos de información que dicho recurso soporta [ISO13335-1.04].

Para la valoración de las amenazas es necesario estimar un ratio anual de ocurrencia y un porcentaje de degradación para cada uno de los requerimientos de seguridad definidos. [MAGE06] [ALBER01] [JONES05A]

Para la estimación de la frecuencia cabe diferenciar las amenazas intencionadas de las fortuitas.

En el caso de amenazas fortuitas, algunos de los principales factores que pueden considerarse para estimar la frecuencia incluyen:

- Información histórica de la realización de las amenazas en el entorno analizado. Por ejemplo, estudio de la climatología y de las catástrofes naturales ocurridas en el entorno de un CPD.
- Exposición de los activos a cada amenaza. Algunos ejemplos relevantes son :
 - Estudios geológicos para determinar la frecuencia de siniestros como inundaciones, terremotos, corrimientos de tierra, etc.

- Análisis del entorno para determinar la posibilidad de ocurrencia de siniestros específicos como: incendios, pérdida de fluido eléctrico, pérdida de comunicaciones, aislamiento por nevadas, huelgas o manifestaciones, accidentes en medios de locomoción, congestiones graves de tráfico, etc.
- Cambios en la estructura organizativa o tecnológica de la Organización. Cualquier cambio en una Organización supone un periodo de estabilización y de formación del personal en el que se incrementa la frecuencia en la comisión de errores.
- Externalización de procesos. La existencia de procesos externalizados puede incrementar la frecuencia de incidentes fortuitos de seguridad, debidos a la compartición de recursos con otras organizaciones que puedan ser atacadas o por la realización de amenazas sobre los contratistas.

En el caso de las amenazas intencionadas, algunos de los principales factores que pueden considerarse para la estimación de la frecuencia incluyen:

- Beneficio que un potencial atacante puede esperar de la realización del ataque. Si los potenciales atacantes pueden esperar un beneficio elevado de sus ataques, estos se producirán con mayor frecuencia.
- Dificultad que un potencial atacante percibe de la realización del ataque, y conocimientos y material necesarios para su ejecución. Si la Organización proyecta una imagen de debilidad en la protección de su información, por ejemplo, a través de noticias en prensa, o a través de la percepción de empleados y terceros, la frecuencia con la que es atacada puede incrementarse.
- Existencia de motivaciones no económicas para la realización de sabotajes: conflictividad laboral, relaciones agresivas con competidores, proveedores o clientes, etc. El sabotaje se producirá con mayor frecuencia cuanto mayor sea el número de motivaciones para realizarlo.

- El mercado en el que opera la Organización. Industrias como la militar, la seguridad privada, la investigación bio-sanitaria, la cría de determinados animales o el sector financiero están sometidos con mayor frecuencia a ataques contra su información.
- Relevancia de la Organización. Si una Organización tiene una especial exposición al público, por su elevado número de empleados, de clientes, o por su actividad comercial y de marketing, el número de potenciales atacantes que pueden planear un ataque se incrementa, y con ello la frecuencia de los ataques.
- Volumen de tratamiento de información relacionada con terceros. La existencia de un elevado número de puntos de entrada y salida de información con terceros supone la existencia de múltiples puntos de ataque que pueden ser utilizados por potenciales atacantes que tienen noticia de ellos, incrementándose con ello la frecuencia de los ataques.
- Conocimiento de la estructura organizativa y tecnológica de la Organización. La información disponible por parte de terceros o de la opinión pública sobre la Organización puede utilizarse para realizar ataques. Por ello, cuanto mayor sea el volumen de información en manos de terceros: empleados, proveedores, clientes, etc. mayor será la frecuencia en la que esta información será utilizada contra la Organización para la realización de ataques.

La estimación del impacto de las amenazas sobre los distintos requerimientos de seguridad de los recursos de información se expresa en porcentajes de degradación. La estimación de estos porcentajes se realiza en función de diversos factores. Algunos de los principales factores a considerar al realizar las estimaciones son:

- Capacidad de la amenaza de afectar a todo el recurso o sólo a una parte del mismo.
- Si la amenaza afecta a partes clave o a partes accesorias del recurso de información.

- Si la amenaza, una vez realizada, afecta de forma puntual o de forma permanente al recurso.

La metodología proporciona un inventario clasificado de amenazas basado en el proporcionado por la Metodología MAGERIT [MAGE06] que puede consultarse en el anexo V. Este inventario incluye unos valores de referencia de la frecuencia y el impacto de cada amenaza sobre cada uno de los tipos de recurso de información definido que no se han incluido en el documento debido a su elevado volumen.

En función de los objetivos definidos para el análisis de riesgos el inventario de amenazas puede ajustarse a los requerimientos específicos o sustituirse por otro que se adapte mejor a ellos.

Los valores de referencia propuestos pueden aceptarse para la realización de un análisis de riesgos rápido y menos preciso o pueden ajustarse en función de cada uno de los recursos de información identificado, para realizar un análisis de riesgos más laborioso y preciso.

6.2.2.7. Cálculo del riesgo intrínseco

Se considera que el riesgo intrínseco es la pérdida anual esperada considerando que no existe ninguna salvaguarda que proteja los recursos de información de sus amenazas. [MAGE06]

La pérdida anual se calcula teniendo en cuenta:

- El valor de los activos de información.
- La exposición de los recursos de información a las amenazas, medida en términos de frecuencia y porcentaje de degradación.

De acuerdo con las definiciones ya vistas en la introducción, el riesgo intrínseco de los recursos de información puede definirse como:

$$\begin{aligned}\text{Riesgo}_B &= \sum_T (\text{ARO}(T) \times \text{SLE}(T)) = \\ &= \sum_T \left(\text{ARO}(T) \times \sum_A \sum_R \text{Valor}(A, R) \times \text{Degradación}(B, R, T) \right)\end{aligned}$$

Donde:

- B representa el recurso de información a considerar
- A representa el conjunto de activos soportados por el recurso
- R representa cada uno de los requerimientos de seguridad definidos para la realización del análisis
- T representa cada una de las amenazas del recurso

De forma análoga, y también de acuerdo con las definiciones incluidas en la introducción, el riesgo intrínseco de los diferentes activos de información puede definirse como:

$$\begin{aligned}\text{Riesgo}_A &= \sum_B \sum_T (\text{ARO}(T) \times \text{SLE}(T)) = \\ &= \sum_B \sum_T \left(\text{ARO}(T) \times \sum_R \text{Valor}(A, R) \times \text{Degradación}(B, R, T) \right)\end{aligned}$$

Donde:

- A representa el activo de información a considerar.
- B representa el conjunto de recursos de información que soportan a A.
- R representa cada uno de los requerimientos de seguridad definidos para la realización del análisis
- T representa cada una de las amenazas de los distintos recursos que soportan el activo de información.

6.2.2.8. Valoración de salvaguardas

Las salvaguardas son las medidas establecidas por la Organización para mitigar sus riesgos. Las salvaguardas pueden reducir la probabilidad de éxito de una amenaza reduciendo, por tanto, su frecuencia y/o reducir el impacto en caso de producirse. [MAGE06]

La eficacia de una salvaguarda para una determinada amenaza y recurso de información se mide en el porcentaje de reducción de la probabilidad y el impacto. La eficacia de las salvaguardas está determinada por un conjunto de factores que incluye los siguientes:

- **Diseño de la salvaguarda:** capacidad de la salvaguarda para prevenir o reducir el impacto de la amenaza considerada, teniendo en cuenta su naturaleza y la calidad de la implantación.
- **Tipo de salvaguarda:** las salvaguardas preventivas son más eficaces que las detectivas, puesto que son capaces de impedir la realización de la amenaza, y no se limitan a detectar su realización para limitar el impacto.
- En el caso de las salvaguardas detectivas, su eficacia viene determinada por la **fiabilidad** de su detección (porcentaje de falsos positivos y falsos negativos), por la **sensibilidad** (número de incidentes necesarios para su activación) y por la **velocidad de respuesta** que proporcionan, en función de los datos que sea necesario recabar para identificar y delimitar la causa del incidente detectado.
- **Operación de la salvaguarda:** las salvaguardas automáticas son más eficaces que las manuales, puesto que las manuales están sujetas al error humano y al fraude.
- **Formación de los responsables de su configuración y operación:** cuanto mayor sea la formación de los responsables en el ámbito de la salvaguarda mayor será su capacidad de ajustarla a las necesidades y hacerla más eficaz.

- **Facilidad de implantación, configuración y mantenimiento:** las salvaguardas complejas están sometidas a una mayor probabilidad de errores en su implantación y mantenimiento, por lo que pueden considerarse menos eficaces que las sencillas.
- **Especificidad de las salvaguardas:** las salvaguardas definidas específicamente para mitigar un número reducido de riesgos son, generalmente, más eficaces para mitigar estos riesgos que otras salvaguardas más generales.
- **Dependencias entre salvaguardas:** existen salvaguardas que dependen de otras para un funcionamiento óptimo. Esta dependencia supone una debilidad en la medida en que su eficacia puede estar afectada por aspectos externos y, por tanto, se pueden considerar menos eficaces.
- **Dependencia de los usuarios:** existen salvaguardas que dependen del cumplimiento de determinados criterios por parte de los usuarios. Cuanto menor sea la concienciación y formación de los usuarios, mayor sea su número y su dispersión organizativa y/o geográfica y menores los mecanismos de control, menos será la eficacia de la salvaguarda.
- **Control interno:** la existencia de procedimientos de verificación y revisión periódicos o continuos permite evitar que el funcionamiento de la salvaguarda se degrade con el tiempo, y aseguran que la salvaguarda evoluciona con las necesidades de la Organización, aumentando su eficacia.

La metodología incluye un inventario de salvaguardas obtenido del código de buenas prácticas ISO/IEC 27002:2007 [ISO27002.05], según se recoge en el Anexo VI de este documento. Se ha elegido este inventario de salvaguardas por diversos motivos:

- Alineación con el objetivo de implantar un SGSI bajo la norma ISO/IEC 27001:2005 [ISO27001.05].

- Nivel adecuado de granularidad: 133 controles, frente a los 69 controles definidos en el inventario de MAGERIT [MAGE06], los 318 objetivos de control definidos por COBIT [ISACA07], o los más de 3.000 controles definidos en el código de buenas prácticas publicado por el Information Security Forum (ISF)[ISF07] o por CRAMM [CRAMM03].
- Uso extendido y conocimiento del código de buenas prácticas.

En función de los objetivos definidos para el análisis de riesgos, el inventario de salvaguardas puede ajustarse a los requerimientos específicos o sustituirse por otro que se considere más adecuado.

De la misma forma que se estableció una valoración por defecto de las distintas amenazas se ha desarrollado una valoración por defecto de la efectividad de cada una de las salvaguardas para cada tipo de recurso y amenaza, considerando la reducción de la probabilidad y la reducción del impacto para cada uno de los requerimientos de seguridad. Esta tabla no se ha incluido en este documento debido a su volumen: al aplicar la combinatoria entre amenazas y salvaguardas se obtiene una tabla de cerca de 8.000 registros.

Debido a que no existe ninguna fuente de datos fiable sobre la eficacia de los controles para mitigar las distintas amenazas, se ha realizado un análisis cualitativo para realizar dicha valoración:

- Se ha realizado una valoración de la efectividad sobre una escala de 4 valores:
 - **Sin efecto** → La salvaguarda no tiene ningún impacto sobre la amenaza.
 - **Poca efectividad** → La salvaguarda tiene un impacto indirecto o general sobre la amenaza.
 - **Efectivo** → La salvaguarda reduce la frecuencia o el impacto de la amenaza de forma significativa.

- **Muy efectivo** → Salvaguarda específicamente diseñada para la amenaza.
- Se ha asignado un valor numérico a cada nivel de la escala para permitir el uso de los cálculos cuantitativos. La asignación se ha realizado considerando los siguientes criterios:
 - Escala de tipo exponencial, que permita diferenciar las salvaguardas muy efectivas del efecto combinado de salvaguardas menos efectivas.
 - La aplicación de todos los controles supone una mitigación superior al 99% del riesgo. Debido al método de cálculo utilizado en la estimación del riesgo efectivo (ver próximo apartado), no es posible reducir el riesgo hasta cero.

	Eficacia de los controles
Sin efecto	0%
Poca efectividad	1%
Efectivo	4%
Muy efectivo	10%

Tabla 24: Valoración de la eficacia de los controles

Adicionalmente, el grado de implantación de las salvaguardas puede variar en función de las distintas áreas de la Organización o entornos tecnológicos, por lo que la efectividad de cada salvaguarda se condiciona adicionalmente por su grado de implantación en el entorno analizado. La implantación de las salvaguardas se representa por un porcentaje.

La determinación del porcentaje de implantación de las salvaguardas se realiza teniendo en cuenta los siguientes criterios:

- **Calidad del diseño de la salvaguarda:** identificar si existen limitaciones en su aplicación o circunstancias en que el funcionamiento pueda no ser adecuado para el control de las amenazas.

- **Alcance de la implantación:** recursos de información cubiertos y no cubiertos por la salvaguarda.
- **Nivel de madurez de la implantación,** que define en qué medida se puede confiar en el funcionamiento adecuado de la salvaguarda según sus especificaciones. En la determinación del nivel de madurez se considera el modelo CMM (Capability Maturity Model), que define los siguientes niveles de madurez aplicables a cualquier proceso o control [SEI06] [ISACA07]:
 - **Nivel 0 (Inexistente):** La salvaguarda no se ha implantado.
 - **Nivel 1 (Inicial):** La implantación de la salvaguarda depende de la iniciativa de personas individuales, por lo que no se puede garantizar su aplicación de forma consistente ni en todos los casos.
 - **Nivel 2 (Repetible):** La salvaguarda se aplica de forma generalizada debido al conocimiento de todos los interesados de su necesidad y de su funcionamiento, pero no se ha llevado a cabo una formalización que asegure la aplicación de forma consistente ni que la aplicación de la medida se mantendrá a lo largo del tiempo al cambiar las personas responsables.
 - **Nivel 3 (Formalizado):** La aplicación de la salvaguarda está formalmente documentada en políticas, procedimientos, guías, estándares, cuadernos de carga, definiciones de puestos, etc. Esta formalización asegura que la salvaguarda se aplicará de forma generalizada y consistente y se mantendrá independientemente de las personas responsables.
 - **Nivel 4 (Gestionado):** La aplicación de la salvaguarda se monitoriza y se revisa periódicamente. Esta monitorización y revisión permite detectar cualquier desviación en la aplicación de la salvaguarda, garantizando su funcionamiento permanente.
 - **Nivel 5 (Optimizado):** La monitorización y la revisión de la salvaguarda se utiliza para introducir mejoras que permitan aumentar la eficacia a lo largo del tiempo.

6.2.2.9. Cálculo del riesgo efectivo

Se considera que el riesgo efectivo es la pérdida anual esperada considerando el efecto de las salvaguardas actualmente implantadas para proteger a los recursos de información de sus amenazas. [MAGE06]

La pérdida anual se calcula teniendo en cuenta:

- El valor de los activos de información.
- La exposición de los recursos de información a las amenazas, medida en términos de frecuencia y porcentaje de degradación.
- La eficacia de las salvaguardas para reducir la frecuencia o el impacto de las amenazas, teniendo en cuenta la medida en que están implantadas.

De acuerdo con las definiciones ya vistas en la introducción, el riesgo efectivo de los recursos de información puede definirse como:

$$\begin{aligned}
 \text{Riesgo}_B &= \\
 &= \sum_T (\text{ARO}'(T) \times \text{SLE}'(T)) = \\
 &= \sum_T \left(\left(\text{ARO}(T) \times \prod_S (1 - P(S, T, B)) \right) \times \sum_A \sum_R \text{Valor}(A, R) \times \text{Degradación}(B, R, T) \times \prod_S (1 - I(S, T, B, R)) \right)
 \end{aligned}$$

Donde:

- B representa el recurso de información a considerar
- A representa el conjunto de activos soportados por el recurso
- R representa cada uno de los requerimientos de seguridad definidos para la realización del análisis
- T representa cada una de las amenazas del recurso
- P(S, T, B) representa la probabilidad con la que la salvaguarda S podrá prevenir la realización de la amenaza T sobre el recurso B. A su vez, P(S) se calcula en función de la eficacia de la salvaguarda y de su grado de implantación:

$$P(S, T, B) = \text{Probabilidad}(S, T, B) \times \text{Implantación}(S, B)$$

- $I(S)$ representa la reducción del impacto de la amenaza T sobre el recurso B . A su vez, $I(S)$ se calcula en función de la eficacia de la salvaguarda y de su grado de implantación, para cada uno de los requerimientos de seguridad:

$$I(S, T, B, R) = \text{Reducción del impacto}(S, T, B) \times \text{Implantación}(S, B)$$

De forma análoga, y también de acuerdo con las definiciones incluidas en la introducción, el riesgo efectivo de los diferentes activos de información puede definirse como:

$$\begin{aligned} \text{Riesgo}_A &= \\ &= \sum_B \sum_T (\text{ARO}'(T) \times \text{SLE}'(T)) = \\ &= \sum_B \sum_T \left(\left(\text{ARO}(T) \times \prod_S (1 - P(S, T, B)) \right) \times \sum_R \text{Valor}(A, R) \times \text{Degradación}(B, R, T) \times \prod_S (1 - I(S, T, B, R)) \right) \end{aligned}$$

Donde:

- A representa el activo de información a considerar.
- B representa el conjunto de recursos de información que soportan a A .
- R representa cada uno de los requerimientos de seguridad definidos para la realización del análisis
- T representa cada una de las amenazas de los distintos recursos que soportan el activo de información.
- $P(S, T, B)$ representa la probabilidad con la que la salvaguarda S podrá prevenir la realización de la amenaza T sobre el recurso B . A su vez, $P(S)$ se calcula en función de la eficacia de la salvaguarda y de su grado de implantación:

$$P(S, T, B) = \text{Probabilidad}(S, T, B) \times \text{Implantación}(S, B)$$

- $I(S)$ representa la reducción del impacto de la amenaza T sobre el recurso B . A su vez, $I(S)$ se calcula en función de la eficacia de la salvaguarda y de su grado de implantación, para cada uno de los requerimientos de seguridad:

$$I(S, T, B, R) = \text{Reducción del impacto } (S, T, B) \times \text{Implantación } (S, B)$$

6.2.2.10. Gestión de riesgos

Una vez identificados y cuantificados los riesgos de seguridad se define el plan para su gestión y mitigación.

Debido a que no es posible la mitigación total de los riesgos, es necesario definir un nivel de riesgo que se considere aceptable por parte de la Organización. Esta decisión debe ser tomada por la Dirección y será el elemento determinante en la elaboración de los planes para mitigar los riesgos.

Para la definición del nivel de riesgo tolerable se utiliza el modelo ALARP (As Low As Reasonably Practicable), que define que los riesgos pueden clasificarse en tres zonas:

- **Acceptable:** El nivel de riesgo es bajo y, por tanto, no es necesario establecer salvaguardas adicionales.
- **Tolerable:** El nivel de riesgo es medio y se deberá considerar la implantación de salvaguardas para reducirlo, siguiendo criterios de coste/beneficio.
- **Inacceptable:** El nivel de riesgo es alto y se deberán considerar obligatoriamente salvaguardas adicionales para reducirlo.

La definición de los límites entre las tres zonas es responsabilidad de la Dirección de la Organización.

Teniendo en cuenta las tres zonas del modelo ALARP, para cada uno de los riesgos identificados es necesario definir una estrategia de entre las siguientes [ISC2.04] [ISACA07]:

- **Aceptación:** Se produce cuando el nivel de riesgo es inferior al nivel de riesgo tolerable, o en base a una decisión extraordinaria de la Dirección. Supone que la Organización está dispuesta a asumir el riesgo y por tanto no asumirá ningún coste para su reducción. Se puede utilizar en las zonas Aceptable y Tolerable.
- **Reducción:** Se produce cuando la Organización decide la implantación de salvaguardas adicionales para reducir un riesgo que sobrepasa el umbral de riesgo tolerable. Se puede utilizar en las zonas Tolerable e Inaceptable.
- **Traspaso:** Se produce cuando la Organización decide traspasar el riesgo a otra Entidad. Como ejemplos de traspaso del riesgo se puede citar la contratación de una póliza de seguros que cubra la contingencia del riesgo que se quiere traspasar, la contratación de un servicio que se responsabilice de la mitigación aportando garantías suficientes ya sean técnicas o económicas o la externalización de funciones. Se puede considerar en las zonas Tolerable e Inaceptable.
- **Evitación:** Se produce cuando la Organización decide eliminar de su operativa la causa del riesgo. Como ejemplos de evitación se puede citar el abandono de una determinada línea de negocio o la retirada de recursos de información no críticos. Se puede considerar en las zonas Tolerable e Inaceptable.

Para aquellos riesgos en los que la estrategia elegida haya sido la reducción del riesgo, es necesario definir un conjunto de salvaguardas que reduzcan el riesgo hasta un nivel tolerable.

Una vez seleccionadas las salvaguardas a implantar es necesario establecer una priorización, que debe realizarse teniendo en cuenta:

- Efectividad de cada salvaguarda: es conveniente implantar primero aquellas salvaguardas que proporcionen una mayor reducción del riesgo.

- Dependencias entre las salvaguardas: necesidad que un conjunto determinado de salvaguardas estén implantadas antes de implantar otra salvaguarda que las requiera.
- Disponibilidad de recursos humanos, materiales y económicos necesarios para la implantación de cada una de las salvaguardas.
- Relación con otros proyectos que puedan estar planificados o en curso por la Organización, y que puedan tener relación con la implantación de las salvaguardas.

6.2.2.11. Cálculo del riesgo residual

Se considera que el riesgo residual es la pérdida anual esperada considerando el efecto de las salvaguardas actualmente implantadas para proteger a los recursos de información de sus amenazas más las salvaguardas consideradas en el plan de acción definido.

La pérdida anual se calcula teniendo en cuenta:

- El valor de los activos de información.
- La exposición de los recursos de información a las amenazas, medida en términos de frecuencia y porcentaje de degradación.
- La eficacia de las salvaguardas implantadas o planificadas para reducir la frecuencia o el impacto de las amenazas, teniendo en cuenta el grado de implantación que tendrán tras la ejecución del plan de acción.

De acuerdo con las definiciones ya vistas en la introducción, el riesgo residual de los recursos de información puede definirse como:

$$\begin{aligned}
 \text{Riesgo}_B &= \\
 &= \sum_T (\text{ARO}'(T) \times \text{SLE}'(T)) = \\
 &= \sum_T \left(\left(\text{ARO}(T) \times \prod_S (1 - P(S, T, B)) \right) \times \sum_A \sum_R \text{Valor}(A, R) \times \text{Degradación}(B, R, T) \times \prod_S (1 - I(S, T, B, R)) \right)
 \end{aligned}$$

Donde:

- B representa el recurso de información a considerar
- A representa el conjunto de activos soportados por el recurso
- R representa cada uno de los requerimientos de seguridad definidos para la realización del análisis
- T representa cada una de las amenazas del recurso
- P(S, T, B) representa la probabilidad con la que la salvaguarda S podrá prevenir la realización de la amenaza T sobre el recurso B. A su vez, P(S) se calcula en función de la eficacia de la salvaguarda y de su grado de implantación:

$$P(S, T, B) = \text{Probabilidad}(S, T, B) \times \text{Implantación}(S, B)$$

- I(S) representa la reducción del impacto de la amenaza T sobre el recurso B. A su vez, I(S) se calcula en función de la eficacia de la salvaguarda y de su grado de implantación, para cada uno de los requerimientos de seguridad:

$$I(S, T, B, R) = \text{Reducción del impacto}(S, T, B) \times \text{Implantación}(S, B)$$

De forma análoga, y también de acuerdo con las definiciones incluidas en la introducción, el riesgo residual de los diferentes activos de información puede definirse como:

$$\text{Riesgo}_A = \sum_B \sum_T (\text{ARO}'(T) \times \text{SLE}'(T))$$

$$\text{Riesgo}_A = \sum_B \sum_T \left(\left(\text{ARO}(T) \times \prod_S (1 - P(S, T, B)) \right) \times \sum_R \text{Valor}(A, R) \times \text{Degradación}(B, R, T) \times \prod_S (1 - I(S, T, B, R)) \right)$$

Donde:

- A representa el activo de información a considerar.
- B representa el conjunto de recursos de información que soportan a A.

- R representa cada uno de los requerimientos de seguridad definidos para la realización del análisis
- T representa cada una de las amenazas de los distintos recursos que soportan el activo de información.
- $P(S, T, B)$ representa la probabilidad con la que la salvaguarda S podrá prevenir la realización de la amenaza T sobre el recurso B. A su vez, $P(S)$ se calcula en función de la eficacia de la salvaguarda y de su grado de implantación:

$$P(S, T, B) = \text{Probabilidad (S, T, B)} \times \text{Implantación (S, B)}$$

- $I(S)$ representa la reducción del impacto de la amenaza T sobre el recurso B. A su vez, $I(S)$ se calcula en función de la eficacia de la salvaguarda y de su grado de implantación, para cada uno de los requerimientos de seguridad:

$$I(S, T, B, R) = \text{Reducción del impacto (S, T, B)} \times \text{Implantación (S, B)}$$

6.3. Desarrollo de inventarios

Para facilitar la aplicación de la metodología en casos reales, se han identificado e incluido diversos inventarios de elementos. La función de estos inventarios es asegurar que todos los elementos relevantes para el análisis se tienen en consideración, de forma eficaz y eficiente.

Los inventarios incluyen no sólo la relación de elementos a considerar, sino unos valores asignados por defecto para el análisis. Estos valores por defecto facilitan la aplicación de la metodología de diversas formas:

- Pueden utilizarse directamente para la realización de un análisis de riesgos rápido a costa de perder precisión.

- Pueden utilizarse como punto de partida para un análisis individual de los diferentes elementos reales que forman parte del análisis de riesgos, permitiendo dar valores en función de la relación del elemento a analizar con un elemento tipo.
- Pueden utilizarse directamente en elementos que no sean particularmente relevantes para el análisis y como punto de partida para un análisis más detallado de los elementos más relevantes.

Los inventarios realizados se consideran genéricos y pueden adaptarse a las necesidades de diferentes análisis de riesgos, o sustituirse por otros que se adapten mejor a las necesidades específicas.

Los inventarios incluidos en la metodología son:

- Requerimientos de seguridad. Sólo contiene la lista de requerimientos de seguridad a considerar. El inventario de requerimientos de seguridad está recogido en el anexo III de este documento. [MAGE06]
- Tipos de recursos de información. Sólo contiene la lista de tipos de recursos de información a considerar. Para la elaboración de este inventario se utilizó como punto de partida el inventario proporcionado por MAGERIT, si bien fue necesario modificarlo debido a que MAGERIT no diferencia entre activos y recursos de información. El inventario de tipos de recursos de información está recogido en el anexo IV de este documento. [MAGE06]
- Amenazas. Contiene la lista de amenazas y una estimación de la frecuencia y la degradación que causa a cada tipo de recursos de información, teniendo en cuenta cada uno de los requerimientos de seguridad. Para la elaboración de este inventario se utilizó como punto de partida el inventario proporcionado por MAGERIT. El inventario de amenazas está recogido en el anexo V de este documento. [MAGE06]

- Salvaguardas. Contiene la lista de salvaguardas y una estimación de la efectividad en la reducción de la frecuencia de cada amenaza sobre cada tipo de recurso, así como la efectividad en la reducción del impacto de cada amenaza sobre cada tipo de recurso y requerimiento de seguridad. Para la elaboración de este inventario se utilizó como punto de partida el listado de controles del código de buenas prácticas ISO/IEC 27002:2005. El inventario de salvaguardas está recogido en el anexo VI de este documento, si bien, debido a su elevado volumen, no se incluye la información de la eficacia de cada salvaguarda. [ISO27002.05]

6.4. Desarrollo de plantillas

Para agilizar la recogida de la información necesaria para la realización del análisis de riesgos se ha definido un conjunto de cuestionarios tipo, que pueden adaptarse a las necesidades de distintos análisis de riesgos.

Los cuestionarios, personalizados para este análisis de riesgos pueden encontrarse en el anexo VIII de este documento.

7. FASE II: DESARROLLO DE LA HERRAMIENTA

Una vez definida la metodología a emplear, se desarrolló una herramienta informática para soportar su implantación. El desarrollo se realizó utilizando un ciclo de vida en espiral, en el que se realizaron 3 iteraciones:

- Prototipo funcional, que constaba de un modelo de datos completo y la mayor parte de las funcionalidades.
- Prototipo de demostración, que constaba de un diseño completo del interfaz de usuario, con una lógica muy limitada.
- Aplicación final.

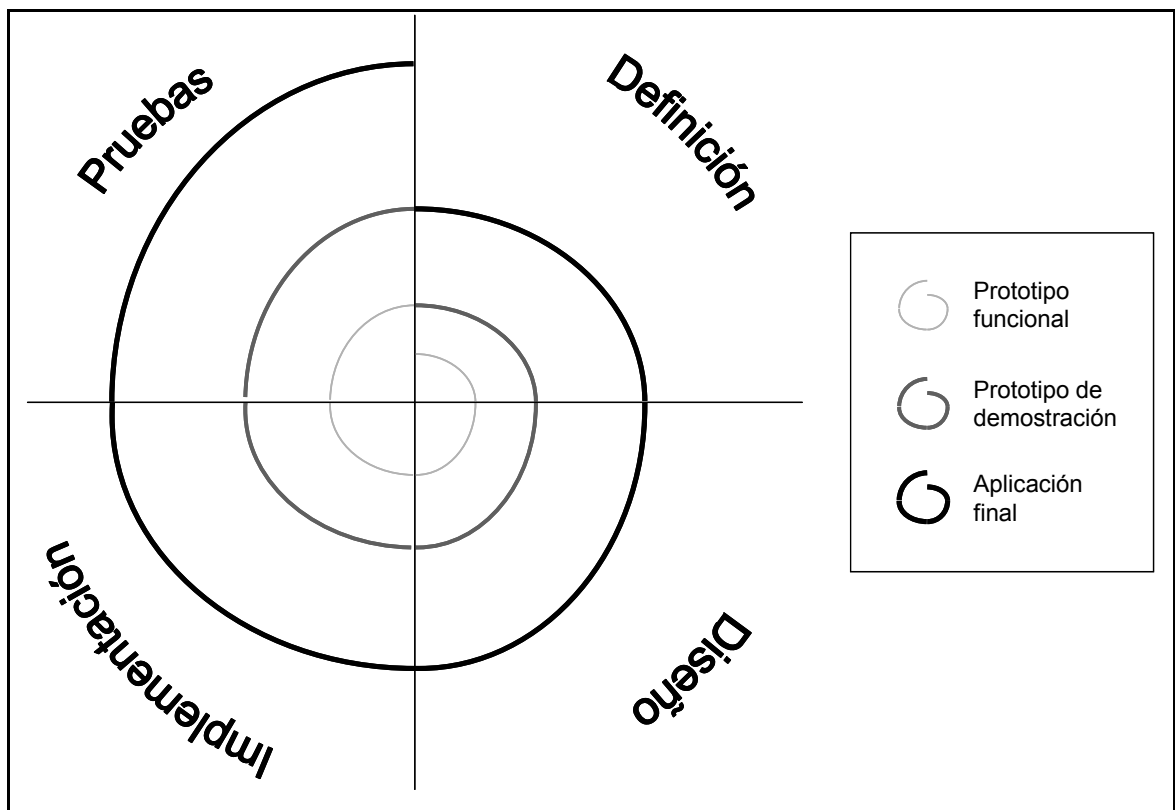


Figura 24: Ciclo de vida en espiral

7.1. Definición de requerimientos

Un extracto de los requerimientos definidos para la aplicación se muestra en el anexo VII.

7.2. Modelo de datos

El modelo de datos definido para la aplicación es el siguiente:

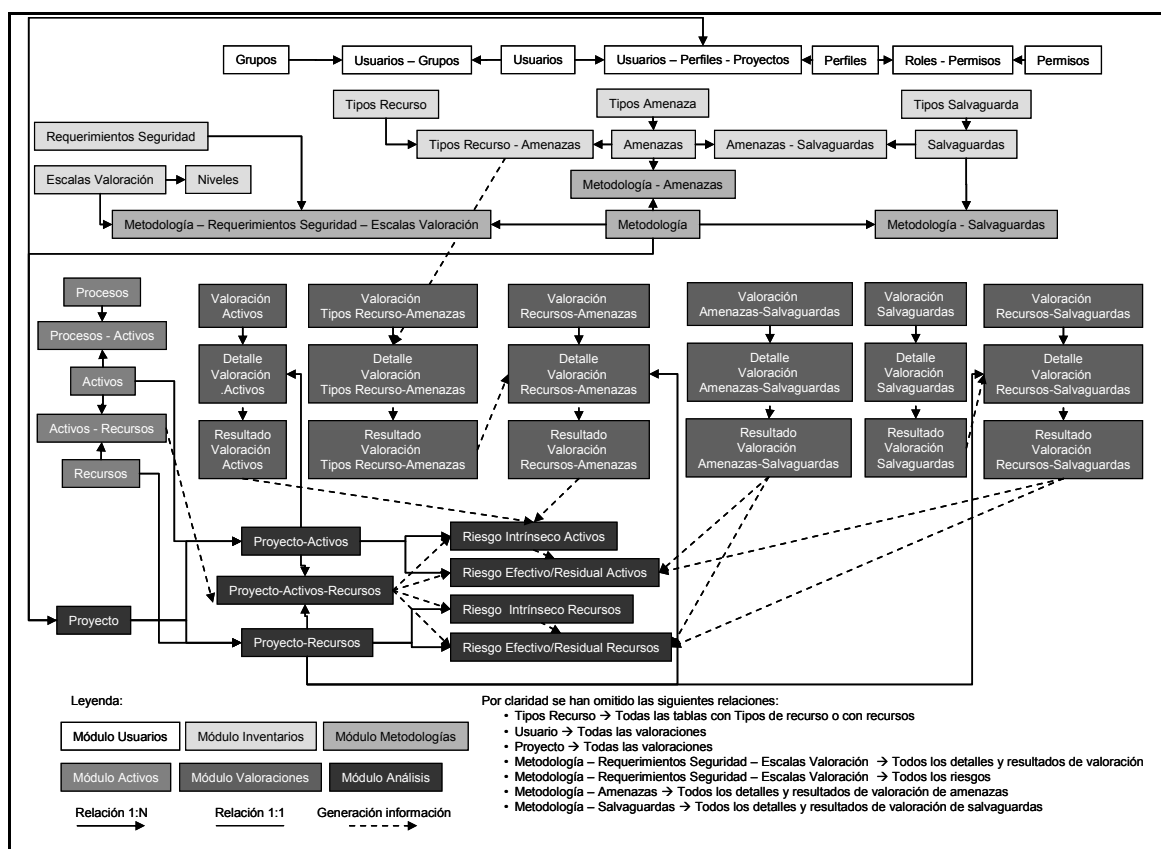


Figura 25: Modelo de datos de la aplicación

7.3. Prototipo funcional

Constó de un modelo de datos completo y la mayor parte de las funcionalidades relacionadas con el análisis de riesgos.

Se desarrolló en Microsoft Access, utilizando macros y consultas encadenadas, debido a la facilidad para introducir cambios en el modelo de datos y en la lógica, así como el conocimiento disponible sobre la herramienta en el equipo encargado del desarrollo de la metodología.

Este prototipo se desarrolló con los siguientes objetivos:

- Desarrollar y definir las funciones de cálculo de la metodología. Debido a la complejidad conceptual y computacional de algunos de los cálculos involucrados en el proceso, el prototipo facilitó el desarrollo del modelo matemático mediante el análisis del funcionamiento de las diferentes alternativas disponibles para el análisis de la metodología con un juego de datos de prueba sencillo.
- Definir el modelo de datos de la aplicación, teniendo en cuenta la información tanto de entrada como intermedia y de salida que era necesario gestionar.
- Evaluar el rendimiento de la aplicación en función de los volúmenes de información a tratar, debido a la explosión combinatoria inherente al enfoque de análisis de riesgos. Los resultados de este análisis se utilizaron en el diseño de la aplicación final, facilitando la determinación de los cálculos que debían realizarse en el momento de la introducción de los datos, aquellos que debían realizarse en el momento de presentar los resultados y aquellas tablas intermedias que era necesario almacenar para optimizar el rendimiento.
- Realizar las pruebas de la aplicación final, debido al excesivo coste de realizar los cálculos manualmente, incluso manejando conjuntos de datos de prueba sencillos.

Se pueden encontrar algunas capturas de pantalla del prototipo funcional en el Anexo VII de este documento.

7.4. Prototipo de demostración

Constó de una interfaz de usuario completa, que simulaba la realización de un caso sencillo de análisis de riesgos.

Se desarrolló en java, utilizando el compilador Eclipse, debido a que las funcionalidades de diseño de interfaces era conocido por el miembro del equipo encargado de su desarrollo.

Este prototipo se desarrolló con los siguientes objetivos:

- Identificación de requerimientos no directamente relacionados con el análisis de riesgos.
- Evaluación de aspectos ergonómicos de la aplicación, analizando la capacidad de comprender el flujo definido para el análisis de riesgos por parte de personas sin conocimientos previos de análisis de riesgos.
- Concreción del alcance y objetivos detallados del proyecto junto a los responsables de su ejecución dentro de la Organización.
- Presentación a la Dirección de la Organización de los resultados finales a obtener como resultado del proyecto.

Se pueden encontrar algunas capturas de pantalla del prototipo de demostración en el Anexo VII de este documento.

7.5. Versión final

El desarrollo de la aplicación se encargó a un desarrollador de software externo.

El desarrollo se realizó en .net sobre una base de datos Microsoft SQL Server, por los siguientes motivos:

- Conocimiento de la plataforma por parte de la Organización, para que pudiera asumir fácilmente el mantenimiento de la aplicación una vez finalizado el proyecto.

- Posibilidad de reutilizar gran parte del desarrollo en un momento posterior para desarrollar una versión web de la aplicación.

Para el desarrollo de la aplicación se proporcionó al desarrollador la siguiente documentación:

- Presentación general del proyecto.
- Documento de requerimientos.
- Prototipo técnico.
- Prototipo de demostración.
- Documentación de la metodología de análisis de riesgos.

Una vez analizada la documentación, se decidió limitar el alcance de la primera versión, teniendo en cuenta las restricciones de tiempo y presupuesto. Las funcionalidades que se modificaron fueron:

- Arquitectura web: el desarrollo se hizo en arquitectura cliente/servidor.
- Múltiples idiomas.
- Ayuda en línea.
- Importación de datos desde ficheros Microsoft Excel.
- Clonación de elementos de la base de datos.
- Gestión de usuarios simplificada.
- Simplificación de la interfaz de usuario.
- Segregación de la aplicación en dos ejecutables independientes, para asegurar el control de acceso con la nueva gestión de usuarios:
 - Aplicación del gestor de riesgos. Incluye todas las funcionalidades del gestor de riesgos: gestión de usuarios, gestión de proyectos de análisis de riesgos y obtención de resultados de los análisis.
 - Aplicación de toma de datos. Incluye la obtención selectiva de información de los diferentes usuarios de la Organización en relación a activos, recursos, amenazas y salvaguardas.
- Cálculo del riesgo residual.

- Eliminación de diversas funcionalidades menores:
 - Inventario de procesos
 - Reducción del número de informes

Los resultados presentados por el desarrollador fueron:

- Código fuente de la aplicación desarrollada con su documentación correspondiente.
- Programa instalable de la aplicación desarrollada.
- Manual técnico de la aplicación, con instrucciones para su instalación y mantenimiento.

El despliegue de la aplicación supuso los siguientes pasos principales:

- Pruebas de aceptación, que se realizaron comparando los resultados obtenidos de la aplicación con los resultados obtenidos del prototipo funciona, utilizando diversos juegos de datos:
 - Ejemplos utilizados en el desarrollo de la metodología.
 - Datos reales del análisis de riesgos.
- Instalación de la aplicación en un entorno de preproducción, para la realización de las pruebas de certificación exigidas por la Organización para todo el software de producción. Como parte de la instalación se realizó una carga inicial de datos, utilizando algunos de los casos de prueba utilizados durante el desarrollo de la aplicación.
- Desarrollo del manual de usuario de la aplicación.
- Formación a los usuarios de la aplicación.
- Pase a producción de la aplicación, incluyendo la carga inicial de datos.

Se pueden encontrar algunas capturas de pantalla de la aplicación en el Anexo VII de este documento.

8. FASE III: ANÁLISIS DE RIESGOS

8.1. Arranque del proyecto

8.1.1. Equipo de trabajo

Se constituyó el equipo de proyecto según se definió en el plan de proyecto, asignándose y comunicándose las distintas funciones, responsabilidades y tareas.

8.1.2. Definición del alcance

El alcance del análisis de riesgos vino determinado, en este caso, por el objetivo principal de servir de soporte para la implementación de un SGSI. La Organización incluyó dentro del alcance las nueve Sociedades del Grupo más relevantes en términos de volumen de negocio, beneficios y dependencia de sistemas automatizados.

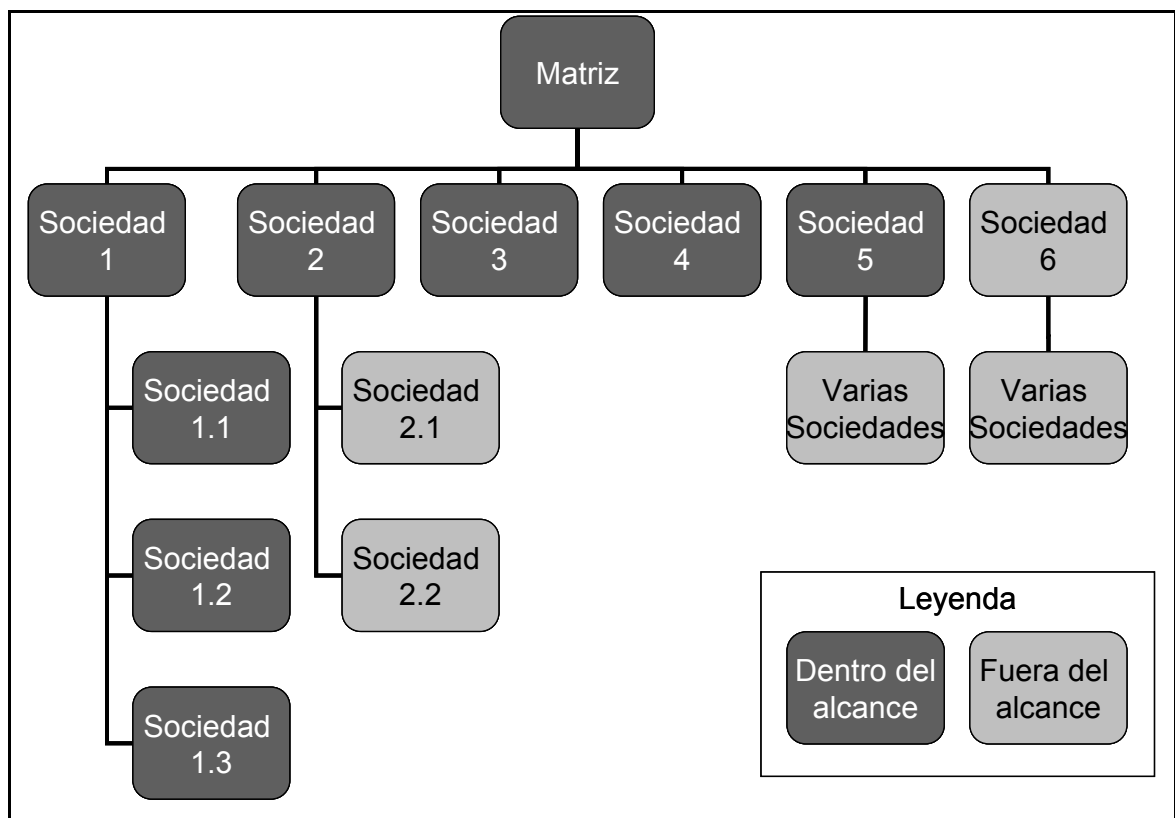


Figura 26: Estructura societaria de la Organización

Una vez definido el alcance se notificó a cada una de las Sociedades seleccionadas su inclusión dentro del alcance del análisis de riesgos. La Dirección de las distintas Sociedades definió un coordinador encargado de proporcionar la documentación y la colaboración del personal necesarios para el desarrollo del proyecto.

Con cada uno de los coordinadores se fijó un calendario, teniendo en cuenta los distintos proyectos y cargas de trabajo de cada una de las Sociedades, siempre respetando los hitos fijados para el proyecto de implantación del SGSI.

El resultado de la definición del alcance fue un calendario de trabajo acordado por todos los intervinientes para la realización del proyecto.

8.1.3. Adaptación de la metodología

La metodología definida en la Fase II del proyecto se definió para ser adaptable a diferentes circunstancias y tipos de proyecto, por lo que fue necesario fijar los parámetros para adaptarla al análisis requerido para soportar el SGSI.

Para el análisis de riesgos a realizar en este proyecto se definieron las siguientes características para el análisis de riesgos:

- Requerimientos de seguridad de los activos de información:
 - Confidencialidad
 - Integridad
 - Disponibilidad
 - Autenticidad
 - Trazabilidad
- Escala de valoración de los requerimientos de seguridad:
 - 5 niveles (ver descripción en el anexo III de este documento)
- Inventario de tipos de recursos de información:
 - Adaptado del inventario de tipos de activos de información de MAGERIT (ver detalle en el anexo IV de este documento)

- Inventario de amenazas:
 - Adaptado del inventario de amenazas de MAGERIT (ver detalle en el anexo V de este documento)
- Inventario de salvaguardas:
 - Controles del código de buenas prácticas ISO/IEC 27002 (ver detalle en el anexo VI de este documento)

Debido a que se utilizaron los inventarios básicos definidos en la metodología no fue necesario parametrizar las relaciones genéricas entre los distintos elementos del modelo:

- Tipos de activo – Amenazas, en la que se parametriza la frecuencia y la degradación de cada una de las amenazas sobre cada tipo de activo.
- Tipos de activo – Amenazas – Salvaguardas, en la que se parametriza la reducción de la frecuencia y la degradación de cada amenaza sobre cada tipo de activo, por la acción de cada salvaguarda.

8.2. Obtención de información

8.2.1. Preparación de cuestionarios

Se definió un conjunto de cuestionarios que permitiera hacer la toma de datos más eficaz, eficiente y homogénea. En la elaboración de los cuestionarios se tuvo en cuenta tanto las necesidades de información de la metodología como las adaptaciones particulares realizadas en ella.

En particular se prepararon los siguientes tres cuestionarios:

- **Presentación del proyecto y solicitud inicial de colaboración.**
Este cuestionario se dirigió al coordinador de las distintas Sociedades que formaron parte del alcance. Su objetivo fue confirmar, consolidar y ampliar la información previa que habían recibido sobre el proyecto, informar sobre los aspectos generales de la metodología a utilizar y realizar una primera solicitud de documentación para preparar la reunión de arranque del proyecto para la Sociedad. El enfoque para la solicitud de la información fue de máximos, es decir, se solicitó toda la información cuyo análisis se consideró que se consideró que podría agilizar el proceso, si bien ninguno de los documentos solicitados era de presentación obligatoria, en caso de que la Sociedad no dispusiera de ellos. El formato utilizado fue correo electrónico.
- **Cuestionario de identificación y valoración de activos de información**
Este cuestionario se dirigió a los miembros de la Dirección de cada Sociedad llamados a participar en el proyecto. Su objetivo fue identificar los diferentes activos de información relevantes en los distintos procesos de negocio y de soporte. Los coordinadores de las distintas Sociedades se encargaron de enviarlo con anterioridad a las reuniones, si bien su principal utilidad fue facilitar la reunión de obtención de información con los interlocutores.
- **Cuestionario de identificación de recursos de información**
Este cuestionario se dirigió al personal de Sistemas de Información llamado a participar en el proyecto. Su objetivo fue identificar los recursos de información que soportaban los activos de información identificados en el cuestionario anterior. Los coordinadores de las distintas Sociedades se encargaron de enviarlo con anterioridad a las reuniones, si bien su principal utilidad fue facilitar la reunión de obtención de información con los interlocutores.

- Cuestionario de identificación de recursos de información

Este cuestionario se dirigió al Responsable de Seguridad de cada Sociedad. Su objetivo fue valorar el grado de implantación de los diferentes controles definidos en el código de buenas prácticas ISO/IEC 27002:2005 en cada una de las Sociedades. Debido al enfoque utilizado, no se detalló el grado de implantación a nivel de activos ni recursos individuales, sino el grado de implantación general en la Sociedad. Los coordinadores de las distintas Sociedades se encargaron de enviarlo con anterioridad a las reuniones, si bien su principal utilidad fue facilitar la reunión de obtención de información con los interlocutores.

Se utilizaron como punto de partida las plantillas definidas en la propia metodología.

Los cuestionarios desarrollados pueden encontrarse en el anexo VIII de este documento.

8.2.2. Solicitud inicial de colaboración

Se envió a los coordinadores de las distintas Sociedades incluidas en el alcance del proyecto el cuestionario de presentación del proyecto y solicitud inicial de colaboración (Ver anexo VIII).

Como respuesta a este cuestionario algunos coordinadores solicitaron información adicional sobre el proyecto y sus requerimientos.

Como respuesta a este cuestionario algunos coordinadores enviaron anticipadamente parte de la documentación solicitada.

8.2.3. Reunión de arranque

Para cada Sociedad dentro del alcance se mantuvo una reunión de arranque con el coordinador asignado.

Algunos coordinadores enviaron anticipadamente parte de la documentación solicitada. Esa documentación fue analizada como parte de la preparación de la reunión de arranque, y permitió que la reunión fuera más eficaz y eficiente.

Los objetivos planteados para la reunión fueron los siguientes:

- Incidir en los aspectos más importantes del proyecto y solucionar las dudas de los coordinadores, referentes al propio proyecto, a la metodología o a la colaboración solicitada.
- Revisar la documentación entregada, pendiente de entregar y no existente.
- Identificar los interlocutores necesarios para completar la información no disponible en documentos y para completar y aclarar la información presente en documentos.
- Realizar un análisis de alto nivel de los distintos procesos de negocio y de soporte, diferenciando aquellos procesos críticos para la Sociedad de los procesos menos importantes, y los procesos que requieren y procesan grandes volúmenes de información de los procesos que no utilizan información relevante.
- Decidir, para cada proceso, si se debe incluir o no en el análisis de riesgos.
- Identificar los interlocutores que tienen responsabilidad y/o conocimiento de los procesos seleccionados para realizar el análisis, para que el coordinador pueda preparar un programa de trabajo detallado teniendo en cuenta la colaboración necesaria de cada uno de ellos.
- Identificar los interlocutores de las áreas de Sistemas de Información que pueden proporcionar información sobre los recursos de información que soportan los activos de información de la Sociedad.
- Identificar al Responsable de Seguridad de la Sociedad para que colabore en la valoración de las salvaguardas establecidas.

8.2.4. Análisis de documentación

El objetivo principal del análisis de la documentación fue proporcionar al equipo de análisis de riesgos un conocimiento suficiente del entorno, situación y organización de cada Sociedad, para aumentar su eficacia y eficiencia en la ejecución de las tareas. En particular, el hecho de que el equipo de análisis de riesgos disponga de este conocimiento agiliza las reuniones con los distintos interlocutores, dado que no es necesario realizar una introducción inicial de los principales aspectos de la Organización.

La documentación de cada Sociedad recibida por el equipo de análisis de riesgos fue analizada y formalizada en los cuestionarios desarrollados. Si bien la función del equipo no consistía en realizar la identificación y la valoración de los elementos, la realización de este ejercicio presentaba un conjunto de ventajas importante:

- Facilitar la comprensión de la documentación heterogénea recibida por el equipo de análisis de riesgos, al formalizarse toda en un formato común que contenía toda la información necesaria para la realización del análisis.
- Facilitar la comunicación con los interlocutores, al poder mantenerse parte de la reunión con cuestiones cerradas, en lugar de con cuestiones abiertas. Las cuestiones abiertas fueron necesarias sólo para completar la información no cubierta por la documentación recibida.

La documentación solicitada a las Sociedades para su revisión por parte del equipo de análisis de riesgos fue la siguiente, teniendo en cuenta que no se consideró la lista exhaustiva, ni toda la información estuvo disponible en todas las Sociedades:

- Documentación de negocio:
 - Mapa de procesos
 - Organigrama
 - Relación de puestos de trabajo
 - Documentación de procesos y procedimientos

- Cartas o catálogos de servicios (parte de esta información la obtuvo el equipo de análisis de riesgos a través de las páginas web de las distintas Sociedades)
- Inventario de servicios subcontratados
- Manuales de gestión (por ejemplo, los desarrollados para cumplir con estándares de calidad como el ISO 9001)
- Resultados de auditorías
- Análisis de riesgos de negocio realizados con anterioridad (por ejemplo los realizados como parte del cumplimiento de códigos de buen gobierno).
- Documentación técnica:
 - Mapa de aplicaciones
 - Inventario de aplicaciones
 - Documentación funcional de aplicaciones (documentación de requerimientos y análisis funcional)
 - Mapa de sistemas y comunicaciones
 - Inventario de sistemas
 - Manuales de gestión (por ejemplo, los desarrollados para cumplir con estándares de calidad como el ISO 9001)
 - Planes de Continuidad de Negocio y/o Planes de Recuperación de Desastres (en particular el Análisis de Impacto sobre el Negocio)
 - Inventario de ficheros declarados a la Agencia de Protección de Datos en cumplimiento de la LOPD
 - Documento de seguridad de la LOPD
 - Resultados de auditorías técnicas
 - Cuadros de mandos y listas de comprobación de seguridad
 - Análisis de riesgos realizados con anterioridad

8.2.5. Entrevistas con interlocutores

El contenido de las entrevistas mantenidas con los diferentes intervinientes de las Sociedades fue el siguiente:

- Breve presentación del proyecto de análisis de riesgos al interlocutor, para asegurar que conoce el contexto en el que se solicita su colaboración y para poder responder cualquier duda.
- Análisis de los procesos de negocio y de soporte conocidos por el interlocutor, revisando sus clasificaciones como relevantes o no relevantes de cara al análisis de riesgos. La principal información a obtener fue:
 - Objetivo del proceso
 - Subprocesos, tareas y actividades principales del proceso
 - Identificar quién asume las principales funciones y responsabilidades del proceso, teniendo en cuenta el Modelo RACI:
 - R → Realiza
 - A → Responsables
 - C → Colabora
 - I → Es informado
- Identificación y valoración de los activos de información relevantes de cada proceso incluido dentro del alcance del análisis, tomando como punto de partida la información preparada por el equipo de análisis de riesgos con la documentación recibida y el cuestionario cumplimentado previamente por el interlocutor (en caso de haberlo hecho). La principal información a recabar de los activos de información es:
 - Nombre y descripción del activo de información.
 - Uso del activo de información en el contexto de la ejecución del proceso.
 - Valoración de los requerimientos de seguridad del activo de información.

- Identificación de los recursos que soportan los diferentes activos de información, y sus responsables. Para facilitar la identificación de todos los recursos relevantes se tuvieron en cuenta los diferentes tipos de procesamiento:
 - Obtención de la información.
 - Almacenamiento de la información.
 - Tratamiento de la información.
 - Salida de información.
- Identificación de las salvaguardas e incidentes de seguridad conocidos por el interlocutor.

Como acta de las reuniones mantenidas se envió a cada interlocutor el cuestionario final cumplimentado durante la revisión, para su aprobación. El análisis de riesgos se realizó con la información contenida en dichos cuestionarios aprobados por los intervinientes.

8.3. Análisis de riesgos

8.3.1. Cálculo del riesgo intrínseco

El cálculo del riesgo intrínseco para cada una de las Sociedades se realizó introduciendo en la herramienta desarrollada en la Fase II la información de los cuestionarios aprobados por los distintos interlocutores referentes a los activos de información, recursos de información y amenazas.

La introducción de los datos en la herramienta lo realizaron directamente los interlocutores debido a que habría requerido un esfuerzo importante de formación en el uso de la misma, así como habría supuesto potenciales retrasos en el proyecto en caso de que algún interlocutor no hubiera cumplido los plazos establecidos.

8.3.2. Cálculo del riesgo efectivo

El cálculo del riesgo efectivo para cada una de las Sociedades se realizó introduciendo en la herramienta desarrollada en la Fase II la información de los cuestionarios aprobados por los distintos interlocutores referente a las salvaguardas, que se añadió a la información sobre los activos de información, recursos de información y amenazas que ya se habían cargado anteriormente.

La introducción de los datos en la herramienta lo realizaron directamente los interlocutores debido a que habría requerido un esfuerzo importante de formación en el uso de la misma, así como habría supuesto potenciales retrasos en el proyecto en caso de que algún interlocutor no hubiera cumplido los plazos establecidos.

8.4. *Presentación de resultados*

Los resultados presentados por la herramienta desarrollada en la Fase II del proyecto fueron:

- **Mapa de riesgos intrínsecos:** Tabla con el riesgo intrínseco de cada activo de información, teniendo en cuenta los diferentes requerimientos de seguridad.
- Diagrama de barras con el riesgo intrínseco de cada activo de información, teniendo en cuenta los diferentes requerimientos de seguridad.
- **Mapa de riesgos efectivos:** Tabla con el riesgo efectivo de cada activo de información, teniendo en cuenta los diferentes requerimientos de seguridad.
- Diagrama de barras con el riesgo efectivo de cada activo de información, teniendo en cuenta los diferentes requerimientos de seguridad.

Alrededor de la información suministrada por la herramienta se realizó un breve informe donde se detallaba:

- Descripción general del estado de riesgo de la Sociedad.
- Descripción de los principales activos de información a proteger y los principales recursos de información que los soportan.
- Descripción de los mayores riesgos efectivos que deben ser atendidos por la Sociedad.

Adicionalmente se generó un informe consolidado con la información de todas las Sociedades dentro del alcance. Este informe contenía:

- Información de riesgos de todas las Sociedades obtenida de la herramienta.
- Comparativa del nivel de riesgo total de cada Sociedad, teniendo en cuenta los diferentes requerimientos de seguridad.
- Descripción de los mayores riesgos efectivos que deben ser atendidos a nivel Organización, obtenidos a partir de los mayores riesgos efectivos de las distintas Sociedades.

9. FASE IV: GESTIÓN DE RIESGOS

9.1. *Definición de umbrales*

En base a los informes obtenidos en la fase anterior, se definieron dos umbrales de riesgo a nivel de Sociedad:

- **Umbral de riesgo aceptable:** nivel de riesgo a partir del cual la Sociedad considera innecesario realizar inversiones adicionales para su mitigación.
- **Umbral de riesgo inaceptable:** nivel de riesgo a partir del cual la Sociedad debe obligatoriamente tomar medidas mitigantes.

Los umbrales se consideraron teniendo en cuenta el volumen de riesgos en cada categoría, de modo que la dimensión de los trabajos a realizar fuera manejable.

El Responsable de Gestión de Riesgos de la Organización aprobó los umbrales definidos y los comunicó a la Dirección de la Organización.

9.2. *Identificación de riesgos no cubiertos*

Una vez definidos los umbrales de riesgos, se realizó un análisis de los riesgos que no habían quedado automáticamente aceptados, para los que era necesario definir una estrategia:

- Aceptación
- Mitigación
- Transferencia
- Evitación

Las estrategias de transferencia y evitación no se seleccionaron para ninguno de los riesgos.

9.3. *Elaboración del plan de acción*

El plan de acción se desarrolló teniendo en cuenta los riesgos para los que se seleccionó una estrategia de mitigación.

9.3.1. Selección de salvaguardas

Para cada uno de los riesgos se realizó un análisis para determinar la mejor estrategia de mitigación entre las siguientes:

- Fortalecer salvaguardas ya implantadas.
- Establecer nuevas salvaguardas.
- Fortalecer salvaguardas existentes y establecer otras nuevas.

Para aquellos riesgos cuya mitigación requirió la implantación de nuevas salvaguardas se definieron las nuevas salvaguardas a implantar, teniendo en cuenta:

- Capacidad de la salvaguarda para mitigar el riesgo correspondiente y otros riesgos afines.
- Experiencia existente en la Organización para la implantación de dichas salvaguardas. Por ejemplo, si alguna otra Sociedad de la Organización tenía experiencia en ellas.
- Acuerdos con proveedores existentes a nivel Organización.
- Relaciones entre salvaguardas. Por ejemplo, posibilidad de adquirir módulos adicionales de productos de seguridad ya implantados en la Sociedad.
- Dificultad y coste para implantar y mantener cada salvaguarda teniendo en cuenta el entorno y las circunstancias de la Sociedad.
- Otros proyectos en curso o previstos por la Sociedad que pudieran influir en la conveniencia de implantar determinadas salvaguardas. Por ejemplo, conveniencia de implantar medidas relevantes de seguridad en el ciclo de vida de desarrollo si está previsto actualizar los sistemas principales de una Sociedad próximamente.

9.3.2. Cálculo del riesgo residual

Una vez seleccionadas las salvaguardas a implantar, se introdujeron en la herramienta para verificar su impacto en el mapa de riesgos.

La selección de salvaguardas y el cálculo del riesgo residual se realizaron de forma iterativa hasta alcanzar un compromiso adecuado entre un volumen de medidas a implantar asumible por la Sociedad y una adecuada mitigación del riesgo.

9.3.3. Definición de proyectos

Con el inventario de salvaguardas a implantar, se definió un conjunto de proyectos. Cada proyecto se diseñó para lograr la implantación de un conjunto de salvaguardas afines. La agrupación de salvaguardas en proyectos se realizó teniendo en cuenta los siguientes criterios:

- La consecución de objetivos afines o similares. Por ejemplo, la adecuación a una normativa, como la LOPD, supondrá la implantación de controles de distinta naturaleza, pero se puede acometer como un proyecto individual puesto que existe un objetivo común.
- La consideración de los mismos entornos tecnológicos. Por ejemplo, se puede plantear un proyecto de fortificación de la plataforma Unix, que supondrá la implantación de controles de distinta naturaleza.
- La necesidad de involucrar a un conjunto determinado de personas o de áreas de la Organización. Por ejemplo, se puede plantear un proyecto de concienciación a los usuarios en materia de seguridad de la información, que supondrá la implantación de diferentes medidas con una participación importante del Departamento de Recursos Humanos. Otro ejemplo podría ser el cumplimiento normativo, que en colaboración con el Departamento de Asesoría Jurídica podría tratar temas tan dispares como la LOPD, LSSI, LISI, Firma electrónica y Facturación electrónica.

- La existencia de proveedores o herramientas que ofrezcan un servicio integrado. Por ejemplo, la implantación de un software de gestión de red puede utilizarse para el mantenimiento del inventario de sistemas, para la detección de la instalación de software no autorizado en los equipos y como un sistema de detección o prevención de intrusiones (IDS/IPS).

El contenido de cada plan de proyecto fue:

- Introducción. Incluyó una referencia al proyecto del análisis de riesgos y a sus resultados, para permitir que el documento fuera autocontenido, es decir, que no requiriera de documentos adicionales del análisis de riesgos para su comprensión por un lector objetivo.
- Objetivo: conjunto de salvaguardas a implantar.
- Alcance: definición del entorno de la Sociedad donde se van a implantar las distintas salvaguardas, y el nivel de implantación que se quiere alcanzar con cada una de ellas.
- Enfoque: principales tareas y actividades que deben formar parte del proyecto.
- Relaciones con otros proyectos:
 - Identificación de los proyectos o tareas que deben haberse finalizado antes del inicio del proyecto o de alguna de sus fases.
 - Identificación de los proyectos que dependen de la finalización de este proyecto o de alguna de sus fases o tareas.
- Responsabilidades: asignación de funciones y responsabilidades para el proyecto. La asignación formal de tareas permite ganar eficiencia en el trabajo, al no realizarse tareas repetidas ni quedar tareas sin hacer. También permiten detectar y corregir desviaciones en el cumplimiento de los objetivos individuales.

Para la asignación de responsabilidades se tuvo en cuenta el Modelo RACI:

- R → Realiza
- A → Responsables
- C → Colabora
- I → Es informado
- Presupuesto: estimación de los recursos necesarios para la ejecución del proyecto, teniendo en cuenta:
 - Costes de implantación:
 - Hardware
 - Software
 - Servicios
 - Personal interno
 - Costes de mantenimiento:
 - Hardware
 - Software
 - Servicios
 - Personal interno
 - Costes indirectos como costes de formación, impacto sobre los recursos utilizados por otros procesos, etc.
- Plazo de ejecución: tiempo necesario para la ejecución del proyecto y principales hitos intermedios.

A continuación se incluye una plantilla resumen para los planes de proyecto:

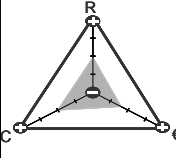
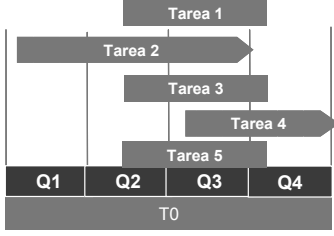
INTRODUCCIÓN Y ANTECEDENTES		DESCRIPCIÓN	RESPONSABILIDADES	
			Responsable	
			Encargado	
			Consultado	
			Informado	
OBJETIVOS	DEPENDENCIAS	PRESUPUESTO		
			IMPLANTACIÓN	MANTENIMIENTO
ALCANCE- ÁMBITO DE APLICACIÓN	FACTORES CLAVE DE ÉXITO	Hardware	0 €	0 €
		Software	0 €	
		Servicios	0 €	
		FTE	0	
		TOTAL	0 €	135.000€
ANÁLISIS CUALITATIVO	ESTRATEGIA DE EJECUCIÓN Y DESPLIEGUE		PLANIFICACIÓN	
				

Figura 27: Plantilla resumen de plan de proyecto

9.3.4. Definición de planes de acción

Una vez definidos los distintos planes de proyecto se realizó una priorización entre ellos, para regir el orden y los plazos en que deben ser acometidos por la Sociedad. Como resultado de esta actividad, cada Sociedad tuvo un plan de acción consolidado.

Los principales aspectos a considerar para la priorización son:

- Mitigación del riesgo: los proyectos que mitigan el riesgo en mayor medida deben ejecutarse lo antes posible.
 - Relaciones de dependencia entre los proyectos. Para la implantación de determinados proyectos puede ser deseable o incluso necesario haber finalizado otros proyectos previamente. Por ejemplo, un proyecto de segmentación de redes puede facilitar la implantación de un sistema de detección o prevención de intrusiones (IDS/IPS). Un aspecto interesante a tener en cuenta para la priorización es la madurez de los procesos, que define cinco niveles de madurez aplicables a cualquier proceso y establece las acciones necesarias para aumentar su madurez de forma eficaz y eficiente. Un modelo relevante a tener en cuenta al establecer relaciones entre los diferentes proyectos es el CMM, que considera necesario consolidar un determinado nivel de madurez para acometer con garantías el paso al siguiente. Por tanto, es necesario acometer primero los proyectos que permitan alcanzar niveles más bajos de madurez, acometiendo posteriormente los siguientes niveles.
- Relación con otros proyectos en curso o previstos por la Sociedad, de modo que se puedan aprovechar sinergias. Por ejemplo, el desarrollo del Plan de Continuidad de Negocio o el Plan de Contingencias teniendo en cuenta la construcción un segundo edificio de oficinas que pueda albergar el CPD de respaldo.
- Requerimientos de recursos y presupuesto de los distintos proyectos, de modo que no haya en ningún momento unos requerimientos excesivos que la Sociedad no pueda cumplir, tanto para tareas de implantación como de mantenimiento.

A continuación se incluye una plantilla de calendario de plan de acción:

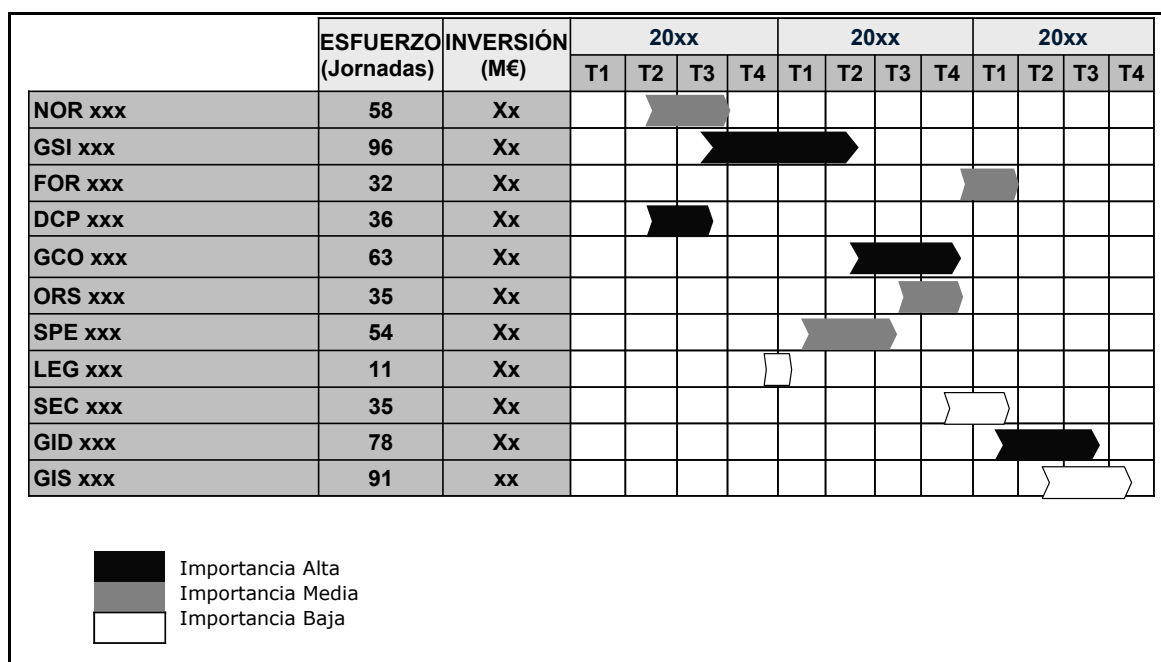


Figura 28: Plan de acción - Calendario

9.3.5. Definición del plan de acción consolidado

Una vez definidos los planes de acción por Sociedad se definió un plan de acción consolidado de todos ellos. Este plan consolidado se definió con varios fines:

- Identificar sinergias entre los proyectos definidos para distintas Sociedades, de modo que la implantación sea más eficaz y/o eficiente.
- Proporcionar una visión global del plan de acción útil para realizar el seguimiento de las tareas previstas.

La definición del plan de acción consolidado realimentó a los planes individuales, de modo que se hicieron varias iteraciones alcanzar una solución adecuada para todas las Sociedades.

9.4. *Aprobación del plan de acción*

Una vez preparados los planes de acción, el Responsable de Gestión de Riesgos de la Organización los presentó a las respectivas Direcciones para su aprobación, y para la obtención de la financiación y los recursos necesarios para su ejecución.

Asimismo, el Responsable de Gestión de Riesgos de la Organización presentó el plan consolidado a la Dirección de la Organización para su revisión y aprobación.

10. CONTROL Y GESTIÓN DEL PROYECTO

Para asegurar el cumplimiento de los objetivos del proyecto, controlar el cumplimiento de los hitos y plazos planificados y detectar y solucionar convenientemente y a tiempo todos los problemas, se mantuvieron reuniones periódicas de control y gestión del proyecto, según se describe a continuación.

10.1. *Reunión de arranque del proyecto*

El objetivo de la reunión de arranque fue formalizar el inicio del proyecto y establecer la organización para un desarrollo adecuado de todas las tareas.

- Asistentes:
 - Responsable de Gestión del Riesgo Tecnológico de la Organización
 - Equipo de trabajo
- Orden del día:
 - Presentación del proyecto: objetivos, alcance y entregables.
 - Presentación del equipo de trabajo y funciones asignadas.
 - Presentación de la metodología y las herramientas a utilizar.
 - Revisión de la planificación detallada del proyecto.
 - Definición de los mecanismos de comunicación, control y seguimiento del proyecto.
 - Solicitud inicial de información:
 - Estructura societaria.
 - Organigrama de cada Sociedad.
 - Información general de cada Sociedad: fines, principales procesos, infraestructura tecnológica, etc.
 - Coordinación de aspectos logísticos:
 - Material de trabajo
 - Ubicación del equipo de trabajo
 - Permisos de acceso a edificios y a sistemas de información
 - Revisión detallada de las primeras tareas a realizar.

10.2. Reuniones de seguimiento del proyecto

El objetivo de las reuniones semanales de seguimiento era verificar el desarrollo normal del plan de trabajo y cumplimiento de los objetivos establecidos, así como detectar y actuar ante los riesgos y dificultades encontrados en la ejecución de las tareas.

- Asistentes:
 - Responsable de Gestión del Riesgo Tecnológico de la Organización
 - Responsables del equipo de trabajo
- Tareas finalizadas:
 - Nombre de la tarea
 - Responsable
 - Fecha finalización
 - Fecha planificada de finalización
- Tareas en curso:
 - Nombre de la tarea
 - Responsable
 - % de avance
 - Fecha planificada de arranque
 - Fecha real de arranque
 - Fecha planificada de finalización
 - Fecha prevista de finalización
 - ¿Está en el camino crítico del proyecto?
 - Dificultades encontradas y acciones correctivas
 - Riesgos previstos y acciones mitigantes
- Tareas planificadas:
 - Nombre de la tarea
 - Responsable
 - Fecha planificada de inicio
 - Fecha prevista de inicio
 - ¿Está en el camino crítico del proyecto?
 - Riesgos previstos y acciones mitigantes

10.3. Reunión de cierre del proyecto

El objetivo de la reunión de cierre del proyecto fue realizar la entrega formal de los resultados del proyecto y verificar el cumplimiento de los objetivos definidos.

- Asistentes:
 - Responsable de Gestión del Riesgo Tecnológico de la Organización
 - Equipo de trabajo
- Orden del día:
 - Entrega formal de los resultados del proyecto
 - Evaluación del cumplimiento de los objetivos del proyecto
 - Valoración de los siguientes pasos
 - Cierre formal del proyecto

11. LÍNEAS FUTURAS DE TRABAJO

Una vez finalizado el análisis de riesgos se considera necesario acometer diferentes líneas de trabajo que permitan obtener un máximo aprovechamiento del ejercicio realizado. Las principales líneas de trabajo identificadas se describen en los siguientes apartados.

11.1. Realización de pruebas

El análisis de riesgos se realiza a partir del inventario de activos de información, recursos de información, amenazas y salvaguardas, teniendo en cuenta la información de que dispone la Organización.

Para dar validez al análisis realizado es conveniente realizar una selección de las salvaguardas más relevantes y verificar que su grado de implantación y su eficacia se corresponden con las registradas.

En función de las salvaguardas seleccionadas se pueden realizar distintos tipos de prueba:

- **Pruebas de caja negra:** Son pruebas técnicas en las que se simula la realización de un ataque por parte de un atacante que no dispone de información sobre la infraestructura tecnológica de la Organización. Pueden realizarse desde el interior, simulando las potenciales actividades de un empleado que intente cometer fraude o desde el exterior, simulando las potenciales actividades de un atacante externo a la Organización.
- **Pruebas de caja blanca:** Son pruebas técnicas en las que se verifica la configuración real de los sistemas de información en referencia a las guías o estándares de configuración publicados por la Organización, por los fabricantes o por distintas organizaciones independientes.

- **Pruebas de procedimiento:** Son pruebas destinadas a conocer el grado de cumplimiento de los procedimientos establecidos por parte de los encargados de la ejecución de los diferentes controles. Generalmente se basan en la verificación del cumplimiento de las especificaciones del control para una selección de los casos planteados durante un periodo de tiempo definido.
- **Pruebas sustantivas:** Son pruebas destinadas a conocer el grado de cumplimiento de una determinada propiedad en los miembros de una determinada población, mediante el análisis de la población completa o de una muestra representativa.

Para ilustrar la diferencia entre los distintos enfoques propuestos, se puede tomar como ejemplo la verificación de los controles de autenticación y control de acceso de usuarios a aplicaciones:

- Una prueba de caja negra se realizaría intentando obtener la contraseña realizando ataques de fuerza bruta (probar todas las contraseñas de un espacio determinado), de diccionario (probar palabras existentes en diccionarios o similares al identificador de usuario), o utilizando vulnerabilidades conocidas del sistema operativo.
- Una prueba de caja blanca se realizaría verificando la configuración de las contraseñas en el sistema operativo y comparándola con las recomendaciones publicadas por el fabricante o por organizaciones independientes, como el NIST o la ISACA.
- Una prueba de procedimiento se realizaría verificando el funcionamiento de los mecanismos de solicitud, aprobación, distribución o reactivación de contraseñas, teniendo en cuenta, por ejemplo, que los formularios de solicitud están convenientemente cumplimentados y archivados.
- Una prueba sustantiva supondría obtener el listado completo de usuarios y verificar, para todos ellos, o para una muestra significativa de ellos, si los permisos concedidos son acordes con las necesidades.

Estos diferentes enfoques no son excluyentes, pudiéndose combinar dos o más para verificar el funcionamiento de cualquiera de los controles especificados.

11.2. *Análisis continuo de riesgos*

La exposición al riesgo cambia con la evolución de la Organización y de su entorno. Por eso, es necesario establecer los mecanismos necesarios para que el esfuerzo empleado en la realización del análisis de riesgos no quede obsoleto en un periodo breve de tiempo.

Algunos de los cambios que afectan a la exposición al riesgo, y que por tanto es necesario seguir de manera continua son los siguientes:

- **Cambios en la Organización.** Las organizaciones son dinámicas, tratando de adecuarse permanentemente a su entorno para incrementar su eficacia y su eficiencia. Los cambios, tanto en la estructura como en la estrategia y los objetivos de la Organización pueden afectar de forma directa al análisis de riesgos realizado de múltiples formas: aumento o disminución de activos y recursos de información, cambios en la valoración de los activos de información, aparición o desaparición de amenazas internas, cambios en el perfil de riesgo, cambios en las estrategias de gestión del riesgo, etc.
- **Cambios en el entorno.** El entorno de las organizaciones también evoluciona con el tiempo, por lo que el análisis de riesgos debe tenerlo en cuenta para no perder su validez. Algunos de los cambios en el entorno que puedan afectar al análisis de riesgos son: aparición de nuevas amenazas, cambios legislativos o regulatorios, cambios en la competencia que pueden afectar a la valoración de los activos de información, cambios en la eficacia de las salvaguardas ante la evolución de las amenazas, etc.

Para realizar el análisis de riesgo continuo es posible establecer distintos tipos de mecanismos, que pueden estar relacionados entre sí. Algunos de los principales mecanismos para ello son:

- **Establecimiento de procedimientos de mantenimiento del análisis de riesgos.** Muchos de los cambios que se producen en las organizaciones, tanto en las áreas de negocio y soporte como en las áreas de TI, se realizan utilizando determinados procesos de gestión del cambio. Como parte constituyente de estos procesos de gestión de cambios debe incluirse la actualización del análisis de riesgos, de modo que el análisis de riesgos pueda evolucionar en paralelo a la Organización. Asimismo, deben establecerse procedimientos que actualicen el análisis de riesgos a partir de la información del entorno que la Organización reciba por distintas vías: informes sectoriales, informes de mercado, Sistemas de Información de Gestión empleados para la toma de decisiones, etc. De esta forma, el análisis de riesgos podrá evolucionar en paralelo al entorno de la Organización. El desarrollo de estos procedimientos de actualización debe llevar asociada la asignación de funciones y responsabilidades, así como la dotación de recursos técnicos, humanos y económicos necesarios.
- **Carga automática de recursos de información** en la herramienta de análisis de riesgos, de modo que la valoración del riesgo se adapte permanentemente con los cambios en los recursos empleados. Este mecanismo debe estar acompañado de los procedimientos necesarios para mantener la integridad del sistema. El establecimiento de las relaciones entre los activos y los recursos de información se deberá realizar, en general, de forma manual, reflejándose las sustituciones de unos recursos por otros en el soporte de determinados activos o la asignación de los activos que van a soportar los nuevos recursos que se incorporen. Si no se lleva a cabo este establecimiento de relaciones, no será posible la propagación del valor desde los activos de información hasta los recursos, y por tanto no será posible realizar un cálculo del riesgo fiable.

- **Establecimiento de procedimientos periódicos de revisión** del análisis de riesgos. Aunque se lleven a cabo los procedimientos adecuados para la evolución del análisis de riesgos con la evolución de la Organización y de su entorno, es conveniente realizar periódicamente una revisión completa del análisis realizado. Esto se debe a que los procedimientos de actualización continua pueden pasar por alto determinados cambios leves que, sostenidos en el tiempo, pueden terminar impactando sobre la valoración de los riesgos. También es posible que exista una determinada tasa de errores en la ejecución de los procesos de actualización del análisis de riesgos, provocando una desvirtuación progresiva del análisis de riesgos. Las revisiones periódicas del análisis de riesgos pueden realizarse utilizando la misma metodología empleada en el primer desarrollo, si bien, generalmente, su aplicación podrá ser mucho más ligera, por existir una base de partida importante, si bien esta base deberá utilizarse con cuidado para evitar que su uso introduzca un sesgo en la revisión del análisis. El desarrollo de estos procedimientos de revisión debe llevar asociada la asignación de funciones y responsabilidades, así como la dotación de recursos técnicos, humanos y económicos necesarios.

11.3. Implantación del SGSI

Un Sistema de Gestión de Seguridad de la Información (SGSI) consta de todos los elementos necesarios para planificar, definir, implantar, verificar y supervisar las medidas de seguridad necesarias para cumplir los requerimientos de seguridad de la Organización. Es estándar más extendido para la definición e implantación de un SGSI es el ISO/IEC 27001:2005 [ISO27001.05].

El SGSI se basa en la aplicación del Ciclo de Deming, o de la mejora continua en el ámbito de la seguridad de la información:

- Planificar: establecer las políticas, objetivos, normas, procesos, procedimientos necesarios para gestionar los riesgos y mejorar la seguridad de la información, de acuerdo a las necesidades y requerimientos de la Organización.
- Ejecutar: implantar y operar las políticas, procesos, procedimientos y controles definidos.
- Verificar: evaluar la eficacia y eficiencia de las políticas, procesos, procedimientos y controles para lograr los objetivos de seguridad de la información definidos. Identificar aquellas no conformidades con la planificación realizada.
- Actuar: definir las medidas preventivas y correctivas destinadas a solucionar las no conformidades detectadas, a mejorar el cumplimiento de los requerimientos de seguridad de la información definidos y adaptar el sistema a los cambios internos y externos relevantes.

Un SGSI conforme con el estándar ISO/IEC 27001:2005 consta, fundamentalmente, de los siguientes elementos:

- Análisis de riesgos
- Cuerpo normativo, incluyendo:
 - Definición del alcance del SGSI
 - Política de seguridad.
 - Declaración de aplicabilidad, que detalla los controles necesarios para alcanzar los objetivos de seguridad fijados.
 - Procesos de seguridad.
 - Procedimientos de seguridad.
 - Registros de seguridad.

- Asignación de funciones y responsabilidades:
 - Dirección
 - Ejecución de procesos y controles
 - Revisión del SGSI
 - Formación a todos los participantes

11.4. Implantación del Plan de Seguridad

Una vez finalizado el análisis de riesgos, se dispone de un conjunto de medidas de seguridad (y de un conjunto de líneas futuras de trabajo) que es necesario implantar para alcanzar el nivel de riesgo considerado tolerable por la Dirección.

Debido al elevado número de controles a implantar y al impacto que muchos de ellos suponen para los procesos y los sistemas, es necesario dedicar recursos suficientes a la gestión de los diferentes proyectos, para garantizar su coordinación y la calidad del resultado final. Algunas de las tareas principales serían:

- Planificar los proyectos. La planificación de los proyectos requerirá considerar diferentes aspectos:
 - Definición de fechas de inicio, finalización e hitos destacados para cada proyecto. Esta definición permitirá que todos los participantes tengan claros sus objetivos, que el cumplimiento de estos objetivos sea medible y que las desviaciones sobre la planificación se detecten a tiempo y puedan corregirse.
 - Coordinar las actividades de los distintos proyectos que lo requieren, estableciendo funciones y responsabilidades claras y coordinando los calendarios de los distintos proyectos involucrados.
- Realizar un seguimiento continuo de la evolución de los diferentes proyectos a nivel presupuestario, temporal, de calidad, etc.

Las metodologías más extendidas para la gestión de los proyectos son PMBOK (Project Management Base Of Knowledge) [PMI00] y PRINCE2 (PRojects IN Controlled Environments) [PRINCE05] [PRINCE06] [P3M3.06].

11.5. Medición de los resultados

Tanto el análisis de riesgos como el desarrollo de un SGSI o de un Plan de Seguridad son iniciativas costosas y que requieren largos periodos de ejecución, por lo que es necesario proporcionar a la Organización información sobre su evolución y sobre su utilidad.

Los principales objetivos en la elaboración de métricas en el ámbito de la seguridad de la información son:

- Disponer de información actualizada sobre la ejecución de los diferentes proyectos de seguridad, a nivel presupuestario y a nivel de tiempos de ejecución.
- Disponer del grado de consecución de los objetivos, en relación con los requerimientos de seguridad planteados.
- Comparar el nivel de seguridad de la Organización con el nivel de otras organizaciones similares, ya sea dentro o fuera del sector o teniendo en cuenta criterios de volumen, geográficos, etc., mediante la utilización de comparativas y estudios realizados por entidades independientes.

Las principales tareas a considerar para realizar la medición de los resultados del análisis de riesgos son:

- Definir los objetivos de las mediciones.
- Identificar un conjunto reducido de indicadores relevantes que permita dar información precisa sobre los diferentes aspectos a medir.
- Establecer los mecanismos tecnológicos y operativos que permitan realizar el cálculo de los indicadores de forma rápida y precisa.

Actualmente está en elaboración el estándar ISO/IEC 27004 Information technology — Security techniques — Information security management — Measurement, que definirá los requerimientos para la medición de los controles de seguridad implantados. Su publicación está prevista para finales de 2009.

11.6. Integración con otras áreas

A medida que el enfoque de la seguridad informática entendida desde un punto de vista meramente tecnológico evoluciona hacia un enfoque más amplio de seguridad de la información, la necesidad de interactuar con diferentes áreas de la Organización se incrementa, haciéndose necesario desarrollar mecanismos para fomentar la colaboración o incluso, adecuar la estructura organizacional.

Algunas de las áreas cuya colaboración es necesaria en el ámbito de la seguridad de la información son:

- **Dirección**, para la definición de los objetivos de seguridad y la coordinación de iniciativas que requieran la colaboración de diferentes áreas de la Organización.
- **Sistemas de Información**, para la implantación de determinadas medidas tecnológicas, para participar en los principales proyectos de desarrollo e implantación y evolución de sistemas, tanto a nivel de aplicativos como de infraestructura.
- **Seguridad Patrimonial**, debido a la necesidad de establecer de determinadas medidas de seguridad física en salas técnicas (CPD, salas de comunicaciones, etc.), salas de usuarios o archivos de información en papel.
- **Riesgos**, debido a la necesidad de integrar los riesgos de seguridad de la información en el marco general de control de riesgos de la Organización.
- **Recursos Humanos**, debido a la necesidad de asignar funciones y responsabilidades en materia de seguridad de la información, aumentar el control sobre el acceso de los empleados a la información y la necesidad de realizar campañas de formación y concienciación.
- **Asesoría Jurídica**, debido a la existencia de requerimientos legales, normativos, regulatorios y contractuales relativos al cumplimiento de seguridad de la información.

- **Auditoría Interna**, debido a la necesidad de revisar periódicamente el cumplimiento de los procedimientos y controles de seguridad de la información.

La necesidad de interactuar con todas estas áreas de la Organización pueden conducir a diversas medidas organizativas, como:

- Creación de comités y grupos de trabajo dedicados a la seguridad de la información.
- Creación de áreas de seguridad corporativa que integren la seguridad desde los diferentes puntos de vista (patrimonial, de la información, de recursos humanos, medioambiental, etc.)

11.7. Evolución de las metodologías de análisis de riesgos

Si bien el análisis es una actividad necesaria para la definición de la estrategia y el plan de seguridad de la información, las metodologías de análisis de riesgo actuales son bastante pesadas, de modo que su ejecución es costosa en tiempo y en esfuerzo. [CARD08] [MORAL07] [MORAL08]

Adicionalmente, las metodologías actuales de análisis de riesgos muestran una imagen estática de los riesgos de seguridad de la información, siendo la actualización una tarea también costosa en tiempo y en esfuerzo.

Existen actualmente diversas propuestas para la mejora del análisis de riesgos que, si bien aún no tienen un uso extenso fuera de la experimentación de sus desarrolladores, en el futuro pueden ser alternativas viables para la realización del análisis de riesgos.

Las estrategias para la mejora del análisis de riesgos pueden clasificarse en dos grandes grupos:

- Mejora de las herramientas disponibles, incluyendo elementos como:
 - Optimización del modelo de análisis, buscando detectar la información no relevante en los momentos iniciales del análisis, de modo que no sea necesaria su consideración.
 - Desarrollo de interfases que permitan cierto grado de automatización en la introducción de datos, especialmente en el mantenimiento de inventarios.
 - Desarrollo de inventarios estándar de vulnerabilidades, amenazas, tipos de activos, etc. que faciliten la automatización de determinados cálculos.
 - Segmentación del análisis utilizando dominios de seguridad.
- Búsqueda de modelos alternativos o complementarios al probabilístico. Si bien no existe ningún modelo alternativo que destaque, existen diversos desarrollos sobre varios modelos, entre los que cabe destacar:
 - Análisis de árboles de ataque.
 - Modelos basados en teoría de juegos.
 - Análisis de las cinco fuerzas de Porter.
 - Modelo de océano azul.
 - Análisis coste/beneficio.
 - Ley de Pareto.
 - Análisis de la cadena de valor.
 - Análisis RAR (Rentabilidad Ajustada al Riesgo)
 - Empleo de técnicas de inteligencia artificial.

- Otra debilidad de las metodologías actuales de análisis de riesgo se debe a que actualmente no existe ninguna base de datos histórica que permita definir con precisión la probabilidad y el impacto que pueden tener las amenazas sobre los activos de información, así como la eficacia de las salvaguardas que pueden definirse para su mitigación. Esto obliga a elaborar la información a emplear en el análisis de riesgos en función de datos parciales y de consenso de los expertos implicados.

12. CONCLUSIONES

Las principales conclusiones obtenidas de la ejecución de este trabajo han sido:

- Se han identificado los principales activos de información de la Organización en términos de los requerimientos de seguridad definidos, lo que ha permitido identificar las áreas que requieren mayor atención, diferenciándolas de aquellas para las que puede ser suficiente el baseline actual de seguridad.
- Se han inventariado y valorado las salvaguardas implantadas, lo que ha permitido identificar el nivel de seguridad general de la Organización y los aspectos de seguridad más débiles en relación con los requerimientos de seguridad generales y específicos.
- El apoyo de la Dirección es un factor imprescindible para el éxito del proyecto, debido a la necesidad de contar con la colaboración de personal de diversas áreas de la Organización, en muchos casos de niveles gerenciales o directivos. Adicionalmente, los resultados del análisis de riesgos debe elevarse y someterse a la aprobación de la Dirección, que debe conocer los resultados del análisis y las alternativas propuestas para cumplir los requerimientos identificados y formalizados.
- La existencia de documentación previa que recoja inventarios, aunque sean parciales, de procesos, activos de información, recursos de información, etc., aumentan significativamente la eficiencia y la calidad en la realización del análisis, ya que permiten realizar un trabajo previo a las entrevistas que las hace más productivas.
- Es necesario integrar la información de negocio, que determina lo que es importante y lo que no lo es para el cumplimiento de los objetivos corporativos definidos y la información tecnológica que determina los elementos que es necesario proteger para asegurar un soporte adecuado al cumplimiento de los objetivos de negocio.

- Las medidas de seguridad necesarias para proteger la información de la Organización deben ser de diversos tipos: organizativos, tecnológicos, etc. y trabajar adecuadamente de forma integrada.
- La explosión combinatoria de los datos involucrados en el análisis es un aspecto crítico a controlar para el éxito del proyecto. Por ejemplo, el cálculo del riesgo efectivo de un único activo debe considerar los siguientes parámetros:

5 requerimientos x 60 amenazas x 133 salvaguardas = 39.900 combinaciones.

- Uno de los aspectos más importantes para el control de la explosión combinatoria es realizar el análisis con un nivel adecuado de granularidad de la información. Si se trata de llegar a un nivel excesivamente detallado (por ejemplo, inventariando PCs de usuario, con requerimientos similares de seguridad salvo excepciones) se realiza un esfuerzo considerable del que se obtiene poco rendimiento, o incluso rendimiento negativo, puesto que los resultados del análisis pueden resultar menos claros.
- Otro aspecto relevante para controlar la explosión combinatoria consiste en respetar escrupulosamente los alcances definidos para el análisis (por ejemplo, a nivel de procesos de negocio, entornos tecnológicos o estructura societaria), y tener en cuenta el objetivo final del mismo (por ejemplo descartando aspectos de seguridad física, legales, etc., si no forman parte del alcance considerado). Esto permite evitar realizar trabajo que finalmente no va a soportar el objetivo final del proyecto.
- Es necesario disponer de un conocimiento profundo tanto de la tecnología como de los procesos de negocio para ejecutar adecuadamente un proyecto de análisis de riesgos que obtenga unos resultados ajustados a la realidad.
- La función del analista de riesgos consiste en guiar en el proceso y en aplicarlo con la información proporcionada por el personal de negocio o de tecnología. Se requiere una importante capacidad de comunicación para extraer toda la información necesaria de los participantes sin introducir sesgos ni contaminación.

- Dado que uno de los aspectos más importantes del análisis de riesgos es su carácter sistemático, es muy importante la aplicación escrupulosa de la metodología definida, de modo que las técnicas, métodos y criterios empleados sean adecuados y homogéneos. Para ello, es importante mantener reuniones de coordinación en las que se traten todos los casos particulares identificados, y que se documenten los criterios seguidos, de modo que sean conocidos inequívocamente por parte de todo el equipo.

13. BIBLIOGRAFÍA

13.1. Bibliografía

- ISO - International Standards Office (<http://www.iso.ch>)
 - [ISO13335-1.04] ISO/IEC TR 13335-1:2004, Information technology -- Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management.
 - [ISO13335-2.97] ISO/IEC TR 13335-2:1997, Information technology -- Security techniques – Management of information and communications technology security – Part 2: Managing and planning IT Security.
 - [ISO13335-3.98] ISO/IEC TR 13335-3:1998, Information technology -- Security techniques – Management of information and communications technology security – Part 3: Techniques for the management of IT Security.
 - [ISO13335-4.00] ISO/IEC TR 13335-4:2000, Information technology -- Security techniques – Management of information and communications technology security – Part 4: Selection of safeguards.
 - [ISO13335-5.01] ISO/IEC TR 13335-5:2001, Information technology -- Security techniques – Management of information and communications technology security – Part 5: Management guidance on network security.
 - [ISO27001.05] ISO/IEC 27001:2005, Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI)
 - [ISO27002.05] ISO/IEC 27002:2005, Tecnología de la información. Técnicas de seguridad. Código de buenas prácticas de la Gestión de la Seguridad de la Información.

- [ISO27005.08] ISO/IEC 27005:2008, Tecnología de la información. Técnicas de seguridad. Gestión de riesgos de Seguridad de la Información.
- [ISO7498-2.89] ISO 7498-2:1989, Information processing systems -- Open Systems Interconnection – Basic Reference Model -- Part 2: Security Architecture”.
- [ISO15408-1.05] ISO/IEC 15408-1:2005, Information technology -- Security techniques – Evaluation criteria for IT security (Common criteria) – Part 1: Introduction and general model
- [ISO15408-2.08] ISO/IEC 15408-2:2008, Information technology -- Security techniques – Evaluation criteria for IT security (Common criteria) – Part 2: Security functional components
- [ISO15408-3.08] ISO/IEC 15408-3:2008, Information technology -- Security techniques – Evaluation criteria for IT security (Common criteria) – Part 3: Security assurance components
- [ISO15443-1.05] ISO/IEC TR 15443-1:2005, Information technology -- Security techniques -- A framework for IT security assurance -- Part 1: Overview and framework
- [ISO15443-2.05] ISO/IEC TR 15443-2:2005, Information technology -- Security techniques -- A framework for IT security assurance -- Part 2: Assurance methods
- [ISO15443-3.07] ISO/IEC TR 15443-3:2007, Information technology -- Security techniques -- A framework for IT security assurance -- Part 3: Analysis of assurance methods
- [ISO16085.06] ISO/IEC 16085:2006, Ingeniería de software y sistemas – procesos del ciclo de vida – Gestión de riesgos
- [ISO18028-1.06] ISO/IEC 18028-1:2006, Tecnología de la información – Técnicas de seguridad – Seguridad de redes TI – Parte 1: Gestión de la seguridad de redes de comunicaciones
- [ISO20000-1.05] ISO/IEC 20000-1:2005, Tecnología de la información – Gestión del servicio – Especificación.

- [ISO20000-2.05] ISO/IEC 20000-2:2005, Tecnología de la información – Gestión del servicio – Código de buenas prácticas.
- [ISO21827.02] ISO/IEC 21827:2002, Tecnología de la Información – Técnicas de seguridad – Ingeniería de Seguridad de Sistemas – Modelo de Madurez de Capacidades (SSE-CMM)
- [ISO72.01]ISO Guide 72:2001, Guidelines for the justification and development of management system standards.
- [ISO73.05] ISO/IEC Guía 73:2005, Gestión del riesgo. Vocabulario. Directrices para la utilización de las normas.
- AENOR – Asociación Española de Normalización y Certificación (<http://www.aenor.es>)
 - [UNE71501.01] UNE 71501 Tecnología de la Información (TI). Guía para la gestión de la seguridad de TI, 2001.
 - [UNE71502.04] UNE 71502 Tecnología de la Información (TI). Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI), AENOR, 2004.
 - [UNE71504.08] UNE 71504 Tecnología de la Información (TI). Metodología de análisis y gestión de riesgos para los sistemas de información, AENOR, 2008.
- BSI – British Standards Institution (<http://www.bsi-global.com/>)
 - [BS7799-3.06] BS 7799-3:2006 Information Security Management Systems. Guidelines for information Security Risk Management.
 - [BS25999-1.06] BS 25999-1:2006 Business continuity management. Code of practice.
 - [BS25999-2.07] BS 25999-2:2007 Business continuity management. Specification.
- AS/NZS – Australian Standards / New Zealand Standards (<http://www.standards.com.au/> <http://www.standards.com.nz/>)
 - [AS4360.04] AS/NZS 4360:2004 Risk management

- MAGERIT (<http://publicaciones.administracion.es>)
 - [MAGE06] Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, versión 2, F. López, M.A. Amutio, J. Candau y J.A. Mañas, Ministerio de Administraciones Públicas, 2006.
- OCTAVE (<http://www.cert.org/octave>)
 - [ALBER01] OCTAVE Method Implementation Guide Version 2.0, C. Alberts y A. Dorofee, Carnegie Mellon University, 2001.
 - [ALBER03A] Managing information Security Risks. The OCTAVE Approach, C. Alberts y A. Dorofee, Addison Wesley, 2003.
 - [ALBER03B] Introduction to the OCTAVE Approach, C. Alberts, A. Dorofee, J. Stevens, C. Woody, Carnegie Mellon University, 2003.
 - [ALBER05] OCTAVE-S Implementation Guide, Version 1.0, Alberts, A. Dorofee, J. Stevens, C. Woody, Carnegie Mellon University, 2005.
 - [ALBER07] Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, R. Caralli, J. Stevens, L. Young, W. Wilson, Carnegie Mellon University, 2007.
- CRAMM (<http://www.cramm.com>)
 - [CRAMM03] CCTA Risk Análisis and Management Method (CRAMM), Versión 5.0, CCTA - Central Computing and Telecommunications Agency, 2003.
- NIST – National Institute of Standards and Technology (<http://www.nist.gov>)
 - [NIST800-30.02] NIST SP 800-30, Risk Management Guide for Information Technology Systems, G. Stoneburner, A. Goguen y A. Feringa, NIST Special Publication, 2002.
 - [NIST800-12.95] NIST SP 800-12, An Introduction to Computer Security: the NIST Handbook, NIST Special Publication, 1995.
 - [NIST800-14.96] NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, M. Swanson, B. Guttman, 1996.

- [NIST800-18.98] NIST SP 800-18. Guide For Developing Security Plans for Information Technology Systems. NIST y Federal Computer Security Managers' Forum Working Group, 1998.
- [NIST80-26.01] NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems, NIST Special Publication, 2001.
- [NIST800-27.01] NIST SP 800-27. Engineering Principles for IT Security. NIST Special Publication, 2001.
- [NIST800-53.04] NIST SP 800-53, Recommended Security Controls for Federal Information Systems, R. Ross, S. Katzke, A. Johnson, M. Swanson, G. Stoneburner y G. Rogers, NIST Special Publication, 2004.
- ISF – Information Security Forum (<http://www.securityforum.org/>)
 - [ISF06] Information Risk Analysis Methodologies (IRAM) Project, ISF, 2006.
 - [ISF07] Standard of Good Practice for Information Security. ISF, 2007.
- CORAS (<http://coras.sourceforge.net/>)
 - [STOL01] The CORAS framework for a model-based risk management process, R. Fredriksen, M. Kristiansen, B. Gran y K. Stolen, 2001.
 - [STOL02A] Model-based risk assessment -- The CORAS approach, K. Stolen, F. den Braber, S. Lund y J. Aagedal, 2002.
 - [STOL02B] The CORAS approach for model-based risk management applied to e-commerce domain, D. Raptis, T. Dimitrakos, A. Gran y K. Stolen, 2002.
 - [STOL06] A Graphical Approach to Risk Identification, Motivated by Empirical Investigations, I. Hogganvik, K. Stolen, SINTEF, 2006.
 - [STOL07A] Model-based security analysis in seven steps –a guided tour to the CORAS method, F. den Braber, I. Hogganvik, S. Lund, K. Stolen, F. Vraalsen, BT Technology Journal, 25(1): 101 –117, 2007.

- [STOL07B] Structured semantics for the CORAS security risk modelling language, H. Dahl, I. Hogganvik, K. Stolen, Technical report STF07 A970, SINTEF Information and Communication Technology, 2007.
- [HOGG07A] A graphical approach to security risk analysis, I. Hogganvik, PhD thesis, Faculty of Mathematics and Natural Sciences, University of Oslo, 2007.
- SOMAP – Security Officers Management & Análisis Project (<http://www.somap.org/>)
 - [SOMAP07] Open Information Security Risk Assessment Guide, Version 1.0, SOMAP.org, 2007
 - [SOMAP06] Open Information Security Risk Management Handbook, Version 1.0, SOMAP.org, 2006
- FAIR – Factor Analysis of Information Risk (www.riskmanagementinsight.com)
 - [JONES05A] An Introduction to Factor Analysis of Information Risk (FAIR). A framework for understanding, analyzing, and measuring information risk. J. Jones, Risk Management Insight, 2005.
 - [JONES05B] FAIR (Factor Analysis of Information Risk). Basic Risk Assessment Guide. J. Jones, Risk Management Insight, 2005.
 - [JONES08A] Improving Risk Decisions. J. Jones. Risk Management Insight, 2008.
 - [JONES08B] Risk Evolution Part II. J. Jones. Risk Management Insight, 2008.
- Comparación de modelos de análisis de riesgos:
 - [GLAM04] A Critical Discussion of Risk and Threat Analysis Methods and Methodologies. S. Vidalis. School of Computing, University of Glamorgan. 2004.
 - [VORST05] A framework for comparing different information security risk analysis methodologies. A. Vorster, L. Labuschagne, ACM 2005.

- [ENISA06] Inventory of risk assessment and risk management methods. ENISA, 2006.
- COSO - Committee of Sponsoring Organizations of the Treadway Commission (www.coso.org)
 - [COSO92] COSO, Internal Control — Integrated Framework, 1992.
 - [COSO04] COSO, Enterprise Risk Management — Integrated Framework, 2004.
- BIS – Bank for International Settlements (<http://www.bis.org/>)
 - [BIS04] Convergencia internacional de medidas y normas de capital – Marco revisado, Comité de Supervisión Bancaria, 2004.
 - [BIS03] Risk Management Principles for Electronic Banking, Basel Committee on Banking supervision, 2003.
- OGC - Office of Government Commerce (<http://www.ogc.gov.uk>)
 - [ITIL06] ITIL V3 Foundation Handbook, Office of Government Commerce, 2006
 - [PRINCE05] PRINCE2 Manual (Managing Successful Projects with PRINCE2), Office of Government Commerce, 2005.
 - [PRINCE06] PRINCE2 Maturity Model, Version 1.0, Office of Government Commerce, 2006
 - [P3M3.06] Portfolio, programme & project management maturity model (P3M3), Version 1.0, Office of Government Commerce, 2006.
- PMI – Project Management Institute (<http://www.pmi.org>)
 - [PMI00] A Guide to the Project Management Body of Knowledge (PMBOK Guide), Project Management Institute, 2000.
- OCDE – Organización para la Cooperación y el Desarrollo Económico (<http://www.oecd.org/>)
 - [OCDE02] Directrices de la OCDE para la seguridad de sistemas y redes de información: hacia una cultura de seguridad, OCDE, 2002.
 - [OCDE04] Principios de Gobierno Corporativo, OCDE, 2004.

- PCI SSC – Payment Card Industry Security Standards Council (<http://www.pcisecuritystandards.org>)
 - [PCI08] Industria de Tarjetas de Pago (PCI). Normas de seguridad de datos. Requisitos y procedimientos de evaluación de seguridad. Versión 1.2. PCI Security Standards Council LLC, 2008.
- ISACA – Information Systems Audit and Control Association (<http://www.isaca.org>)
 - [ISACA07] Control Objectives for Information and Related Technologies (COBIT), Versión 4.1, ITGI – Information Technology Governance Institute, ISACA, 2007.
- SEI – Software Engineering Institute (<http://www.sei.cmu.edu/cmml>)
 - [SEI06] SEI, Capability Maturity Model Integration (CMMi), Versión 1.2, SEI, 2006
- American Institute of Certified Public Accountants (www.aicpa.org)
 - [AICPA00] AICPA/CICA, WebTrust Program for Certification Authorities, 2000.
 - [AICPA08] Canadian Institute of Chartered Accountants, Webtrust for Certification Authorities – Extended validation audit criteria. Version 1.1., 2008.
- Nuevos modelos de análisis de riesgos:
 - [CARD08] Game Theoretic Risk Analysis of Security Threats, J. Cardoso, P. Diniz. Springer US. 2008.
 - [MORAL08] Alternativas viables para analizar los riesgos de seguridad en tiempos de Mercado: La teoría de juegos. S. Moral. Securmática 2008.
 - [MORAL07] La credibilidad del CISO. S. Moral. Securmática 2007.

- Seguridad de la información:
 - [ISC2.04] Official (ISC)² Guide to the CISSP Exam. S. Hansche, J. Berti, C. Hare. (ISC)². 2004.
 - [HARRIS06] CISSP Exam Guide: All In One 3rd Edition. S. Harris. McGraw-Hill/Osborne, 2006.
 - [ISACA06] CISA review manual 2006. ISACA, 2006.
 - [ISACA08] CISM review manual 2008. ISACA, 2008.

13.2. Mapa de referencias bibliográficas

En el siguiente diagrama se describen las relaciones entre las referencias bibliográficas citadas, clasificadas por sus fuentes y cronológicamente.

Por simplicidad del gráfico no se han reflejado las referencias entre documentos de la misma fuente, considerándose que, en general, la documentación generada por una fuente determinada será íntegra.

Tampoco se incluyen en el gráfico las referencias a documentos procedentes de fuentes no consideradas en la realización de este trabajo, debido a su elevado número.

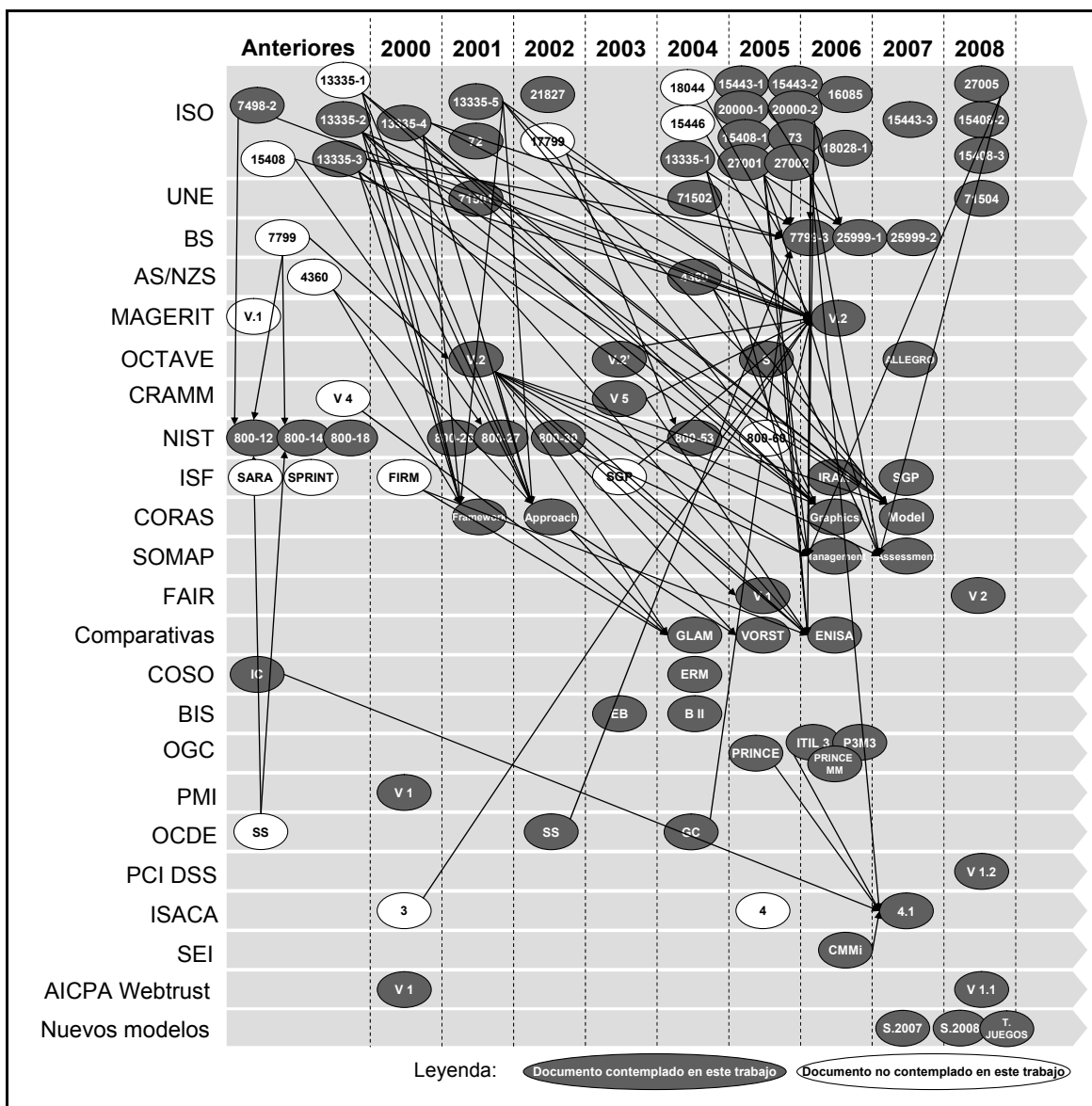


Figura 29: Mapa de referencias bibliográficas

ANEXO I: ESTUDIOS DE TENDENCIAS EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN

Algunos de los principales estudios¹ que se publican periódicamente analizando las tendencias en materia de Seguridad de la Información son los siguientes:

- Difusión libre:
 - <http://www.enisa.europa.eu> → Enisa, European Network and Information Security Agency
 - <http://www.inteco.es> → Inteco, Instituto Nacional de Tecnologías de la Comunicación
 - <http://www.gocsi.org> → Computer Security Institute
 - http://www.ey.com/global/Content.nsf/International/Assurance_&_Advisory_-_Technology_and_Security_Risk_-_Global_Information_Security_Survey_2008 → Ernst & Young
 - <http://www.pwc.com/extweb/home.nsf/docid/c1cd6cc69c2676d4852574da00785949> → PriceWaterhouse Coopers
 - http://www.deloitte.com/dtt/cda/doc/content/dtt_fsi_GlobalSecuritySurvey_0901.pdf → Deloitte
 - <http://www.symantec.com/business/theme.jsp?themeid=threatreport> → Symantec
 - <http://www.sophos.com/pressoffice/news/articles/2008/01/security-report.html> → Sophos
 - <http://www.s21sec.com/> → S21Sec

¹ Debido al elevado número de estudios que se publican sobre la materia, esta lista no puede ser exhaustiva, sino simplemente representativa de los estudios de mayor difusión y relevancia en el ámbito nacional y global.

- Bajo suscripción:
 - <http://www.forrester.com> → Forrester Research
 - <http://www.gartner.com> → Gartner Group
 - <http://www.securityforum.org> → Information Security Forum (ISF)
 - <https://www.irec.executiveboard.com/> → Information Risk Executive Council (IREC)
- Incidencias de seguridad:
 - <http://www.idtheftcenter.org> → Identity Theft Resource Center
 - <http://datalossdb.org> → Data Loss Database (Open Security Foundation)
 - <http://www.security-survey.gov.uk> → UK Department of Business, Enterprise and Regulatory Reform (BERR)
- Publicaciones en español:
 - Revista Seguridad de la Información y las Comunicaciones (SIC) (<http://www.revistasic.com>)
 - Revista Red Seguridad (<http://www.bormart.es/redseguridad.php>)
 - Revista e.Security (<http://www.ovecpubli.net/>)
 - Revista Auditoría y Seguridad (<http://www.revista-ays.com>)

Nota: Este listado no incluye las organizaciones encargadas de la publicación de vulnerabilidades o virus/malware identificados desde un punto de vista meramente tecnológico, que se consideran fuera del alcance de este trabajo.

ANEXO II: REFERENCIAS LEGISLATIVAS, REGULATORIAS Y NORMATIVAS AL ANÁLISIS DE RIESGOS

El análisis de riesgos es una práctica exigida por diversas leyes, regulaciones y normativas, y recomendada en diversos códigos de buenas prácticas y marcos de control interno.

A continuación se incluye un extracto de algunas de las principales referencias al uso del análisis de riesgos centradas fundamentalmente en el ámbito español.

Referencias legislativas

Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Extracto del Título II, Principios de la protección de datos, Artículo 9, Seguridad de los datos:

- 1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.*
- 2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.*
- 3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.*

Real Decreto 263/1996, de 16 de Febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.

Extracto del Capítulo I, Disposiciones generales, Artículo 4, Garantías generales de la utilización de soportes, medios y aplicaciones electrónicas, informáticas y telemáticas:

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

Referencias a códigos de buenas prácticas

Directrices de la OCDE para la seguridad de sistemas y redes de información: hacia una cultura de seguridad.

Principio 6: Evaluación del riesgo. Los participantes deben llevar a cabo evaluaciones de riesgo:

La evaluación del riesgo identificará las amenazas y vulnerabilidades, y debe ser lo suficientemente amplia para incluir factores internos y externos fundamentales como tecnología, factores físicos y humanos, y políticas y servicios de terceros que tengan repercusiones en la seguridad. La evaluación del riesgo permitirá determinar los niveles aceptables de seguridad y ayudar en la selección de controles apropiados para administrar el riesgo de daños potenciales a los sistemas y redes de información, en relación a la naturaleza e importancia de la información que debe ser protegida. Debido a la creciente interconexión de los sistemas de información, la evaluación del riesgo debe incluir asimismo consideraciones acerca del daño potencial que se puede causarse a terceros o que pueden tener su origen en terceras personas.

ISO/IEC 27001:2005 Tecnología de Información – Técnicas de seguridad – Sistemas de Gestión de Seguridad de la Información – Requerimientos

Extracto del capítulo 4.2 Establecer y gestionar el SGSI: [ISO27001.05]

La organización debe hacer lo siguiente:

[...]

c) Definir el enfoque de evaluación del riesgo de la organización:

- 1) Identificar una metodología de cálculo del riesgo adecuado para el SGSI y los requerimientos identificados de seguridad, legales y regulatorios de la información de negocio.*
- 2) Definir los criterios para aceptar los riesgos e identificar los niveles de riesgo aceptables.*

La metodología de evaluación del riesgo seleccionada debe asegurar que los cálculos del riesgo produzcan resultados comparables y reproducibles.

d) Identificar los riesgos

- 1) Identificar los activos dentro del alcance del SGSI y sus propietarios.*
- 2) Identificar las amenazas para estos activos.*
- 3) Identificar las vulnerabilidades que podrían ser explotadas por las amenazas.*
- 4) Identificar los impactos que pueden tener las pérdidas de confidencialidad, integridad y disponibilidad sobre los activos.*

e) Analizar y evaluar el riesgo

1) Calcular el impacto de negocio sobre la organización que podría resultar de un fallo de seguridad, teniendo en cuenta las consecuencias de una pérdida de confidencialidad, integridad o disponibilidad de los activos.

2) Calcular la probabilidad de que ocurra dicho fallo teniendo en cuenta las amenazas y vulnerabilidades existentes, los impactos asociados con estos activos y los controles implantados.

3) Calcular los niveles de riesgo.

4) Determinar si el riesgo es aceptable o requiere tratamiento utilizando el criterio de aceptación del riesgo establecido en 4.2.1.

f) Identificar y evaluar las opciones para el tratamiento de los riesgos. Las acciones posibles incluyen:

1) Aplicar los controles apropiados.

2) Aceptar los riesgos consciente y objetivamente, de acuerdo con las políticas y el criterio de aceptación del riesgo de la organización.

3) Evitar los riesgos.

4) Transferir los riesgos de negocio a otras entidades, por ejemplo, aseguradoras o proveedores.

[...]

ISO/IEC 27002:2005 Tecnología de Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información

Extracto del capítulo 4.1 Evaluación de los riesgos de seguridad: [ISO27002.05]

Las evaluaciones del riesgo debieran identificar, cuantificar y priorizar los riesgos en comparación con el criterio para la aceptación del riesgo y los objetivos relevantes para la organización. Los resultados debieran guiar y determinar la acción de gestión apropiada y las prioridades para gestionar los riesgos de la seguridad de la información y para implementar los controles seleccionados para protegerse contra estos riesgos. Es posible que el proceso de evaluación de riesgos y la selección de controles se deba realizar un número de veces para abarcar las diferentes partes de la organización o sistemas de información individuales.

La evaluación del riesgo debiera incluir el enfoque sistemático de calcular la magnitud de los riesgos (análisis del riesgo) y el proceso de comparar los riesgos estimados con un criterio de riesgo para determinar la importancia de los riesgos (evaluación del riesgo).

Las evaluaciones del riesgo también se debieran realizar periódicamente para tratar los cambios en sus requerimientos de seguridad y en la situación del riesgo; por ejemplo, en los activos, amenazas, vulnerabilidades, impactos, evaluación del riesgo, y cuando ocurren cambios significativos. Estas evaluaciones del riesgo se debieran realizar de una manera metódica capaz de producir resultados comparables y reproducibles.

La evaluación del riesgo de seguridad de la información debiera tener un alcance claramente definido para ser efectiva y debiera incluir las relaciones con las evaluaciones del riesgo en otras áreas, si fuese apropiado.

El alcance de la evaluación del riesgo puede ser la organización en su conjunto, partes de la organización, un sistema de información individual, componentes específicos del sistema o servicios donde esto es practicable, realista y útil. Los ejemplos de las tecnologías de evaluación del riesgo se discuten en ISO/IEC TR 13335-3 (Guías para la Gestión de la Seguridad TI: Técnicas para la Gestión de la Seguridad TI)

Extracto del capítulo 4.2 Tratamiento de los riesgos de seguridad:

Antes de considerar el tratamiento del riesgo, la organización debiera decidir el criterio para determinar si se pueden aceptar los riesgos, o no. Los riesgos pueden ser aceptados si, por ejemplo, se ha evaluado que el riesgo es bajo o que el costo del tratamiento no es efectivo en costo para la organización. Estas decisiones debieran ser registradas.

Para cada uno de los riesgos definidos después de una evaluación del riesgo se necesita tomar una decisión de tratamiento del riesgo. Las opciones posibles para el tratamiento del riesgo incluyen:

- a) aplicar los controles apropiados para reducir los riesgos;*
- b) aceptar los riesgos consciente y objetivamente, siempre que cumplan claramente con la política y el criterio de aceptación de la organización de la organización;*
- c) evitar los riesgos no permitiendo acciones que podrían causar que el riesgo ocurra;*
- d) transferir los riesgos asociados a otros grupos; por ejemplo, aseguradores o proveedores.*

BS 25999:2006 Gestión de continuidad de negocio

Extracto del capítulo 3.3 Relación con gestión de riesgos: [BS25999-1.06]
[BS25999-2.07]

La gestión de continuidad de negocio es complementaria con un marco de gestión de riesgos que defina el entendimiento de los riesgos a las operaciones o negocios, y las consecuencias de esos riesgos.

La gestión de riesgos trata de gestionar los riesgos de los productos y servicios clave que proporciona una organización. La producción de productos y servicios puede interrumpirse por una gran diversidad de incidentes, muchos de los cuales son difíciles de predecir o analizar.

Enfocándose en el impacto de la interrupción, la gestión de continuidad identifica los productos y servicios de los que la organización depende para su supervivencia, y puede identificar los requerimientos para que la organización continúe cumpliendo con sus obligaciones. Mediante la gestión de la continuidad de negocio, una organización puede reconocer lo que necesita preparar antes de que ocurra un incidente para proteger las personas, ubicaciones, tecnología, información, cadena de suministros, grupos de interés y reputación. Con ese reconocimiento la organización puede tener una visión realista de las respuestas que puedan necesitarse cuando ocurre una interrupción, de modo que pueda confiar en su capacidad para gestionar las consecuencias sin un retraso inaceptable en la producción de sus productos o servicios.

PCI/DSS – Payment Cards Industry/Data Security Standards

Extracto del requisito 12 Mantenga una política que aborde la seguridad de la información para empleados y contratistas: [PCI08]

<i>Requisitos de las PCI DSS</i>	<i>Procedimientos de prueba</i>
<i>12.1 Establezca, publique, mantenga y distribuya una política de seguridad que logre lo siguiente:</i>	<i>12.1 Examine la política de seguridad de la información y verifique que la política se publique y se distribuya a los usuarios del sistema que corresponda (incluidos proveedores, contratistas y socios comerciales).</i>
<i>12.1.1 Aborde todos los requisitos de PCI DSS.</i>	<i>12.1.1 Verifique que la política aborde todos los requisitos de PCI DSS.</i>
<i>12.1.2 Incluya un proceso anual que identifique las amenazas, y vulnerabilidades, y los resultados en una evaluación formal de riesgos.</i>	<i>12.1.2 Verifique que la política de seguridad de la información incluya un proceso de evaluación formal de riesgos que identifique las amenazas, las vulnerabilidades y los resultados de una evaluación formal de riesgos.</i>
<i>12.1.3 Incluya una revisión al menos una vez al año y actualizaciones al modificarse el entorno.</i>	<i>12.1.3 Verifique que la política de seguridad de la información se revise al menos una vez al año y se actualice según sea necesario de manera que refleje los cambios en los objetivos de la empresa o el entorno de riesgos.</i>

Tabla 25: Requerimientos de análisis de riesgos de PCI DSS

ITIL – Information Technology Infrastructure Library

Extracto del proceso de gestión de la seguridad: [ITIL06]

Gestión de la seguridad: detalla el proceso de planificar y gestionar un nivel definido de seguridad para la información y los servicios de TI, incluyendo todos los aspectos asociados con la reacción ante incidentes de seguridad. También incluye el análisis y la gestión de los riesgos y las vulnerabilidades, y la implantación de salvaguardas justificables en coste.

[...]

La gestión de seguridad de IT debe formar parte del trabajo de cualquier gerente de TI. La gerencia tiene la responsabilidad de tomar las medidas necesarias para reducir la probabilidad de que ocurra un incidente de seguridad hasta niveles aceptables. Esto se logra mediante el proceso de análisis y gestión de riesgos.

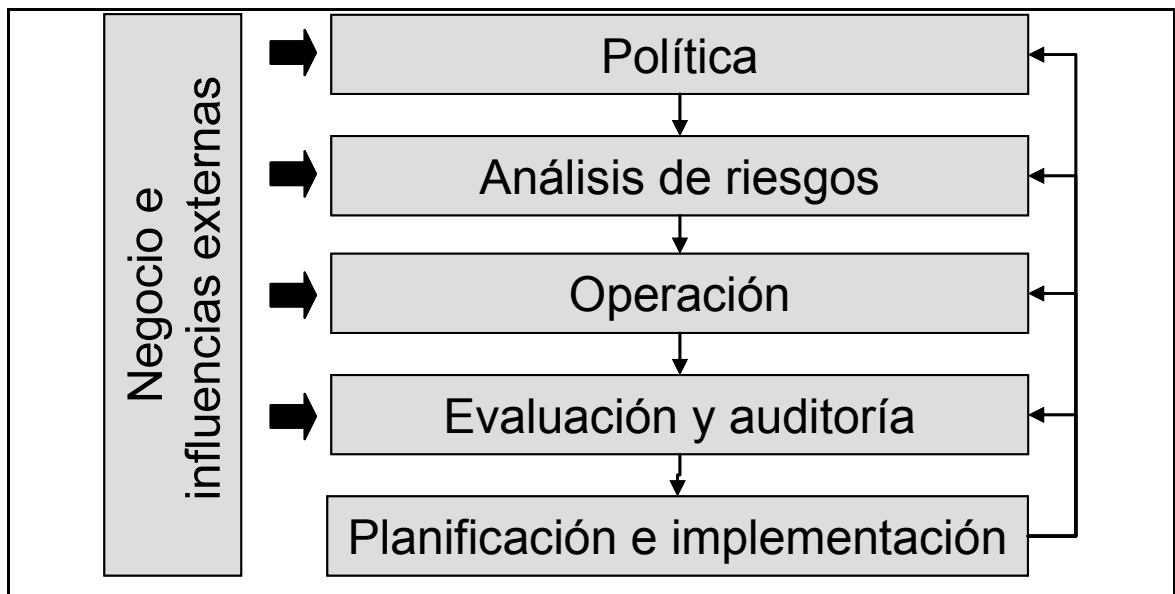


Figura 30: Modelo de Seguridad de la información de ITIL

La evaluación de riesgos y vulnerabilidades y la gestión e implantación de contramedidas de coste justificable son elementos intrínsecos del proceso de gestión de seguridad TI. Estas actividades deben estar coordinadas con las otras áreas de gestión del servicio, especialmente con el proceso de disponibilidad y gestión de la continuidad del servicio de TI.

Extracto del proceso de continuidad de TI:

El servicio de continuidad de TI produce planes de recuperación diseñados para asegurar que, tras cualquier incidente mayor que cause o pueda causar una interrupción del servicio, los servicios de TI se sigan proporcionando hasta un determinado nivel acordado, dentro de un plan acordado. Es importante para todas las organizaciones reconocer que el servicio de continuidad de TI es un componente del Plan de Continuidad de Negocio (PCN, BCP en sus siglas en inglés). El objetivo del servicio de continuidad de TI es ayudar al negocio y al PCN para minimizar la interrupción de los procesos esenciales de negocio durante y después de un incidente mayor. Para asegurar que los planes se mantienen alienados con las necesidades cambiantes del negocio, se deben realizar periódicamente análisis de impacto de negocio (BIA en sus siglas en inglés), análisis de riesgos y gestión de riesgos, así como el mantenimiento y las pruebas de todos los planes de recuperación.

ISO/IEC 20000 Tecnología de información – Gestión del servicio

Extracto del capítulo 6.3 Continuidad del servicio y gestión de la disponibilidad:
[ISO20000-1.05] [20000-2.05]

Objetivo: Asegurar que los compromisos de continuidad del servicio y disponibilidad pueden cumplirse en todas las circunstancias.

Los requerimientos de disponibilidad y continuidad del servicio deberán ser identificados en base a planes de negocio, acuerdos de nivel de servicio (ANS, SLA en sus siglas en inglés) y análisis de riesgos. Los requerimientos deberán incluir derechos de acceso y tiempos de respuesta así como disponibilidad de los componentes del sistema.

[...]

Los controles de seguridad deben estar documentados. La documentación debe describir los riesgos relacionados con los controles y la forma de operar y mantener los controles.

Extracto del apartado 6.6.3 Prácticas para la evaluación de riesgos de seguridad:

La evaluación de riesgos de seguridad debería:

- a) Ejecutarse a intervalos acordados.*
- b) Registrarse.*
- c) Mantenerse en caso de cambios (cambios de necesidades de negocio, procesos y configuración)*
- d) Ayudar a comprender qué puede impactar sobre un servicio gestionado.*
- e) Soportar decisiones sobre los tipos de controles a mantener.*

Extracto del apartado 6.6.4 Riesgos sobre activos de información:

Los riesgos sobre activos de información deberían ser evaluados en relación a:

- a) Su naturaleza (por ejemplo, fallos de software, errores de manejo, fallos en las comunicaciones)*
- b) Probabilidad*
- c) Impacto potencial sobre el negocio*
- d) Experiencias pasadas*

Extracto del apartado 6.6.5 Seguridad y disponibilidad de la información:

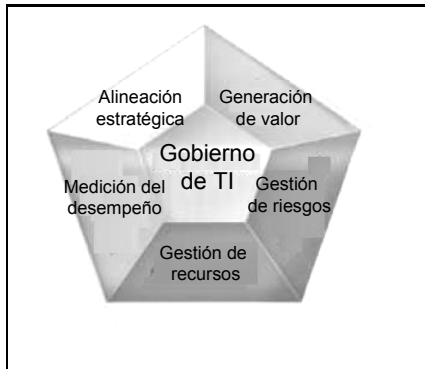
En la evaluación de los riesgos debe tenerse en cuenta:

- a) Acceso no autorizado a información sensible*
- b) Información imprecisa, incompleta o inválida (por ejemplo, fraudulenta)*
- c) Información no disponible para su uso (por ejemplo, fallos en el fluido eléctrico)*
- d) Daños físicos o destrucción del equipamiento necesario para proporcionar el servicio.*

También deben tenerse en cuenta los objetivos definidos en la política de seguridad de la información, la necesidad de cumplir los requerimientos de seguridad especificados por los clientes (por ejemplo, niveles de disponibilidad), y los requerimientos legales y regulatorios que sean aplicables.

COBIT – Control Objectives for Information and related Technology

Extracto del resumen ejecutivo: [ISACA07]



**Figura 31: COBIT -
Áreas del gobierno de TI**

Alineación estratégica se enfoca en garantizar el vínculo entre los planes de negocio y de TI; en definir, mantener y validar la propuesta de valor de TI; y en alinear las operaciones de TI con las operaciones de la empresa.

Generación de valor se refiere a ejecutar la propuesta de valor a lo largo del ciclo de entrega, asegurando que TI genere los beneficios prometidos en la estrategia, concentrándose en optimizar los costes y en proporcionar el valor intrínseco de la TI.

Gestión de recursos trata de la inversión óptima, así como la administración adecuada de los recursos críticos de TI: aplicaciones, información, infraestructura y personas. Los temas clave se refieren a la optimización de conocimiento y de infraestructura.

Gestión de riesgos requiere conciencia de los riesgos por parte de los altos ejecutivos de la empresa, un claro entendimiento del apetito de riesgo que tiene la empresa, comprender los requerimientos de cumplimiento, transparencia de los riesgos significativos para la empresa, y la inclusión de las responsabilidades de gestión de riesgos dentro de la organización.

Medición del desempeño rastrea y monitoriza la estrategia de implementación, la terminación del proyecto, el uso de los recursos, el desempeño de los procesos y la entrega del servicio, con el uso, por ejemplo, de balanced scorecards que traducen la estrategia en acción para lograr las metas que se puedan medir más allá del registro convencional.

Extracto del dominio PO, Planificar y Organizar. Proceso PO9 Evaluar y gestionar los riesgos de TI:

Objetivo de control de alto nivel:

Crear y dar mantenimiento a un marco de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales acordados. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar. Se deben adoptar estrategias de mitigación de riesgos para minimizar los riesgos residuales a un nivel aceptable. El resultado de la evaluación debe ser entendible para los participantes y se debe expresar en términos financieros, para permitir a los participantes alinear los riesgos a un nivel aceptable de tolerancia.

Objetivos principales: Confidencialidad, disponibilidad, integridad.

Objetivos secundarios: Efectividad, eficiencia, cumplimiento, fiabilidad.

Control sobre el proceso TI de:	<i>evaluar y administrar los riesgos de TI</i>
Que satisface el requisito de negocio de TI para:	<i>analizar y comunicar los riesgos de TI y su impacto potencial sobre los procesos y metas de negocio</i>
Enfocándose en:	<i>la elaboración de un marco de trabajo de administración de riesgos el cual está integrado en los marcos gerenciales de riesgo operacional, evaluación de riesgos, mitigación del riesgo y comunicación de riesgos residuales</i>
Se logra con:	<ul style="list-style-type: none"> • <i>La garantía de que la administración de riesgos está incluida completamente en los procesos administrativos, tanto interna como externamente, y se aplica de forma consistente</i> • <i>La realización de evaluaciones de riesgo</i> • <i>Recomendar y comunicar planes de acciones para mitigar riesgos</i>
y se mide con:	<ul style="list-style-type: none"> • <i>Porcentaje de objetivos críticos de TI cubiertos por la evaluación de riesgos</i> • <i>Porcentaje de riesgos críticos de TI identificados con planes de acción elaborados</i> • <i>Porcentaje de planes de acción de administración de riesgos aprobados para su implantación</i>

Tabla 26: Proceso COBIT de evaluación y administración de riesgos de TI

Áreas principales de gobierno de TI: Alineación estratégica, gestión de riesgos.

Áreas secundarias de gobierno de TI: ninguna.

Elementos del sistema: aplicaciones, información, infraestructura, personas.

Diagrama RACI de las funciones relacionadas con el proceso PO9:

	CEO	CFO	Ejecutivo del negocio	CIO	Propietario del proceso de negocio	COO	Arquitecto jefe	Jefe de desarrollo	Jefe de administración TI	PMO	Cumplimiento, auditoría, riesgos, seguridad
<i>Determinar la alineación de la gestión de riesgos</i>	A	R/A	C	C	R/A	I					I
<i>Entender los objetivos estratégicos de negocio relevantes</i>		C	C	R/A	C	C					I
<i>Entender los objetivos de los procesos de negocio relevantes</i>				C	C	R/A					I
<i>Identificar los objetivos de TI y establecer el contexto del riesgo</i>					R/A		C	C	C		I
<i>Identificar los eventos relacionados con los objetivos</i>	I			A/C	A	R	R	R	R		C
<i>Evaluar los riesgos asociados con los eventos</i>				A/C	A	R	R	R	R		C
<i>Evaluar las respuestas a los riesgos</i>	I	I	A	A/C	A	R	R	R	R		C
<i>Priorizar y planificar las actividades de control</i>	C	C	A	A	R	R	C	C	C		C
<i>Aprobar y garantizar la financiación de los planes de acción</i>		A	A		R	I	I	I	I		I
<i>Mantener y monitorizar el plan de acción de riesgos</i>	A	C	I	R	R	C	C	C	C	C	R

Tabla 27: Diagrama RACI de las funciones relacionadas con el proceso PO9

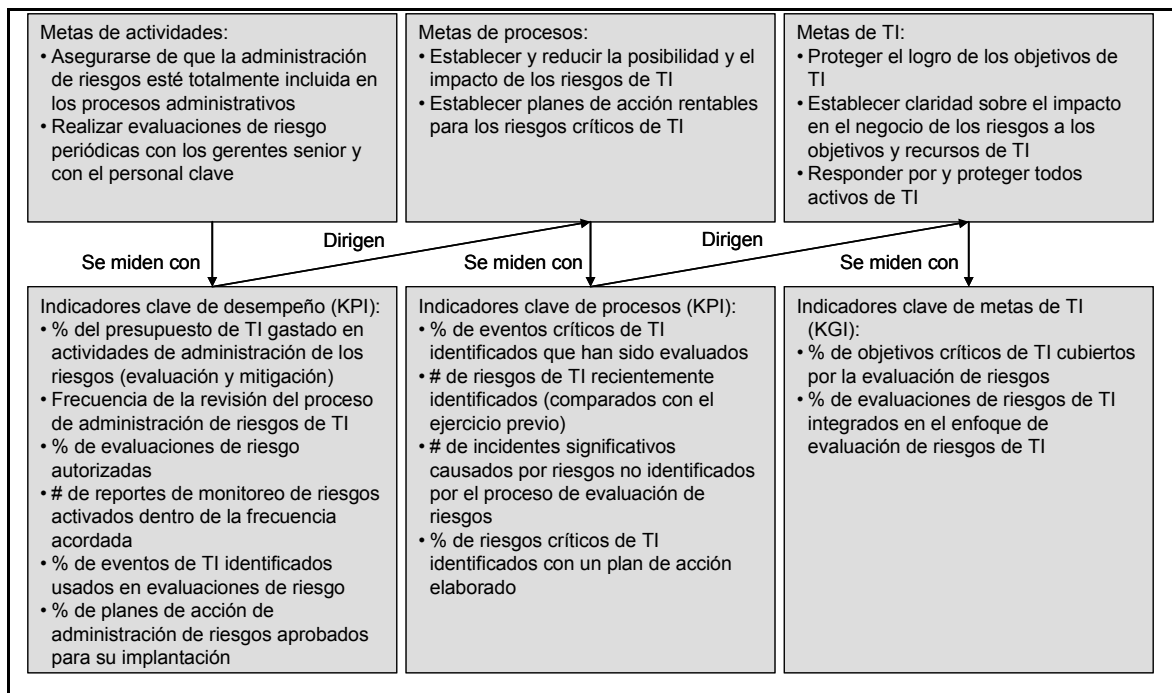


Figura 32: COBIT - Metas y métricas proceso PO9

Objetivos de control detallados:

PO9.1 Alineación de la administración de riesgos de TI y del negocio

Integrar el gobierno, la administración de riesgos y el marco de control de TI, al marco de trabajo de administración de riesgos de la organización. Esto incluye la alineación con el apetito de riesgo y con el nivel de tolerancia al riesgo de la organización

PO9.2 Establecimiento del contexto del riesgo

Establecer el contexto en el cual el marco de trabajo de evaluación de riesgos se aplica para garantizar resultados apropiados. Esto incluye la determinación del contexto interno y externo de cada evaluación de riesgos, la meta de la evaluación y los criterios contra los cuales se evalúan los riesgos.

PO9.3 Identificación de eventos

Identificar todos aquellos eventos (amenazas y vulnerabilidades) con un impacto potencial sobre las metas o las operaciones de la empresa, aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de recursos humanos y operativos. Determinar la naturaleza del impacto – positivo, negativo o ambos – y dar mantenimiento a esta información.

PO9.4 IT Evaluación de riesgos

Evaluar de forma recurrente la posibilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La posibilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio.

PO9.5 Respuesta a los riesgos

Identificar los propietarios de los riesgos y a los dueños de procesos afectados, y elaborar y mantener respuestas a los riesgos que garanticen que los controles rentables y las medidas de seguridad mitigan la exposición a los riesgos de forma continua. La respuesta a los riesgos debe identificar estrategias de riesgo tales como evitar, reducir, compartir o aceptar. Al elaborar la respuesta, considerar los costos y beneficios y seleccionar respuestas que limiten los riesgos residuales dentro de los niveles de tolerancia de riesgos definidos.

PO9.6 Mantenimiento y monitoreo de un plan de acción de riesgos

Asignar prioridades y planear las actividades de control a todos los niveles para implantar las respuestas a los riesgos, identificadas como necesarias, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución. Buscar la aprobación para las acciones recomendadas y la aceptación de cualquier riesgo residual, y asegurarse de que las acciones comprometidas son propiedad del dueño(s) de los procesos afectados. Monitorear la ejecución de los planes y reportar cualquier desviación a la alta dirección.

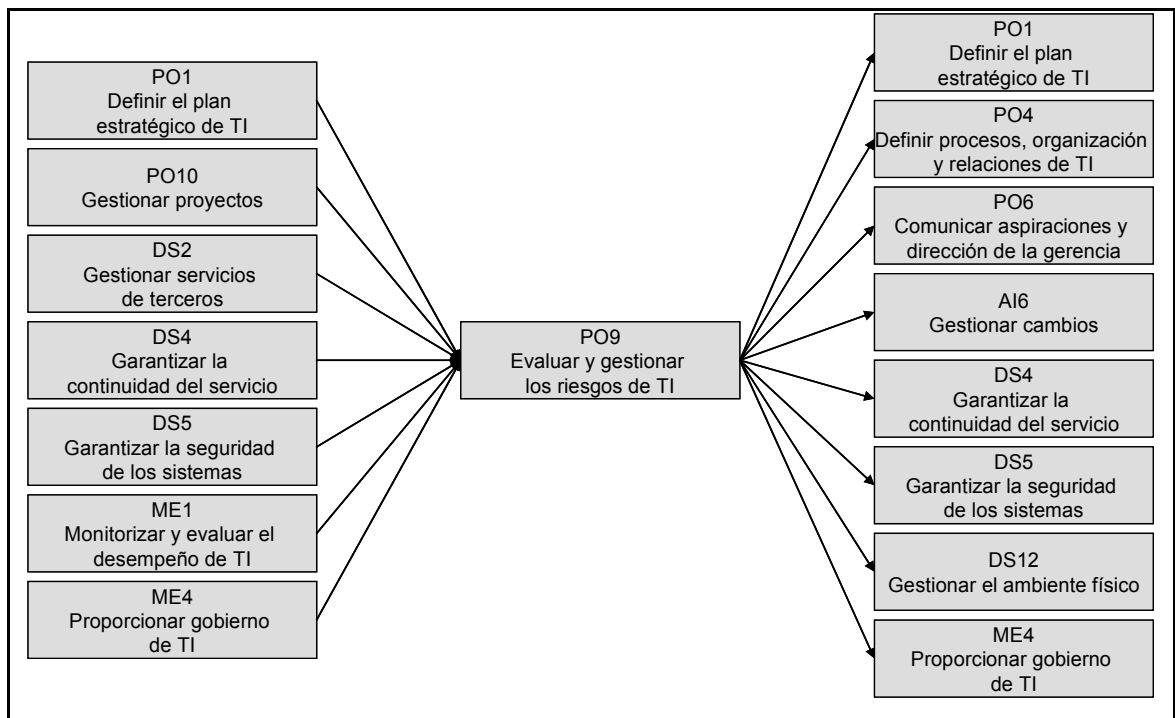


Figura 33: COBIT - Dependencias del proceso PO9

Modelo de madurez

La administración del proceso de Evaluar y administrar los riesgos de TI que satisfaga el requisito de negocio de TI de analizar y comunicar los riesgos de TI y su impacto potencial sobre los procesos y las metas de negocio es:

0 No existente cuando

La evaluación de riesgos para los procesos y las decisiones de negocio no ocurre. La organización no toma en cuenta los impactos en el negocio asociados a las vulnerabilidades de seguridad y a las incertidumbres del desarrollo de proyectos. La administración de riesgos no se ha identificado como algo relevante para adquirir soluciones de TI y para prestar servicios de TI

1 Inicial/Ad Hoc cuando

Los riesgos de TI se toman en cuenta de manera ad hoc. Se realizan evaluaciones informales de riesgos según lo determine cada proyecto. En algunas ocasiones se identifican evaluaciones de riesgos en un plan de proyectos pero se asignan a gerentes específicos con poca frecuencia. Los riesgos específicos relacionados con TI tales como seguridad, disponibilidad e integridad se toman en cuenta ocasionalmente proyecto por proyecto. Los riesgos relativos a TI que afectan las operaciones del día con día, son rara vez discutidas en reuniones gerenciales. Cuando se toman en cuenta los riesgos, la mitigación es inconsistente. Existe un entendimiento emergente de que los riesgos de TI son importantes y necesitan ser considerados.

2 Repetible pero intuitiva cuando

Existe un enfoque de evaluación de riesgos inmaduro y en evolución y se implanta a discreción de los gerentes de proyecto. La administración de riesgos se da por lo general a altos niveles y se aplica de manera típica solo a proyectos grandes o como respuesta a problemas. Los procesos de mitigación de riesgos están en implantación donde se identifican riesgos.

3 Proceso definido cuando

Una política de administración de riesgos para toda la organización define cuándo y cómo realizar las evaluaciones de riesgos. La administración de riesgos sigue un proceso definido el cual está documentado. El entrenamiento sobre administración de riesgos está disponible para todo el personal. La decisión de seguir el proceso de administración de riesgos y de recibir entrenamiento se delega a la discreción del individuo. La metodología para la evaluación de riesgos es convincente y sólida, y garantiza que los riesgos claves sean identificados. Un proceso para mitigar los riesgos clave por lo general se institucionaliza una vez que los riesgos se identifican. Las descripciones de puestos toman en cuenta las responsabilidades de administración de riesgos.

4 Administrado y medible cuando

La evaluación y administración de riesgos son procesos estándar. Las excepciones al proceso de administración de riesgos se reportan a la gerencia de TI. La administración de riesgos de TI es una responsabilidad de alto nivel. Los riesgos se evalúan y se mitigan a nivel de proyecto individual y también por lo regular se hace con respecto a la operación global de TI. La gerencia recibe notificación sobre los cambios en el ambiente de negocios y de TI que pudieran afectar de manera significativa los escenarios de riesgo relacionados con la TI. La gerencia puede monitorear la posición de riesgo y tomar decisiones informadas respecto a la exposición que está dispuesta a aceptar. Todos los riesgos identificados tienen un propietario denominado, y la alta dirección, así como la gerencia de TI han determinado los niveles de riesgo que la organización está dispuesta a tolerar. La gerencia de TI ha elaborado medidas estándar para evaluar el riesgo y para definir las proporciones riesgo/retorno. La gerencia presupuesta para que un proyecto operativo de administración de riesgos re-evalúe los riesgos de manera regular. Se establece una base de datos administrativa y parte del proceso de administración de riesgos se empieza a automatizar. La gerencia de TI toma en cuenta las estrategias de mitigación de riesgo.

5 Optimizado cuando

La administración de riesgos ha evolucionado al nivel en que un proceso estructurado está implantado en toda la organización y es bien administrado. Las buenas prácticas se aplican en toda la organización. La captura, análisis y reporte de los datos de administración de riesgos están altamente automatizados. La orientación se toma de los líderes en el campo y la organización de TI participa en grupos de interés para intercambiar experiencias. La administración de riesgos está altamente integrada en todo el negocio y en las operaciones de TI está bien aceptada, y abarca a los usuarios de servicios de TI. La dirección detectará y actuará cuando se realicen decisiones grandes de inversión, operación o de TI, sin tomar en cuenta el plan de administración de riesgos. La dirección evalúa las estrategias de mitigación de riesgos de manera continua.

Criterios de Seguridad, Normalización y Conservación de las aplicaciones utilizadas para el ejercicio de potestades. Ministerio de Administraciones Públicas, 2004.

Extracto del capítulo IV Modo de utilización:

En general unos y otros [Criterios de seguridad] vendrán determinados por la identificación y clasificación de activos a proteger y las salvaguardas ligadas al personal, que serán a su vez resultado de la gestión global de la seguridad de la información y la política de seguridad. Así mismo, su implementación en el seno de los departamentos administrativos deberá tener en cuenta: el análisis y gestión de riesgos, la seguridad física y la continuidad de los servicios exigirá el Plan de contingencias.

Extracto del capítulo 2 Gestión global de la seguridad de la información:

El análisis y gestión de riesgos se encarga de estudiar los activos, amenazas, vulnerabilidades, impactos, y riesgos que una seguridad insuficiente puede tener para la organización, así como de las salvaguardas necesarias.

Extracto del capítulo 5 Análisis y gestión de riesgos:

El proceso de análisis y gestión de riesgos constituye la tarea primera y a la vez esencial de toda actuación organizada en materia de seguridad. Permite conocer de manera rigurosa el estado de seguridad y determinar la valoración del riesgo. Es adecuado en las fases y actividades de carácter general (gestión global y política de seguridad con la implicación de la dirección) y en las de carácter específico de un determinado sistema de información (planificación, organización, implantación de salvaguardas, sensibilización, operación y mantenimiento).

NIST SP 800-53 Controles de seguridad recomendados para los sistemas de información federales.

Extracto del capítulo 3.1 Gestionando el riesgo organizacional: [NIST800-53.04]

La selección y especificación de controles de seguridad para un sistema de información se realiza como parte de un programa de seguridad que englobe toda la organización que incluya la gestión del riesgo organizacional, es decir, el riesgo asociado con la operación de un sistema de información. La gestión del riesgo organizacional es un elemento clave en el programa de seguridad de la organización y proporciona un marco de trabajo efectivo para seleccionar los controles de seguridad apropiados para un sistema de información – los controles de seguridad necesarios para proteger las operaciones y activos de la organización. Gestionar el riesgo organizacional incluye algunas actividades importantes:

- i) evaluar riesgo*
- ii) realizar análisis coste-beneficio*
- iii) seleccionar, implementar y evaluar controles de seguridad*
- iv) autorizar formalmente el uso del sistema de información (acreditación de seguridad).*

El enfoque orientado a riesgos para la selección y especificación de los controles de seguridad considera la efectividad, eficiencia y restricciones debidas a leyes, directivas, órdenes ejecutivas, políticas, estándares o regulaciones aplicables. Las siguientes actividades relacionadas con la gestión del riesgo organizacional son de suma importancia para un programa de seguridad de la información efectivo y pueden aplicarse tanto a sistemas de información nuevos y antiguos en el contexto del ciclo de vida de desarrollo de software y de la arquitectura federal:

- *Categorizar el sistema de información y la información que contenida en él mediante un análisis de impacto FIPS 199.*
- *Seleccionar un conjunto inicial de controles de seguridad (línea base) para el sistema de información basado en la categorización de seguridad FIPS 199.*
- *Ajustar (o adaptar) el conjunto inicial de controles de seguridad en base a una evaluación del riesgo y las condiciones locales, incluyendo requerimientos de seguridad específicos de la organización, información específica de amenazas, análisis coste-beneficio, la disponibilidad de controles compensatorios, o circunstancias especiales.*
- *Documentar en el plan de seguridad de sistemas el conjunto de controles de seguridad incluyendo la justificación de los ajustes realizados sobre el conjunto de controles inicial.*
- *Implementar los controles de seguridad en el sistema de información. Para sistemas antiguos, algunos o todos de los controles de seguridad seleccionados pueden estar ya implantados.*
- *Evaluar los controles de seguridad utilizando métodos apropiados y procedimientos para determinar en qué medida los controles están implantados correctamente, funcionando según su diseño, y produciendo el resultado esperado para cumplir los requerimientos de seguridad definidos para el sistema.*

- *Determinar el riesgo para los activos y la operativa de la organización debida a la planificación o el funcionamiento del sistema de información.*
- *Autorizar el uso de sistemas de información (o autorizar su continuidad en caso de sistemas antiguos) si el nivel de riesgos para la operativa y los activos de la organización es aceptable.*
- *Monitorizar y evaluar de manera continua los controles de seguridad seleccionados para los sistemas de información, incluyendo documentar los cambios producidos en el sistema, realizar análisis de impacto de seguridad de dichos cambios e informar regularmente del nivel de seguridad de seguridad del sistema a los responsables de la organización.*

ANEXO III: REQUERIMIENTOS DE SEGURIDAD

En este anexo se describen los requerimientos de seguridad básicos definidos en la metodología de análisis de riesgos y la escala a utilizar para su valoración. [MAGE06]

Definición de los requerimientos de seguridad

- Disponibilidad:
 - Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.
 - ¿Qué importancia tendría que el activo no estuviera disponible?
- Integridad de los datos:
 - Garantía de la exactitud y completitud de la información y los métodos de su procesamiento.
 - ¿Qué importancia tendría que los datos fueran modificados sin control?
- Confidencialidad de los datos:
 - Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.
 - ¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?
- Autenticidad:
 - Aseguramiento de la identidad u origen.
 - ¿Qué importancia tendría que quien accede al servicio no sea realmente quien se cree? ¿Qué importancia tendría que los datos no fueran realmente imputables a quien se cree?
- Trazabilidad:
 - Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.
 - ¿Qué importancia tendría que no quedara constancia fehaciente del uso del servicio? ¿Qué importancia tendría que no quedara constancia del acceso o modificación a los datos?

Escala de valoración de requerimientos de seguridad

Criterios de valoración		Valor				
		Crítico (10)	Alto (5)	Medio (2)	Bajo (1)	Nulo (0)
Estrategia de la Organización		Imposibilidad de seguir la estrategia fijada	Impacto grave sobre la estrategia	Impacto moderado sobre la estrategia	Impacto leve sobre la estrategia	No afecta a la estrategia de la Organización
Operaciones	Daños personales	Pérdida de varias vidas	Pérdida de una vida	Lesiones graves a una o varias personas	Daños leves a una o varias personas	No afecta a la seguridad de las personas
	Orden público	Alteración seria del orden público	Manifestaciones o presiones significativas	Protestas puntuales	Generación de malestar	No afecta al orden público
	Actividad de la Organización	Interrupción permanente de las actividades	Interrupción prolongada de las actividades	Interrupción breve de las actividades	Entorpecimiento de las actividades	No afecta a la actividad de la Organización
	Intereses comerciales (valor comercial)	Interés muy grande para la competencia	Alto interés para la competencia	Interés moderado para la competencia	Bajo interés para la competencia	Sin interés para la competencia
	Impacto sobre terceros (clientes, proveedores) (Evaluar la gravedad mediante los otros criterios)	Grave impacto para muchos terceros	Grave impacto para pocos terceros. Impacto moderado para muchos terceros	Grave impacto para un tercero. Impacto moderado para pocos terceros. Impacto leve para muchos terceros.	Impacto moderado para un tercero. Impacto leve para pocos terceros.	Impacto leve para un tercero. Sin impacto para terceros
	Relaciones internacionales	Impacto en las relaciones internacionales a alto nivel	Impacto en las relaciones internacionales a nivel diplomático	Impacto en las relaciones internacionales	Impacto leve en las relaciones internacionales	No tiene impacto en las relaciones internacionales
Información financiera y de gestión		Deficiencias materiales en la información	Deficiencias significativas en la información	Deficiencias moderadas en la información	Deficiencias leves en la información	Sin impacto sobre la información
Cumplimiento	Obligaciones legales y reglamentarias	Incumplimiento excepcionalmente grave de la ley	Incumplimiento grave de la ley	Incumplimiento moderado de la ley	Incumplimiento leve de la ley	Sin impacto sobre el cumplimiento
	Obligaciones contractuales	Incumplimiento excepcionalmente grave de obligaciones contractuales. Posible cancelación de contratos relevantes.	Incumplimiento grave de obligaciones contractuales. Posibilidad de incurrir en penalizaciones relevantes.	Incumplimiento moderado de obligaciones contractuales. Posibilidad de deterioro de las relaciones con terceros relevantes.	Incumplimiento leve de obligaciones contractuales.	Sin impacto sobre el cumplimiento

Tabla 28: Criterios de valoración de activos

ANEXO IV: TIPOS DE RECURSOS DE INFORMACIÓN

En este anexo se detallan los tipos de recursos de información incluidos en el inventario base de la metodología de análisis de riesgos. [MAGE06]

- Procesos y servicios
 - Procesos
 - Servicios internos
 - Servicios externos
- Personas
 - Directivos
 - Usuarios internos
 - Usuarios contratas
 - Administradores de sistemas
 - Clientes
 - Proveedores
 - Accionistas
 - Reguladores/supervisores
- Aplicaciones informáticas
- Software de sistemas
 - Sistemas operativos
 - Bases de datos
- Dispositivos de hardware
 - Servidores
 - Puestos de trabajo
 - Ordenadores portátiles
 - Agendas electrónicas
 - Teléfonos inteligentes
 - Impresoras
 - Scanners

- Modems
 - Hubs
 - Switches
 - Routers
- Redes de comunicaciones
 - Redes locales
 - Enlaces de telecomunicaciones
 - Redes inalámbricas
- Soportes de información
 - Papel
 - Cintas
 - Discos magnéticos
 - CD/DVD
 - Memorias flash
 - Tarjetas de memoria
 - Tarjetas inteligentes
 - Memorias internas dispositivos hardware
- Equipamiento auxiliar
 - Sistemas de alimentación eléctrica
 - Sistemas de aire acondicionado
 - Sistemas de detección/extinción de incendios
 - Sistemas de alarma
 - Sistemas de videovigilancia
 - Sistemas de control de acceso
- Sistemas Ubicaciones físicas
 - Centros de Proceso de Datos
 - Salas de equipamiento auxiliar
 - Salas de comunicaciones
 - Centros de control
 - Salas de operadores
 - Salas de usuarios

- Dispositivos de seguridad
 - IDS/IPS
 - Firewall
 - Antivirus

ANEXO V: INVENTARIO DE AMENAZAS

En este anexo se detallan las amenazas incluidas en el inventario base de la metodología de análisis de riesgos. [MAGE06]

- Desastres naturales
 - Fuego
 - Agua
 - Otros desastres naturales
- De origen industrial
 - Fuego
 - Agua
 - Contaminación mecánica
 - Contaminación electromagnética
 - Avería de origen físico o lógico
 - Corte del suministro eléctrico
 - Condiciones inadecuadas de temperatura y/o humedad
 - Fallo de servicios de comunicaciones
 - Interrupción de otros servicios y suministros esenciales
 - Degradación de los soportes de almacenamiento de la información
 - Emanaciones electromagnéticas
 - Otros desastres industriales
- De origen regulatorio
 - Incumplimiento legal
 - Incumplimiento contractual
 - Incumplimiento normativa interna
- Errores y fallos no intencionados
 - Errores de los usuarios
 - Errores del administrador
 - Errores de monitorización (log)
 - Errores de configuración

- Deficiencias en la organización
- Difusión de software dañino
- Errores de [re-]encaminamiento
- Errores de secuencia
- Escapes de información
- Alteración de la información
- Introducción de información incorrecta
- Degradación de la información
- Destrucción de información
- Divulgación de información
- Vulnerabilidades de los programas (software)
- Errores de mantenimiento / actualización de programas (software)
- Errores de mantenimiento / actualización de equipos (hardware)
- Caída del sistema por agotamiento de recursos
- Indisponibilidad del personal
- Errores y fallos intencionados
 - Manipulación de la configuración
 - Suplantación de la identidad del usuario
 - Abuso de privilegios de acceso
 - Uso no previsto
 - Difusión de software dañino
 - [Re-]encaminamiento de mensajes
 - Alteración de secuencia
 - Acceso no autorizado
 - Análisis de tráfico
 - Repudio
 - Interceptación de información (escucha)
 - Modificación de la información
 - Introducción de falsa información
 - Corrupción de la información
 - Destrucción la información

- Divulgación de información
- Manipulación de programas
- Denegación de servicio
- Robo
- Ataque destructivo
- Ocupación enemiga
- Indisponibilidad del personal
- Extorsión
- Ingeniería social

ANEXO VI: INVENTARIO DE SALVAGUARDAS

En este anexo se detallan las salvaguardas incluidas en el inventario base de la metodología de análisis de riesgos. [ISO27002.05]

- 5 – Políticas, normas y procedimientos
 - 5.1.1 - Política de seguridad de la información
 - 5.1.2 - Revisión de la política de seguridad de la información
- 6 – Organización y estructura
 - 6.1.1 - Compromiso de la dirección con la seguridad de la información
 - 6.1.2 - Coordinación de la seguridad de la información
 - 6.1.3 - Asignación de las responsabilidades de la seguridad de la información
 - 6.1.4 - Proceso de la autorización para las instalaciones de tratamiento de la información
 - 6.1.5 - Acuerdos de confidencialidad
 - 6.1.6 - Contacto con autoridades
 - 6.1.7 - Contacto con los grupos de interés especial
 - 6.1.8 - Revisión independiente de la seguridad de la información
 - 6.2.1 - Identificación de los riesgos relacionados con externos
 - 6.2.2 - Abordando la seguridad al tratar con clientes
 - 6.2.3 - Abordando la seguridad en acuerdos con terceros
- 7 – Control de activos
 - 7.1.1 - Inventario de activos
 - 7.1.2 - Propiedad de los activos
 - 7.1.3 - Uso aceptable de los activos
 - 7.2.1 - Guías de clasificación
 - 7.2.2 - Etiquetado y tratamiento de la información
- 8 – Control de empleados
 - 8.1.1 - Roles y responsabilidades
 - 8.1.2 - Investigación

- 8.1.3 - Términos y condiciones de la ocupación
- 8.2.1 - Responsabilidades de la dirección
- 8.2.2 - Conocimiento, educación, y entrenamiento en la seguridad de la información
- 8.2.3 - Proceso disciplinario
- 8.3.1 - Responsabilidades de la terminación
- 8.3.2 - Devolución de activos
- 8.3.3 - Retirada de los derechos de acceso
- 9 – Control de la seguridad física
 - 9.1.1 - Perímetro de seguridad física
 - 9.1.2 - Controles de entrada física
 - 9.1.3 - Asegurar oficinas, salas, e instalaciones
 - 9.1.4 - Protección contra amenazas externas y ambientales
 - 9.1.5 - Trabajo en áreas seguras
 - 9.1.6 - Acceso público, entrega, y áreas de carga
 - 9.2.1 - Localización y protección de equipos
 - 9.2.2 - Mantenimiento de suministros
 - 9.2.3 - Seguridad del cableado
 - 9.2.4 - Mantenimiento de los equipos
 - 9.2.5 - Seguridad de equipos fuera de los locales de la organización
 - 9.2.6 - Eliminación y re-utilización segura de equipos
 - 9.2.7 - Extracción de propiedades
- 10 – Control de las operaciones de los sistemas de información
 - 10.1.1 - Procedimientos operacionales documentados
 - 10.1.2 - Gestión del cambio
 - 10.1.3 - Segregación de tareas
 - 10.1.4 - Separación de los entornos de desarrollo, pruebas, e instalaciones operacionales
 - 10.2.1 - Entrega de servicio
 - 10.2.2 - Supervisión y revisión de los servicios de terceros
 - 10.2.3 - Gestión de cambios en servicios de terceros

- 10.3.1 - Gestión de capacidades
- 10.3.2 - Aceptación de sistemas
- 10.4.1 - Controles contra código malicioso
- 10.4.2 - Controles contra código móvil
- 10.5.1 - Copia de seguridad de la información
- 10.7.1 - Gestión de soportes extraíbles
- 10.7.2 - Eliminación de soportes
- 10.7.3 - Procedimientos de utilización de la información
- 10.7.4 - Seguridad de la documentación de sistemas
- 10.8.1 - Procedimientos y políticas de intercambio de información
- 10.8.2 - Acuerdos de intercambio
- 10.8.3 - Soportes físicos en tránsito
- 10.8.4 - Mensajería electrónica (Correo Electrónico, EDI, etc.)
- 10.8.5 - Sistemas de información de negocio
- 10.9.1 - Comercio electrónico
- 10.9.2 - Transacciones On-line
- 10.9.3 - Información pública disponible
- 10.10.1 - Registros de auditoría
- 10.10.2 - Monitorización de uso de sistemas
- 10.10.3 - Protección de información de registros
- 10.10.4 - Registros de administrador y operadores
- 10.10.5 - Registro de fallos
- 10.10.6 - Sincronización de relojes
- 11 – Control de acceso lógico
 - 11.1.1 - Política de control de acceso
 - 11.2.1 - Registro de usuario
 - 11.2.2 - Gestión de privilegios
 - 11.2.3 - Gestión de contraseñas de usuarios
 - 11.2.4 - Revisión de los derechos de usuario
 - 11.3.1 - Uso de contraseñas
 - 11.3.2 - Equipo informático de usuario desatendido

- 11.3.3 - Política de puesto de trabajo vacío
- 11.5.1 - Procedimientos de inicio de sesión segura
- 11.5.2 - Identificación y autenticación del usuario
- 11.5.3 - Sistema de gestión de contraseñas
- 11.5.4 - Uso de las utilidades del sistema
- 11.5.5 - Sesiones inactivas
- 11.5.6 - Limitación del tiempo de conexión
- 11.6.1 - Restricción de acceso a la información
- 11.6.2 - Aislamiento de sistemas sensibles
- 11.7.1 - Informática móvil
- 11.7.2 – Teletrabajo
- 10-11 – Control de las comunicaciones
 - 10.6.1 - Controles de red
 - 10.6.2 - Seguridad de servicios de red
 - 11.4.1 - Política de uso de servicios de red
 - 11.4.2 - Autenticación de usuarios por conexiones externas
 - 11.4.3 - Identificación de equipos en red
 - 11.4.4 - Protección de los puertos de diagnóstico remoto
 - 11.4.5 - Segregación de redes
 - 11.4.6 - Control de conexión a redes
 - 11.4.7 - Control de encaminamiento de la red
- 12 – Control de la adquisición, desarrollo y mantenimiento de aplicaciones
 - 12.1.1 - Análisis y especificación de requerimientos de seguridad
 - 12.2.1 - Validación de los datos de entrada
 - 12.2.2 - Control del proceso interno
 - 12.2.3 - Integridad de mensajes
 - 12.2.4 - Validación de los datos de salida
 - 12.3.1. - Política de uso de los controles criptográficos
 - 12.3.2 - Gestión de claves
 - 12.4.1 - Control del software en producción
 - 12.4.2 - Protección de los datos de prueba de sistema

- 12.4.3 - Control de acceso al código de fuente del programa
- 12.5.1 - Procedimientos de control de cambios
- 12.5.2 - Revisión técnica de las aplicaciones tras cambios en el sistema operativo
- 12.5.3 - Restricciones en cambios de paquetes de software
- 12.5.4 - Fuga de información
- 12.5.5 - Desarrollo externalizado del software
- 12.6.1 - Control de vulnerabilidades técnicas
- 13 – Gestión de los incidentes de seguridad
 - 13.1.1 - Comunicación de eventos de seguridad de la información
 - 13.1.2 - Comunicación de vulnerabilidades
 - 13.2.1 - Responsabilidades y procedimientos
 - 13.2.2 - Aprendiendo de las incidencias de seguridad de la información
 - 13.2.3 - Recogida de pruebas
- 14 – Gestión de la continuidad
 - 14.1.1 - Inclusión de la seguridad de la información en el proceso de la gestión de la continuidad del negocio
 - 14.1.2 - Continuidad del negocio y valoración del riesgo
 - 14.1.3 - Desarrollo e implementación de planes de continuidad incluyendo la seguridad de la información
 - 14.1.4 - Marco de planificación para la continuidad del negocio
 - 14.1.5 - Prueba, mantenimiento y reevaluación de los planes de continuidad
- 15 – Cumplimiento regulatorio
 - 15.1.1 - Identificación de la legislación aplicable
 - 15.1.2 - Derechos de propiedad intelectual (IPR)
 - 15.1.3 - Salvaguarda de los registros de la Organización
 - 15.1.4 - Protección de datos de carácter personal y de la intimidad de las personas

- 15.1.5 - Evitar el mal uso de los recursos de tratamiento de la información
- 15.1.6 - Reglamentación de los controles de cifrado
- 15.2.1 - Cumplimiento con políticas y estándares de seguridad
- 15.2.2 - Comprobación del cumplimiento técnica
- 15.3.1 - Controles de auditoría de sistemas de información
- 15.3.2 - Protección de las herramientas de auditoría de sistemas

ANEXO VII: HERRAMIENTAS

En este anexo se describen los tres prototipos desarrollados de la aplicación informática desarrollada para soportar la aplicación de la metodología de análisis de riesgos.

Definición de requerimientos

Un extracto de los requerimientos definidos para la aplicación se muestra a continuación:

- **Objetivos:**
 - Disponer de una herramienta que soporte el proceso de análisis de riesgos realizado según la metodología definida, teniendo en cuenta las distintas fases.
 - No es objetivo de la herramienta soportar el proceso de gestión de riesgos.
- **Actores:**
 - Gestor del riesgo: Persona encargada de la gestión de riesgo. Como tal, adapta los distintos aspectos de la metodología (Requerimientos de seguridad y escalas de valoración) y de los inventarios (Tipos de recursos, amenazas, salvaguardas y valoraciones estándar de los mismos), crea y mantiene los proyectos de análisis de riesgos, gestiona la realización de las valoraciones por los distintos evaluador y obtiene los resultados del análisis de riesgos.
 - Evaluador: Persona que conoce o controla los distintos activos y recursos de información y que disponen de una opinión cualificada acerca de su valor para el negocio (activos de información) y/o las amenazas y salvaguardas (recursos de información). La herramienta recoge, consolida y procesa las valoraciones realizadas por los evaluadores.

- Custodio / propietario: Persona con responsabilidad sobre los distintos recursos de información. La herramienta se encarga de su inventario, pero su concurso sólo es requerido si se considera evaluador.
- Director: Persona que recibe del gestor del riesgo los resultados de los análisis de riesgos realizados y los utiliza para la toma de decisiones.
- Casos de uso definidos:
 - Inventario de activos y recursos de información.
 - Valoración de activos.
 - Valoración de amenazas sobre recursos.
 - Valoración de salvaguardas generales.
 - Valoración de salvaguardas por recurso.
 - Cálculo del riesgo intrínseco.
 - Cálculo del riesgo efectivo.
 - Cálculo del riesgo residual.
- Requerimientos funcionales:
 - Inicio de sesión:
 - La aplicación presentará un formulario donde se podrán introducir el código de usuario y la contraseña propias de la aplicación.
 - La aplicación validará el código de usuario y la contraseña y sólo permitirá el acceso en caso de que sean correctos.
 - En caso de que el código de usuario y la contraseña no sean correctos se mostrará un mensaje de error y no se permitirá el acceso.
 - Bienvenida del usuario:
 - La aplicación deberá presentar una pantalla de bienvenida que contendrá información particular dependiendo del tipo de usuario que se haya conectado. En esta pantalla el usuario encontrará enlaces para:
 - Actualizar su información personal, incluyendo la contraseña.

- Desarrollar las tareas asociadas a su perfil.
 - Salir de la aplicación.
 - Acceder a la ayuda de la aplicación.
- Módulo de usuarios:
 - La aplicación dispondrá de una lista de usuarios con información general referente a:
 - Datos identificativos
 - ◆ Nombre y apellidos
 - ◆ Código de usuario
 - ◆ Contraseña (cifrada)
 - Datos de contacto
 - ◆ Dirección
 - ◆ Correo electrónico
 - ◆ Teléfono
 - Posición en la organización
 - ◆ Empresa
 - ◆ Cargo
 - Perfiles de acceso (Editables sólo por los administradores o por los gestores del riesgo responsables de cada proyecto).
 - ◆ Perfil de acceso para cada proyecto de análisis de riesgo.
 - La aplicación permitirá el alta, baja, modificación y consulta (en listado e individual) de los usuarios.
 - No se permitirá la baja de usuarios que tengan asignados perfiles en proyectos de análisis de riesgos, si bien se permitirá su bloqueo para impedir el acceso. Sólo un usuario administrador podrá bloquear y desbloquear usuarios.

- Módulo de inventarios:
 - La aplicación dispondrá de un inventario de requerimientos de seguridad, permitiendo las operaciones de alta, baja, modificación y consulta (en listado e individual).
 - Los datos que se almacenarán de cada requerimiento de seguridad serán:
 - ◆ Identificador del requerimiento de seguridad
 - ◆ Nombre descriptivo del requerimiento de seguridad.
 - No se permitirá la eliminación de requerimientos de seguridad que estén en uso en proyectos de valoración.
 - La aplicación dispondrá de un inventario de escalas de valoración, permitiendo las operaciones de alta, baja, modificación y consulta (en listado e individual).
 - Los datos que se almacenarán de cada escala de valoración serán:
 - ◆ Identificador de la escala de valoración
 - ◆ Nombre descriptivo de la escala de valoración
 - ◆ Una lista de entre 3 y 10 valores válidos de la escala, incluyendo para cada uno de ellos:
 - Posición dentro de la escala
 - Nombre corto del valor
 - Nombre descriptivo del valor
 - Descripción del valor
 - Rango (valor máximo y mínimo) cuantitativo del valor
 - Valor cuantitativo correspondiente al valor
 - No se permitirá la eliminación de escalas de valoración que estén siendo utilizadas en proyectos de análisis de riesgos.

- La aplicación dispondrá de un inventario de tipos de recurso, permitiendo las operaciones de alta, baja, modificación y consulta (en listado e individual).
 - Los datos que se almacenarán de los tipos de recurso son:
 - ◆ Identificador de tipo de recurso
 - ◆ Nombre descriptivo del tipo de recurso
 - No se permitirá la eliminación de tipos de recurso que estén asociados a recursos registrados en la aplicación.
- La aplicación dispondrá de un inventario de tipos de amenaza, permitiendo las operaciones de alta, baja, modificación y consulta (en listado e individual).
 - Los datos que se almacenarán de los tipos de amenaza son:
 - ◆ Identificador de tipo de amenaza
 - ◆ Nombre descriptivo del tipo de amenaza
 - No se permitirá la eliminación de tipos de amenaza que estén asociados a amenazas registradas en la aplicación.
- La aplicación dispondrá de un inventario de tipos de salvaguarda, permitiendo las operaciones de alta, baja, modificación y consulta (en listado e individual).
 - Los datos que se almacenarán de los tipos de salvaguarda son:
 - ◆ Identificador de tipo de salvaguarda
 - ◆ Nombre descriptivo del tipo de salvaguarda
 - No se permitirá la eliminación de tipos de salvaguarda que estén asociados a salvaguardas registradas en la aplicación.
- La aplicación dispondrá de un inventario de amenazas, permitiendo las operaciones de alta, baja, modificación y consulta (en listado e individual).
 - Los datos que se almacenarán de las amenazas son:
 - ◆ Identificador de amenaza
 - ◆ Nombre descriptivo de la amenaza

- ♦ Descripción larga de la amenaza
- ♦ Tipo de amenaza
- No se permitirá la eliminación de amenazas que estén siendo utilizadas en metodologías de análisis de riesgos.
- Se permitirá la importación de ficheros de amenazas en formato Microsoft Excel.
- La aplicación dispondrá de un inventario de salvaguardas, permitiendo las operaciones de alta, baja, modificación y consulta (en listado e individual).
 - Los datos que se almacenarán de las salvaguardas son:
 - ♦ Identificador de salvaguarda
 - ♦ Nombre descriptivo de la salvaguarda
 - ♦ Descripción larga de la salvaguarda
 - ♦ Tipo de salvaguarda
 - ♦ Tres campos de texto libre para indicar taxonomías adicionales de salvaguardas, como preventiva/detectiva, técnica/procedimental, general/específica, etc.
 - No se permitirá la eliminación de salvaguardas que estén siendo utilizadas en metodologías de análisis de riesgos.
 - Se permitirá la importación de ficheros de salvaguardas en formato Microsoft Excel.
- La aplicación dispondrá de una valoración por defecto de amenazas por tipo de recurso.
 - Se dispondrá de una tabla con todas las combinaciones posibles entre tipo de recurso, amenaza y requerimiento de seguridad, con un porcentaje de degradación asignado.
 - Se creará un requerimiento de seguridad ficticio (vacío) en que se registrará la frecuencia de realización de la amenaza sobre el tipo de recurso, en forma de porcentaje (100% = una vez al año)

- La aplicación dispondrá de una valoración por defecto de la eficacia de las salvaguardas sobre cada amenaza.
 - Se dispondrá de una tabla con todas las combinaciones posibles entre amenaza, salvaguarda y requerimiento de seguridad, con un porcentaje de eficacia en la reducción de la degradación asignado.
 - Se creará un requerimiento de seguridad ficticio (vacío) en que se registrará la eficacia en la reducción de la frecuencia de realización de la amenaza, en forma de porcentaje.
- Módulo metodologías
 - Una metodología estará formada por:
 - Un conjunto de requerimientos de seguridad asociados a una escala de valoración.
 - Un conjunto de amenazas.
 - Un conjunto de salvaguardas.
 - Todos los elementos que forman parte de la metodología serán editables, pudiéndose añadir, eliminar, modificar y consultar (en listado o individualmente).
 - No se podrán modificar elementos en metodologías que estén siendo utilizadas en proyectos de valoración.
 - Existirá una función para clonar metodologías, que permita generar una nueva metodología que sea copia de otra existente.
 - Las metodologías tendrán asociada la siguiente información:
 - Código de metodología
 - Nombre de la metodología
 - Descripción de la metodología

- Módulo de activos
 - La aplicación dispondrá de un repositorio de áreas / procesos de negocio y de soporte, permitiendo las operaciones de alta, baja, modificación y consulta (en listado e individual).
 - Los datos que se almacenarán de las áreas / procesos son:
 - ◆ Identificador de área / proceso
 - ◆ Nombre de área / proceso
 - ◆ Descripción del área / proceso
 - La aplicación dispondrá de un repositorio de activos de información, permitiendo las operaciones de alta, baja, modificación y consulta (en listado e individual).
 - Los datos que se almacenarán de los activos de información son:
 - ◆ Identificador de activo de información
 - ◆ Nombre del activo de información
 - ◆ Descripción del activo de información
 - No se permitirá la eliminación de activos de información que estén siendo utilizados en proyectos de análisis de riesgos.
 - Se permitirá la importación de ficheros de activos de información en formato Microsoft Excel.
 - La aplicación dispondrá de un repositorio de recursos de información, permitiendo las operaciones de alta, baja, modificación y consulta (en listado e individual).
 - Los datos que se almacenarán de los recursos de información son:
 - ◆ Identificador de recurso de información
 - ◆ Nombre del recurso de información
 - ◆ Descripción del recurso de información
 - ◆ Tipo de recurso de información
 - ◆ Propietario del recurso de información

- ♦ Custodio (encargado del mantenimiento) del recursos de información
 - No se permitirá la eliminación de recursos de información que estén siendo utilizados en proyectos de análisis de riesgos.
 - Se permitirá la importación de ficheros de recursos de información en formato Microsoft Excel.
- La aplicación permitirá mantener la relación de activos y recursos de información:
 - Los activos de información dispondrán de una lista de recursos de información que los soportan, desde la que se podrán añadir, eliminar, modificar y consultar (como listado e individualmente) los recursos de información relacionados.
 - Los recursos de información dispondrán de una lista de activos de información soportados, desde la que se podrán añadir, eliminar, modificar y consultar (como listado e individualmente) los activos de información relacionados.
- Módulo de valoraciones
 - La aplicación deberá permitir realizar la valoración de los activos de información teniendo en cuenta los diferentes requerimientos de seguridad definidos en la metodología a seguir.
 - El gestor de riesgos seleccionará los usuarios encargados de la valoración y les asignará permisos de valoración en el proyecto de análisis de riesgos.
 - ♦ Todos los proyectos deberán tener al menos un encargado de la valoración de los activos de información.

- La aplicación creará para cada usuario valorador una matriz con los activos seleccionados en el alcance del proyecto en las filas y los requerimientos de seguridad en las columnas.
- Por defecto, todos los activos tendrán una valoración vacía.
- Cada usuario tendrá la posibilidad de exportar/importar la matriz en formato Microsoft Excel para su tratamiento.
- Una vez cumplimentada la matriz, el usuario deberá marcarla como finalizada. Una vez marcada, no podrá hacer modificaciones sobre las valoraciones introducidas.
- El gestor de riesgos podrá marcar como finalizada o eliminar las valoraciones de cada usuario en cualquier momento.
- Una vez finalizadas todas las valoraciones, el gestor de riesgos podrá obtener el resultado de la valoración, que se calculará automáticamente como la media de los valores introducidos para cada par activo de información – requerimiento de seguridad.
- Los valores vacíos no se tendrán en cuenta en el cálculo. Si una casilla sólo presenta valores vacíos se valorará como cero.
- Una vez calculado el resultado de la valoración, no será posible crear o modificar las valoraciones.

- La aplicación deberá permitir modificar la valoración de amenazas sobre tipos de recursos de información definida por defecto.
 - El gestor de riesgos seleccionará los usuarios encargados de la valoración y les asignará permisos de valoración en el proyecto de análisis de riesgos.
 - ◆ Todos los proyectos deben tener al menos un usuario valorador de las amenazas sobre los tipos de recurso de información.
 - ◆ En caso de que se desee utilizar la valoración por defecto, el gestor de riesgos se asignará a sí mismo como evaluador y aceptará los valores dados por defecto.
 - La aplicación creará para cada usuario valorador una matriz con los tipos de recurso y las amenazas seleccionadas en la metodología en las filas y los requerimientos de seguridad en las columnas, con una columna adicional para la frecuencia.
 - Por defecto, todas las casillas tendrán la valoración por defecto definida en el inventario.
 - Cada usuario tendrá la posibilidad de exportar/importar la matriz en formato Microsoft Excel para su tratamiento.
 - Una vez cumplimentada la matriz, el usuario deberá marcarla como finalizada. Una vez marcada, no podrá hacer modificaciones sobre las valoraciones introducidas.
 - El gestor de riesgos podrá marcar como finalizada o eliminar las valoraciones de cada usuario en cualquier momento.

- Una vez finalizadas todas las valoraciones, el gestor de riesgos podrá obtener el resultado de la valoración, que se calculará automáticamente como la media de los valores introducidos para cada tupla tipo de recurso de información – amenaza – requerimiento de seguridad (más la frecuencia).
- Los valores vacíos no se tendrán en cuenta en el cálculo. Si una casilla sólo tiene valores vacíos se valorará como cero.
- Una vez calculado el resultado de la valoración, no será posible crear o modificar las valoraciones.
- La aplicación deberá permitir valorar las amenazas sobre los recursos de información considerados en un proyecto de análisis de riesgos.
 - El gestor de riesgos seleccionará los usuarios encargados de la valoración y les asignará permisos de valoración en el proyecto de análisis de riesgos.
 - ◆ Todos los proyectos deben tener al menos un usuario valorador de las amenazas sobre los recursos de información.
 - ◆ En caso de que se desee utilizar una valoración genérica, el gestor de riesgos se asignará a sí mismo como evaluador y aceptará los valores dados por defecto.
 - La aplicación creará para cada usuario valorador una matriz con los recursos seleccionados en el proyecto de análisis de riesgos y las amenazas seleccionadas en la metodología en las filas y los requerimientos de seguridad en las columnas, con una columna adicional para la frecuencia.

- Por defecto, todas las casillas tendrán la valoración por defecto definida en la valoración genérica de amenazas sobre los tipos de recurso de información, calculada utilizando el tipo de recurso de información correspondiente.
- Cada usuario tendrá la posibilidad de exportar/importar la matriz en formato Microsoft Excel para su tratamiento.
- Una vez cumplimentada la matriz, el usuario deberá marcarla como finalizada. Una vez marcada, no podrá hacer modificaciones sobre las valoraciones introducidas.
- El gestor de riesgos podrá marcar como finalizada o eliminar las valoraciones de cada usuario en cualquier momento.
- Una vez finalizadas todas las valoraciones, el gestor de riesgos podrá obtener el resultado de la valoración, que se calculará automáticamente como la media de los valores introducidos para cada tupla recurso de información – amenaza – requerimiento de seguridad (más la frecuencia).
- Los valores vacíos no se tendrán en cuenta en el cálculo. Si una casilla sólo tiene valores vacíos se valorará como cero.
- Una vez calculado el resultado de la valoración, no será posible crear o modificar las valoraciones.

- La aplicación deberá permitir modificar la valoración de la eficacia de las salvaguardas sobre cada amenaza definida por defecto en el inventario.
 - El gestor de riesgos seleccionará los usuarios encargados de la valoración y les asignará permisos de valoración en el proyecto de análisis de riesgos.
 - ◆ Todos los proyectos deben tener al menos un usuario valorador de la eficacia de las salvaguardas sobre las amenazas.
 - ◆ En caso de que se desee utilizar la valoración por defecto, el gestor de riesgos se asignará a sí mismo como evaluador y aceptará los valores dados por defecto.
 - La aplicación creará para cada usuario valorador una matriz con las amenazas y salvaguardas seleccionadas en la metodología en las filas y los requerimientos de seguridad en las columnas, con una columna adicional para la frecuencia.
 - Por defecto, todas las casillas tendrán la valoración por defecto definida en el inventario.
 - Cada usuario tendrá la posibilidad de exportar/importar la matriz en formato Microsoft Excel para su tratamiento.
 - Una vez cumplimentada la matriz, el usuario deberá marcarla como finalizada. Una vez marcada, no podrá hacer modificaciones sobre las valoraciones introducidas.
 - El gestor de riesgos podrá marcar como finalizada o eliminar las valoraciones de cada usuario en cualquier momento.

- Una vez finalizadas todas las valoraciones, el gestor de riesgos podrá obtener el resultado de la valoración, que se calculará automáticamente como la media de los valores introducidos para cada tupla amenaza – salvaguarda - requerimiento de seguridad (más la frecuencia).
- Los valores vacíos no se tendrán en cuenta en el cálculo. Si una casilla sólo tiene valores vacíos se valorará como cero.
- Una vez calculado el resultado de la valoración, no será posible crear o modificar las valoraciones.
- La aplicación deberá permitir valorar la implantación de las distintas salvaguardas consideradas en la metodología de análisis de riesgos.
 - El gestor de riesgos seleccionará los usuarios encargados de la valoración y les asignará permisos de valoración en el proyecto de análisis de riesgos.
 - ◆ Todos los proyectos deben tener al menos un usuario valorador de las salvaguardas.
 - La aplicación creará para cada usuario valorador una matriz con las salvaguardas seleccionadas en la metodología en las filas y cinco columnas con el porcentaje de implementación para seis escenarios de valoración. La primera columna representará la situación actual y las restantes representarán cinco escenarios adicionales.
 - Por defecto, todas las casillas tendrán el valor vacío.
 - Cada usuario tendrá la posibilidad de exportar/importar la matriz en formato Microsoft Excel para su tratamiento.
 - Una vez cumplimentada la matriz, el usuario deberá marcarla como finalizada. Una vez marcada, no podrá hacer modificaciones sobre las valoraciones introducidas.

- El gestor de riesgos podrá marcar como finalizada o eliminar las valoraciones de cada usuario en cualquier momento.
- Una vez finalizadas todas las valoraciones, el gestor de riesgos podrá obtener el resultado de la valoración, que se calculará automáticamente como la media de los valores introducidos para cada salvaguarda.
- Los valores vacíos no se tendrán en cuenta en el cálculo. Si una casilla sólo tiene valores vacíos se valorará como cero.
- Una vez calculado el resultado de la valoración, no será posible crear o modificar las valoraciones.
- La aplicación deberá permitir valorar las salvaguardas implantadas en los recursos de información considerados en un proyecto de análisis de riesgos.
 - El gestor de riesgos seleccionará los usuarios encargados de la valoración y les asignará permisos de valoración en el proyecto de análisis de riesgos.
 - ◆ Todos los proyectos deben tener al menos un usuario valorador de las salvaguardas implantadas en los recursos de información.
 - ◆ En caso de que se desee utilizar una valoración genérica, el gestor de riesgos se asignará a sí mismo como evaluador y aceptará los valores dados por defecto.
 - La aplicación creará para cada usuario valorador una matriz con los recursos seleccionados en el proyecto de análisis de riesgos y las salvaguardas seleccionadas en la metodología en las filas y los requerimientos de seguridad en las columnas, con una columna adicional para la frecuencia.

- Por defecto, todas las casillas tendrán la valoración por defecto definida en la valoración genérica de salvaguardas, calculada utilizando la salvaguarda correspondiente.
- Cada usuario tendrá la posibilidad de exportar/importar la matriz en formato Microsoft Excel para su tratamiento.
- Una vez cumplimentada la matriz, el usuario deberá marcarla como finalizada. Una vez marcada, no podrá hacer modificaciones sobre las valoraciones introducidas.
- El gestor de riesgos podrá marcar como finalizada o eliminar las valoraciones de cada usuario en cualquier momento.
- Una vez finalizadas todas las valoraciones, el gestor de riesgos podrá obtener el resultado de la valoración, que se calculará automáticamente como la media de los valores introducidos para cada tupla recurso de información – salvaguarda – requerimiento de seguridad (más la frecuencia).
- Los valores vacíos no se tendrán en cuenta en el cálculo. Si una casilla sólo tiene valores vacíos se valorará como cero.
- Una vez calculado el resultado de la valoración, no será posible crear o modificar las valoraciones.
- Módulo de análisis
 - Los proyectos de análisis de riesgos constarán de:
 - Una metodología (ver definición en el módulo de metodología)
 - Un conjunto de activos de información y de recursos de información obtenidos del inventario de activos (ver módulo de activos)
 - Las relaciones de dependencia entre los activos y los recursos seleccionados.

- Permisos de usuario para la realización de las distintas valoraciones.
 - Datos generales de la valoración: fecha, descripción, alcance, responsable, objetivo, etc.
 - Una vez realizada la valoración de activos y de amenazas, la aplicación utilizará la información obtenida para realizar el cálculo del riesgo intrínseco por activo de información y por recurso de información.
 - Una vez calculado el riesgo intrínseco y valoradas las salvaguardas, el sistema utilizará la información obtenida para calcular el riesgo efectivo.
 - Una vez calculado el riesgo intrínseco se puede repetir el cálculo con los cinco escenarios de implantación de salvaguardas definidos en el módulo de valoraciones. Esto permitirá calcular el riesgo residual para cada uno de dichos escenarios.
 - El gestor de riesgos podrá crear, modificar, eliminar y consultar (como listado o individualmente) los proyectos de análisis de riesgos.
- Módulo de reporting
 - El sistema deberá mostrar informes y gráficos con los resultados de los análisis realizados. Estos informes serán:
 - Riesgo intrínseco
 - ◆ Listado del riesgo intrínseco por activo
 - ◆ Listado del riesgo intrínseco por activo desglosado por requerimiento de seguridad
 - ◆ Gráfico de barras de riesgo intrínseco por activo
 - ◆ Gráfico de barras de riesgo intrínseco por activo desglosado por requerimiento de seguridad

- ♦ Mapa de riesgos por activos, sobre la matriz de activos (por filas) y requerimientos de seguridad (por columnas), con un código semafórico cuyos umbrales serán configurables por el usuario en la propia pantalla, utilizando por defecto los percentiles 33 y 66.
- ♦ Mapa de riesgos por recursos.
- ♦ Mapa de riesgos por activos, con las amenazas.
- ♦ Mapa de riesgos por recursos, con las amenazas.
- Riesgo efectivo
 - ♦ Las mismas gráficas e informes que con el riesgo intrínseco.
 - ♦ Gráfico de radar con la implantación de las salvaguardas (media).
 - ♦ Gráfico de radar con la implantación de las salvaguardas (desglosado).
- Riesgo residual
 - ♦ Las mismas gráficas que con el riesgo efectivo, para cada escenario.
 - ♦ Gráfico de radar con la implantación de las salvaguardas en cada escenario.
- Los informes deberán exportarse en formato Microsoft Word.
- Las tablas deberán exportarse en formato Microsoft Excel.
- Los gráficos deberán exportarse al portapapeles de Windows como imagen.
- Requerimientos no funcionales:
 - Autenticación:
 - El sistema deberá usar un mecanismo de autenticación basado en usuario y contraseña.
 - Las contraseñas deberán almacenarse y transmitirse siempre cifradas.

- El código de usuario se bloqueará tras 3 intentos de acceso fallidos consecutivos.
- Los usuarios dispondrán de una utilidad para modificar su contraseña.
- El usuario administrador podrá actualizar la contraseña de los usuarios en caso de olvido o bloqueo.
- Control de acceso:
 - La aplicación dispondrá de control de acceso por perfiles.
 - Los usuarios recibirán permisos de acceso a cada proyecto de análisis de riesgos mediante perfiles.
 - Los perfiles determinarán las funciones autorizadas a cada usuario en cada proyecto:
 - ◆ Perfil administrador: Acceso completo a la aplicación.
 - ◆ Perfil gestor del riesgo: Acceso completo a los proyectos de análisis de riesgos.
 - ◆ Perfil evaluador: Acceso a las evaluaciones activadas por el gestor del riesgo.
 - ◆ Perfil consulta: Acceso en modo consulta a las evaluaciones realizadas y a los resultados del análisis de riesgos.
- Idioma:
 - El sistema deberá poder usar diferentes idiomas y se deberá poder cambiar el idioma del interfaz en cualquier momento.
 - Inicialmente debe estar en español e inglés pero debe poderse portar a diferentes idiomas simplemente editando un XML o similar.
- Arquitectura:
 - El sistema deberá funcionar basado en arquitectura Web.

- Personalización.
 - El sistema deberá ser altamente personalizable, especialmente en los aspectos relacionados con la metodología de análisis de riesgos.
 - Las estructuras fijas deben ser las mínimas imprescindibles, siendo preferible la utilización de tablas para la parametrización de todos los aspectos de la aplicación.
- Facilidad de uso.
 - El sistema deberá ser fácil de utilizar para usuarios que no estén familiarizados con el análisis de riesgos.
 - Todas las funcionalidades se mostrarán al usuario en un orden lógico según la metodología de análisis de riesgos.
 - La aplicación dispondrá de una funcionalidad de ayuda que permitirá el acceso en línea al manual.
 - La aplicación pedirá confirmación en todas las operaciones que supongan eliminación de datos.
 - La aplicación no mostrará a los usuarios las opciones que tenga deshabilitadas por su perfil.
 - Se utilizarán desplegados en todos los campos que procedan de otras tablas y/o que tengan que mantener la integridad referencial, para facilitar la introducción de información por parte del usuario.

Prototipo funcional

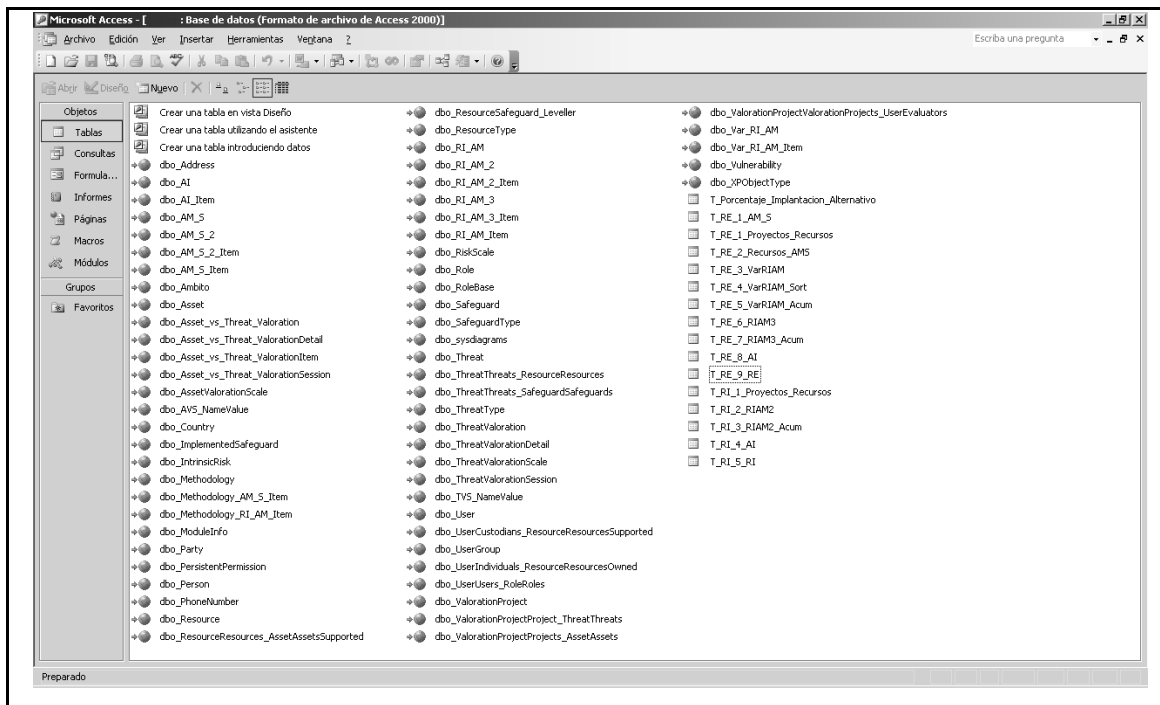


Figura 34: Prototipo funcional - Modelo de datos

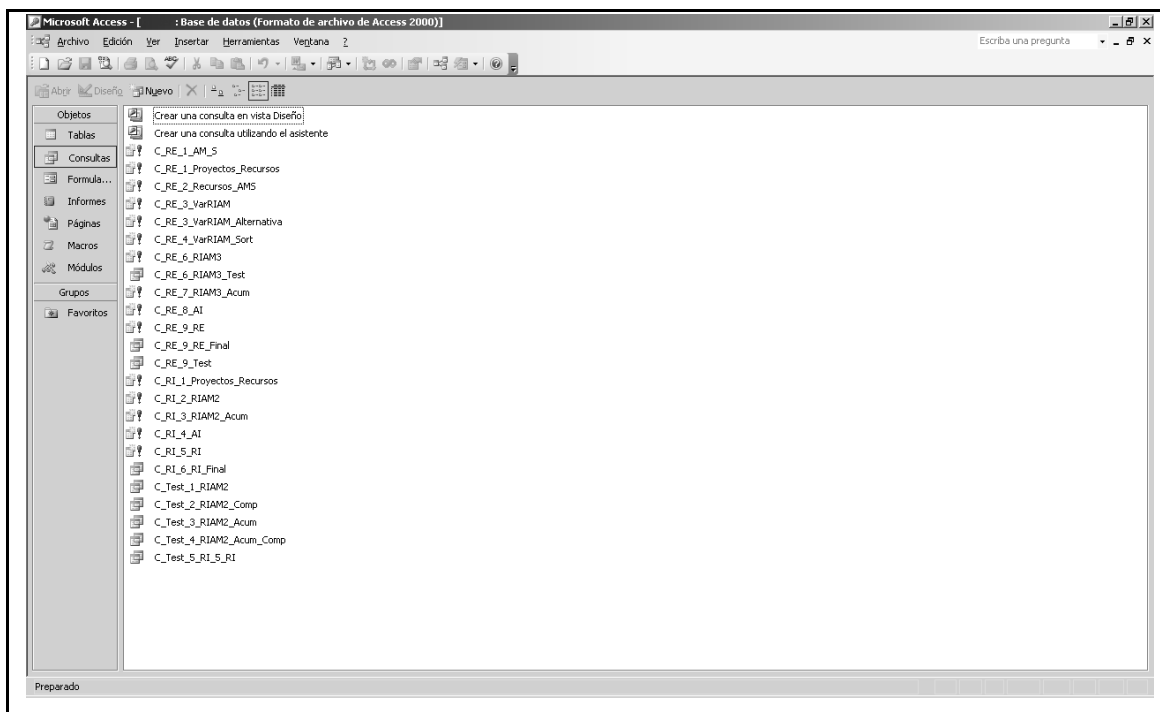


Figura 35: Prototipo funcional – Operaciones

Macro para el cálculo del riesgo intrínseco:

Acción	Consulta/Función	Vista	Modo de datos
OpenQuery	C_RI_1_Proyectos_Recursos	Hoja de datos	Modificar
OpenQuery	C_RI_2_RIAM2	Hoja de datos	Modificar
OpenQuery	C_RI_3_RIAM2_Acum	Hoja de datos	Modificar
OpenQuery	C_RI_4_AI	Hoja de datos	Modificar
OpenQuery	C_RI_5_RI	Hoja de datos	Modificar
OpenQuery	C_RI_6_RI_Final	Hoja de datos	Modificar

Tabla 29: Macro para el cálculo del riesgo intrínseco

Macro para el cálculo del riesgo efectivo:

Acción	Consulta/Función	Vista	Modo de datos
OpenQuery	C_RE_1_AM_S	Hoja de datos	Modificar
OpenQuery	C_RE_1_Proyectos_Recursos	Hoja de datos	Modificar
OpenQuery	C_RE_2_Recursos_AMS	Hoja de datos	Modificar
OpenQuery	C_RE_3_VarRIAM	Hoja de datos	Modificar
OpenQuery	C_RE_4_VarRIAM_Sort	Hoja de datos	Modificar
RunCode	M_RE_5_VarRIAM ()		
OpenQuery	C_RE_6_RIAM3	Hoja de datos	Modificar
OpenQuery	C_RE_7_RIAM3_Acum	Hoja de datos	Modificar
OpenQuery	C_RE_8_AI	Hoja de datos	Modificar
OpenQuery	C_RE_9_RE	Hoja de datos	Modificar
OpenQuery	C_RE_9_RE_Final	Hoja de datos	Modificar

Tabla 30: Macro para el cálculo del riesgo efectivo

Prototipo de demostración

Identificación de Activos

Identificación de Activos → Dominios de Riesgo para Procesos de Negocio → Cálculo de Riesgo Intrínseco → Identificación Controles y Salvaguardas → Cálculo de Riesgo Efectivo → Mapa de Riesgos → Plan de Gestión del Riesgo

Inventario de Activos de Información

Activo: Descripción:

Área de Negocio: Responsable Activo:

Plataforma Tecnológica: Tipo de Activo:

Confidencialidad: Integridad: Disponibilidad:

Auditabilidad: No Repudio: Regulatorio:

Buscar Limpiar

Identificador	Nombre	Descripción	Área Negocio	Plataforma	Tipo de Activo	Confidencialidad	Integridad	Disponibilidad	Auditabilidad	No Repudio	Regulatorio
1	Producto	Características...	Área Técnica	Externo	Información	No Aplica	Crítica	Alto	Total	Ninguno	Alto
9	Usuario Internet	Usuario y contr...	Oficina Virtual	HOST	Información	Confidencial	Crítica	Alto	Total	Interno	Alto
13	Ficheros	Ficheros envía...	Plataforma Inte...	Middleware U...	Información	Confidencial	Alta	Crítica	Total	Interno	Alto
14	Fuentes Extern...	Información pr...	Gestión de Mer...	Middleware U...	Información	Pública	Alta	Crítica	Total	Ninguno	Medio
73	Activo de Prueba		Área Técnica	Externo	Servicios	Secreta	Crítica	Alto	Total	Destino	Alto
74	Wigo										

Importar Activos Modificar Activo Borrar Activo Nuevo Activo Responsable Aprobación: Fecha Aprobación:

Figura 36: Prototipo de demostración - Inventario de activos

Cálculo del Riesgo Intrínseco

Identificación de Activos → Dominios de Riesgo para Procesos de Negocio → Cálculo de Riesgo Intrínseco → Identificación Controles y Salvaguardas → Cálculo de Riesgo Efectivo → Mapa de Riesgos → Plan de Gestión del Riesgo

Valoración del Impacto

Dominio: Dominio 3

Activos Dominio

Nombre	Tipo
Incidenias	Información
BITÁCORA	Información

Requerimientos de Seguridad

Requerimiento	Valor	Vulnerabilidad
Confidencialidad	Confidencial	6
Integridad	Alto	2
Disponibilidad	Crítica	6
Auditabilidad	Total	7
No Repudio	Interno	8

Recalcular

Amenaza	Vulnerabilidad	Ocurrencia	Percepción Probabil...	Impacto Medio	Impacto Máximo	Riesgo Medio	Riesgo Máximo
Suplantación o en...	6.7	2.3	3.9	4.0	9.0	1.6	3.5
Ataques intrusivos ...	6.0	8.1	7.0	5.0	9.0	3.5	6.3
Acceso lógico no a...	5.8	2.3	3.7	3.0	5.0	1.1	1.9
Acceso físico no aut...	4.7	8.3	6.2	5.0	8.0	3.1	5.0
Accidentes de orige...	2.0	5.1	3.2	0.0	0.0	0.0	0.0
Ausencia de trazabi...	7.5	3.9	5.4	3.0	9.0	1.6	4.9
Averías de origen fi...	2.0	7.4	3.8	0.0	0.0	0.0	0.0
Indisponibilidad de ...	2.0	6.1	3.5	1.0	7.0	0.4	2.5
Envío erróneo de inf...	5.7	1.9	3.3	3.0	8.0	1.0	2.6
Errores en la utiliza...	4.0	3.4	3.7	2.0	6.0	0.7	2.2

Evaluación Riesgo Valorar Impacto

Figura 37: Prototipo de demostración - Valoración de amenazas

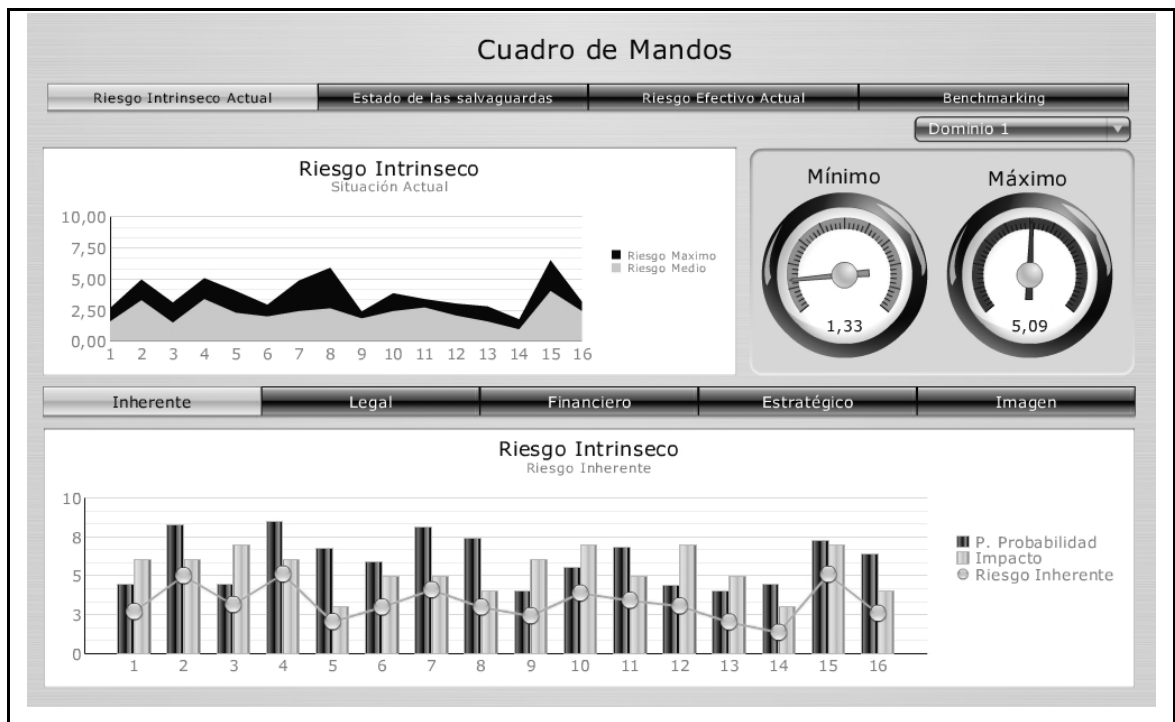


Figura 38: Prototipo de demostración – Generación de informes

Versión final

Usuario

Contraseña

✓ Aceptar
✗ Cancelar

Figura 39: Aplicación final - Autenticación de usuarios

Módulo usuarios

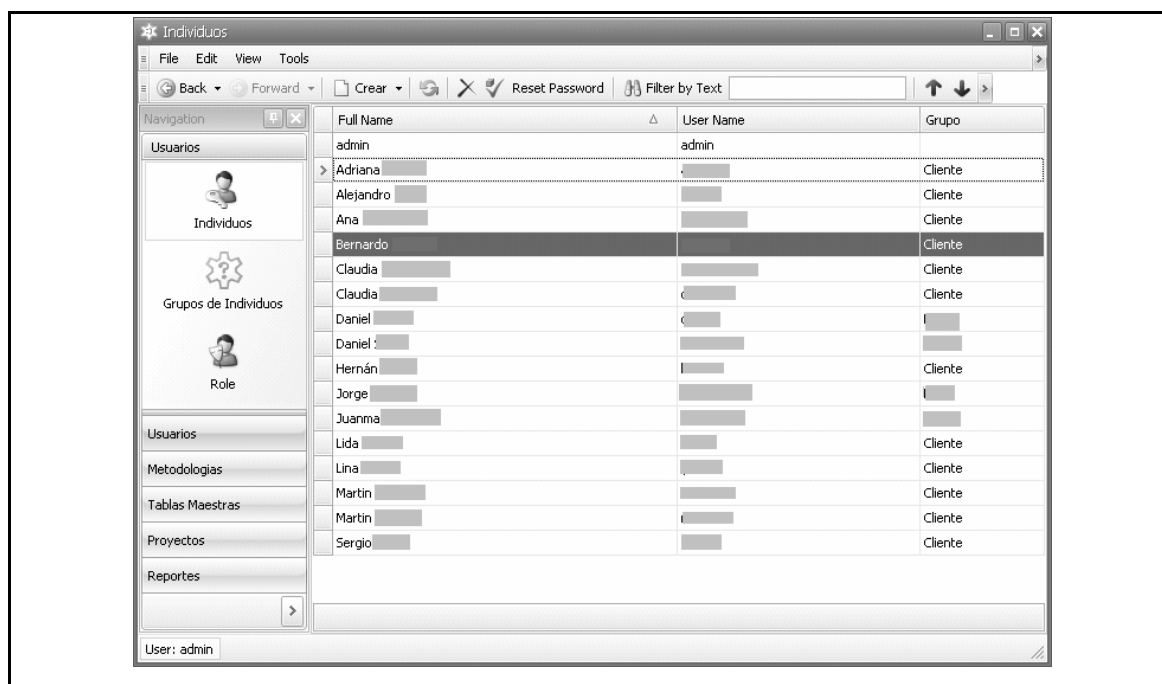


Figura 40: Aplicación final - Gestión de usuarios

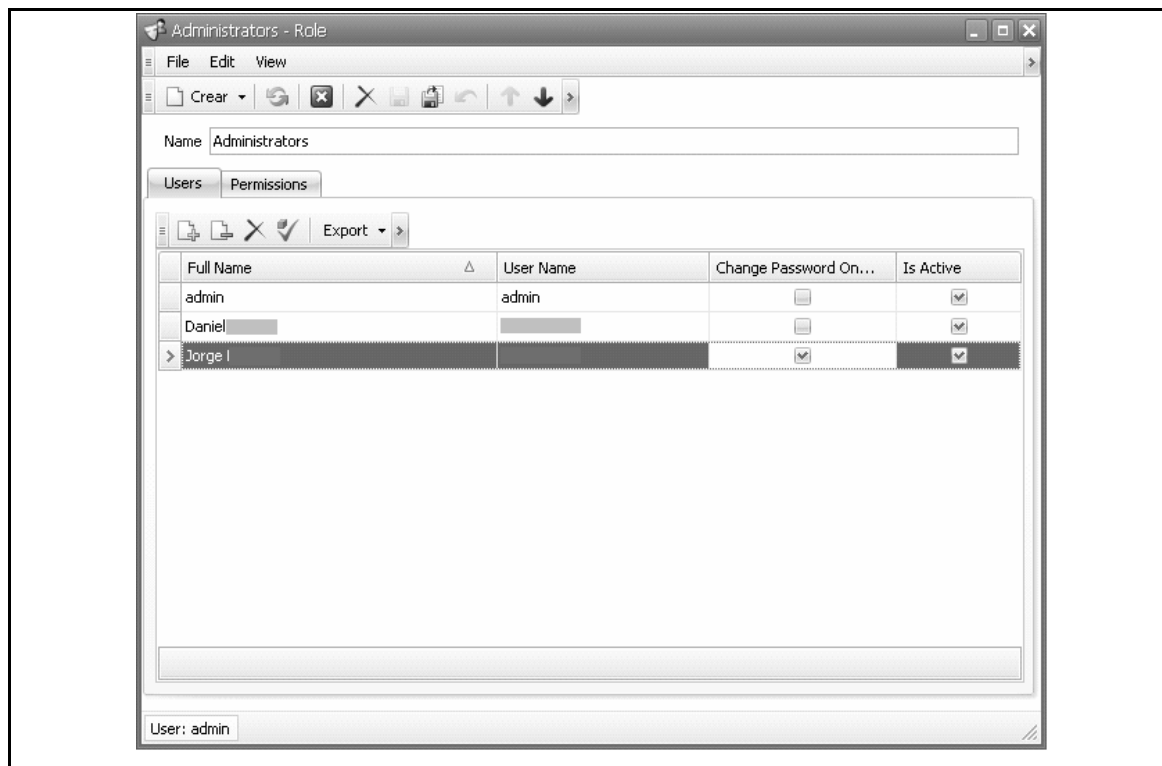


Figura 41: Aplicación final - Gestión de perfiles

Módulo inventarios

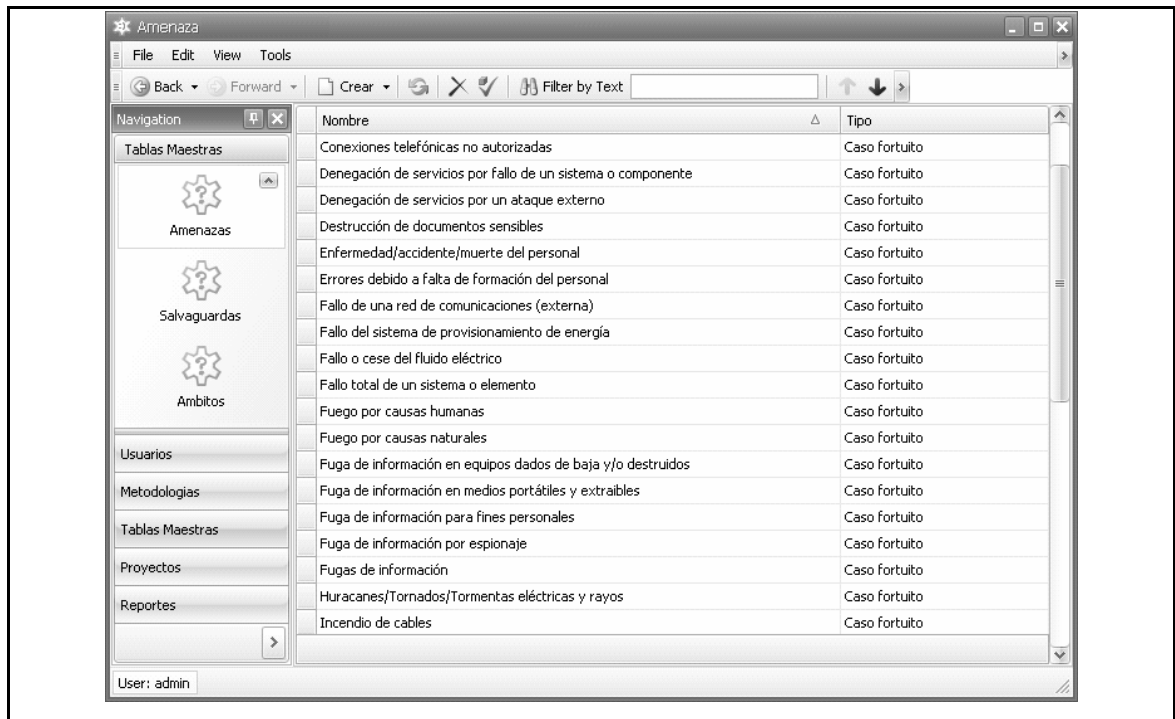


Figura 42: Aplicación final - Inventario de amenazas

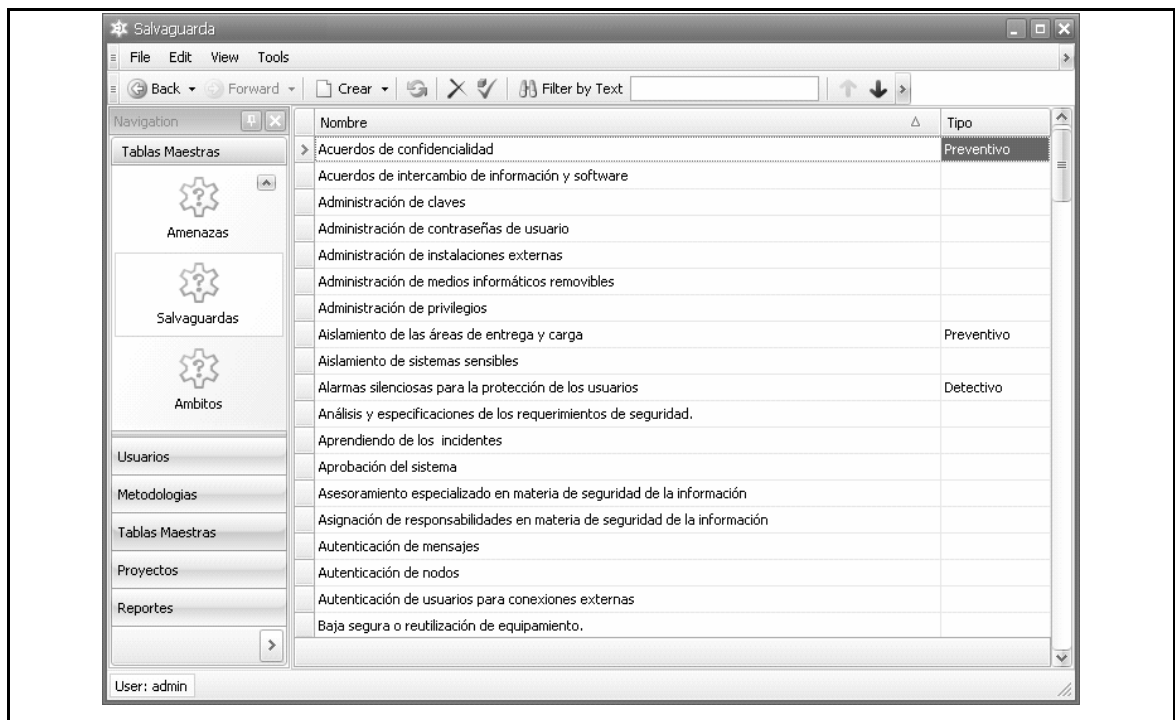


Figura 43: Aplicación final - Inventario de salvaguardas

Módulo metodologías

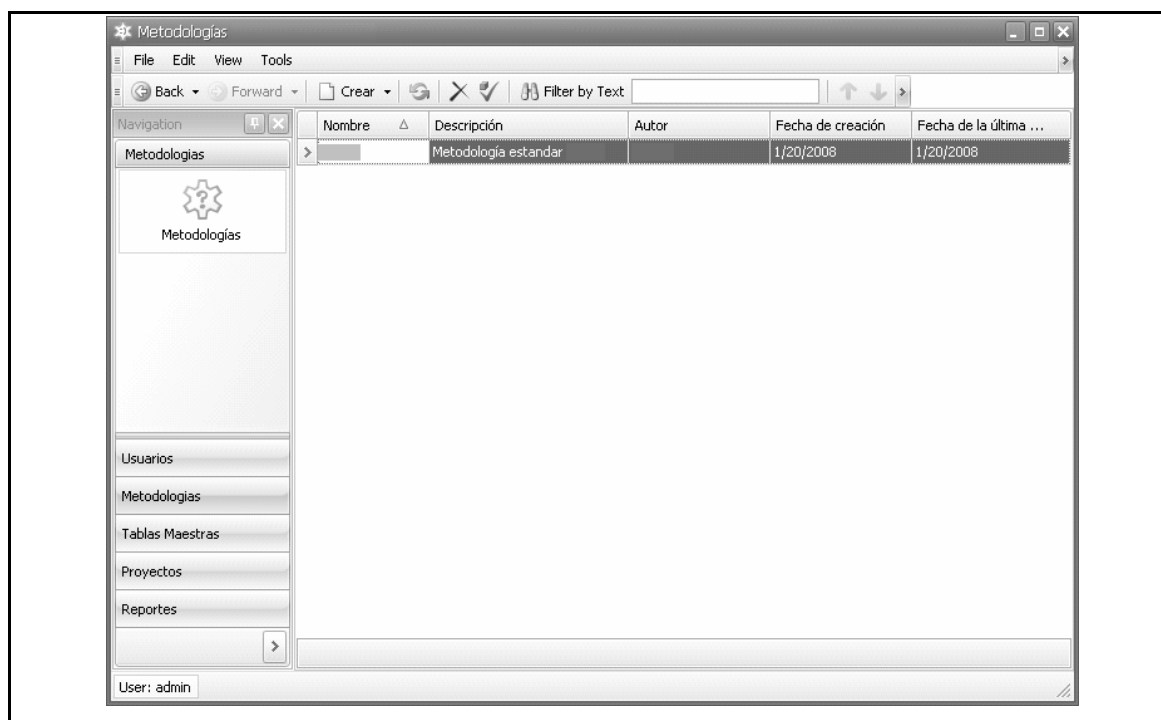


Figura 44: Aplicación final - Gestión de metodologías

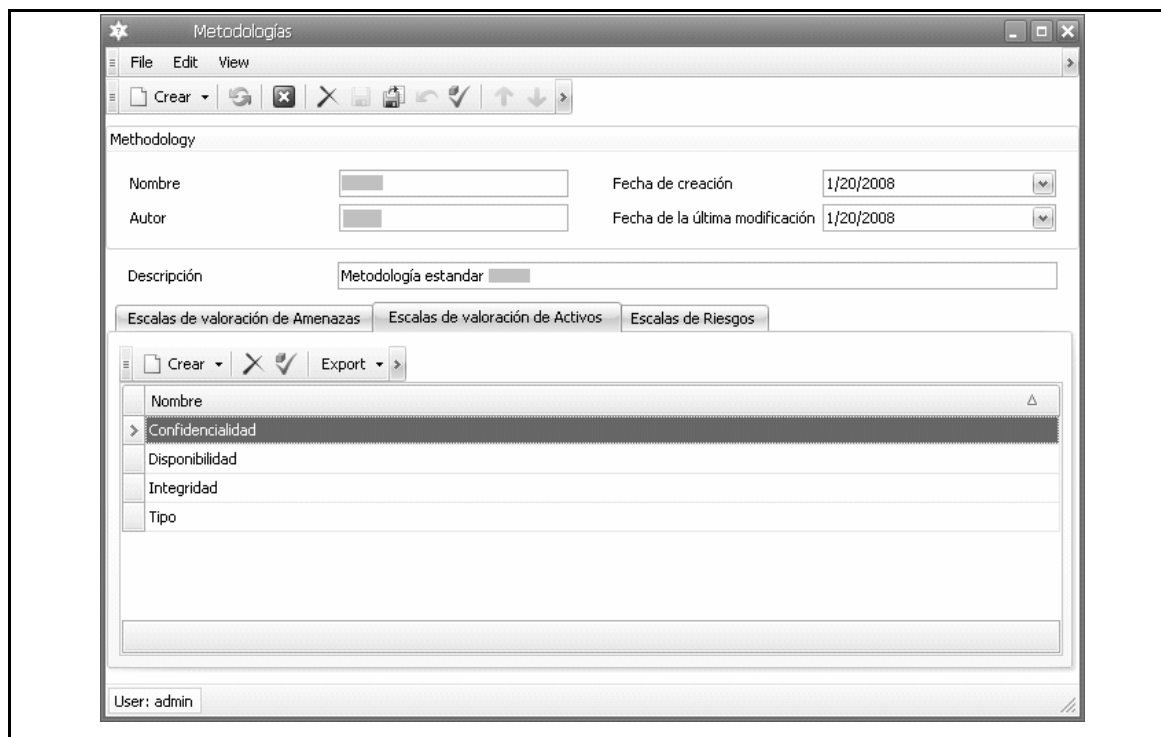


Figura 45: Aplicación final - Gestión de requerimientos de seguridad

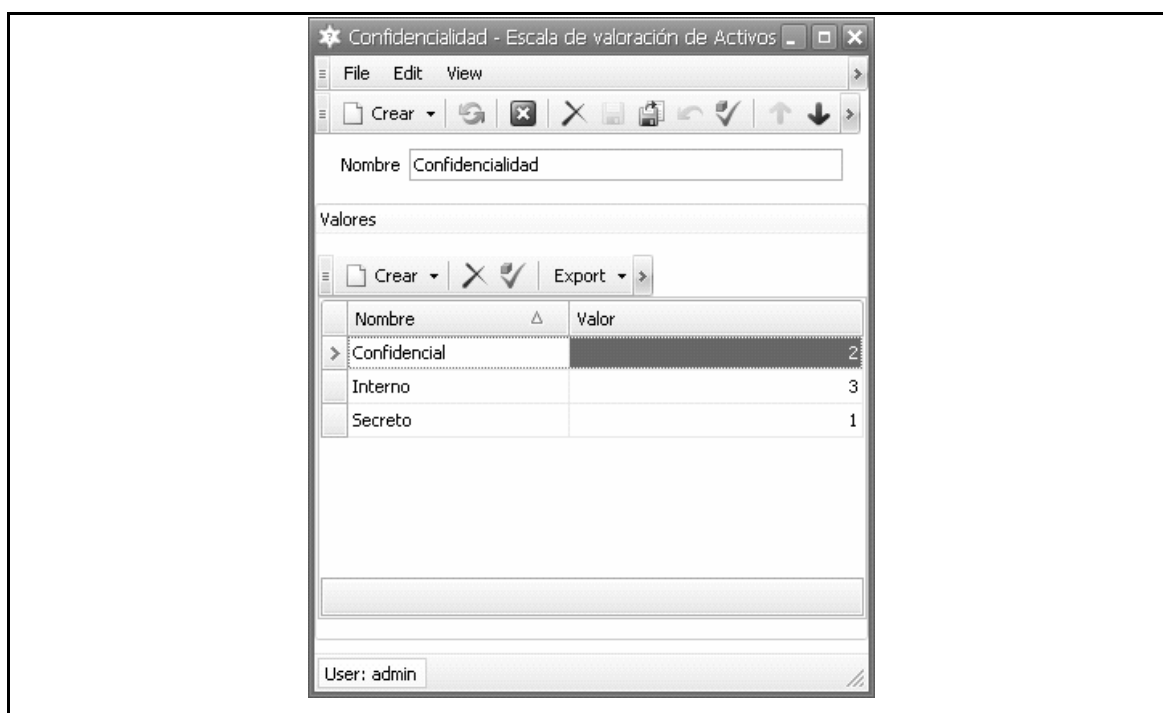


Figura 46: Aplicación final - Gestión de escalas de valoración

Módulo activos

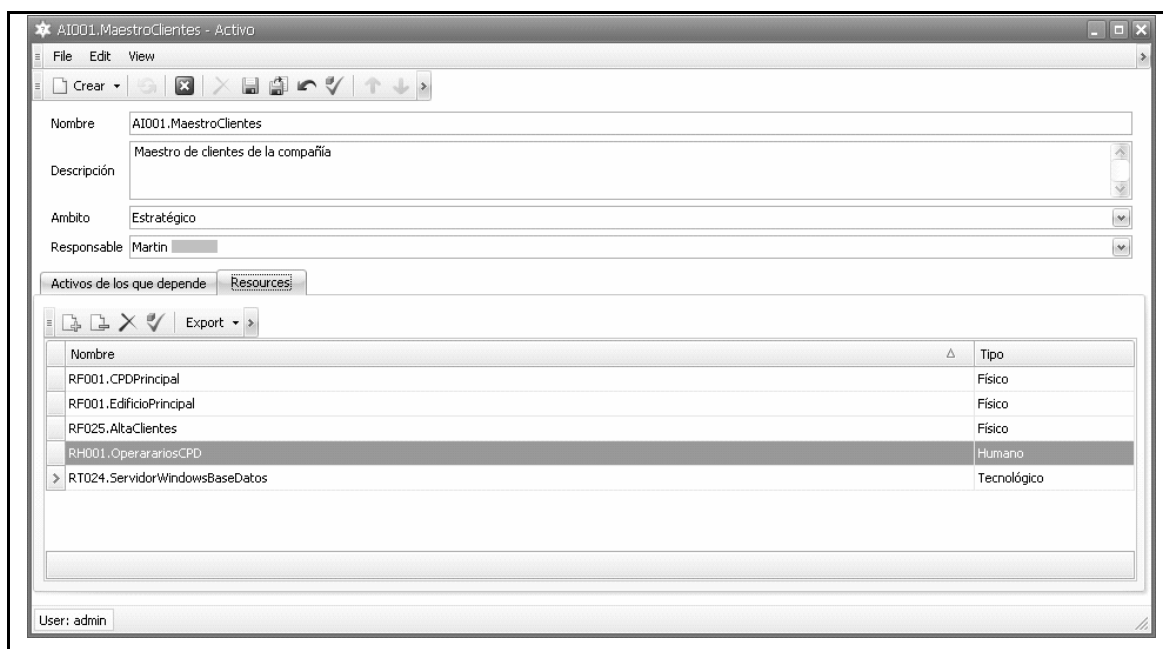


Figura 47: Aplicación final - Inventario de activos

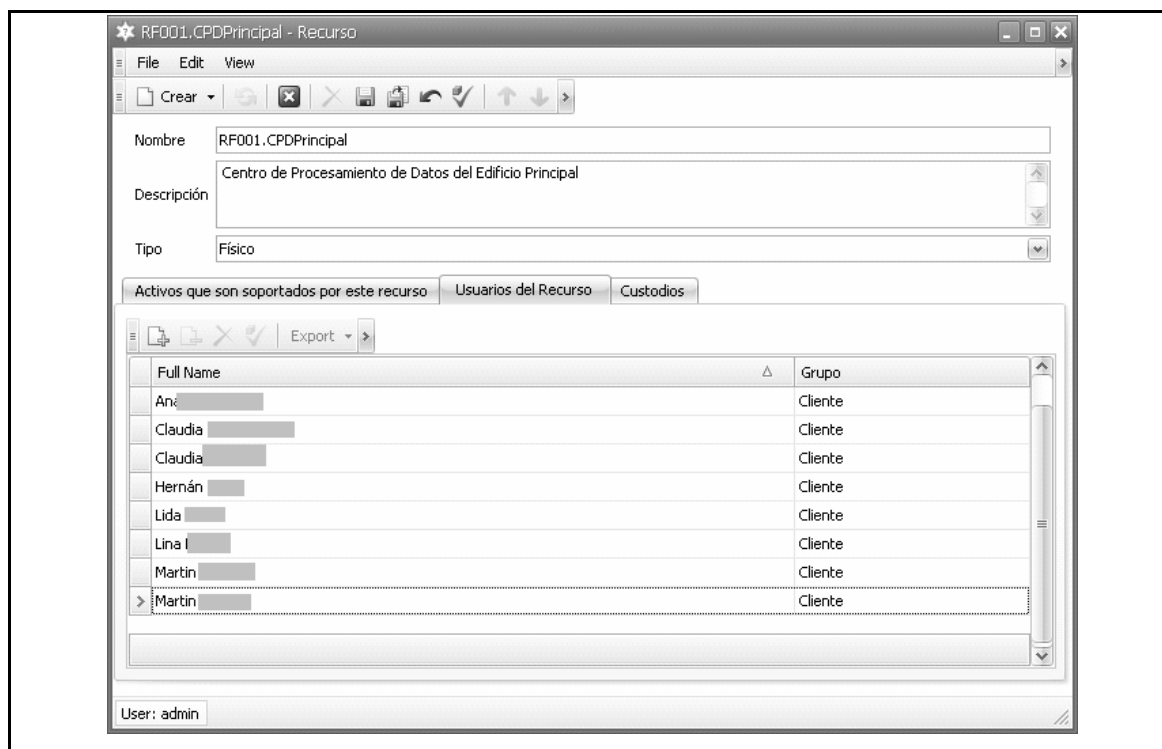


Figura 48: Aplicación final - Inventario de recursos

Módulo análisis

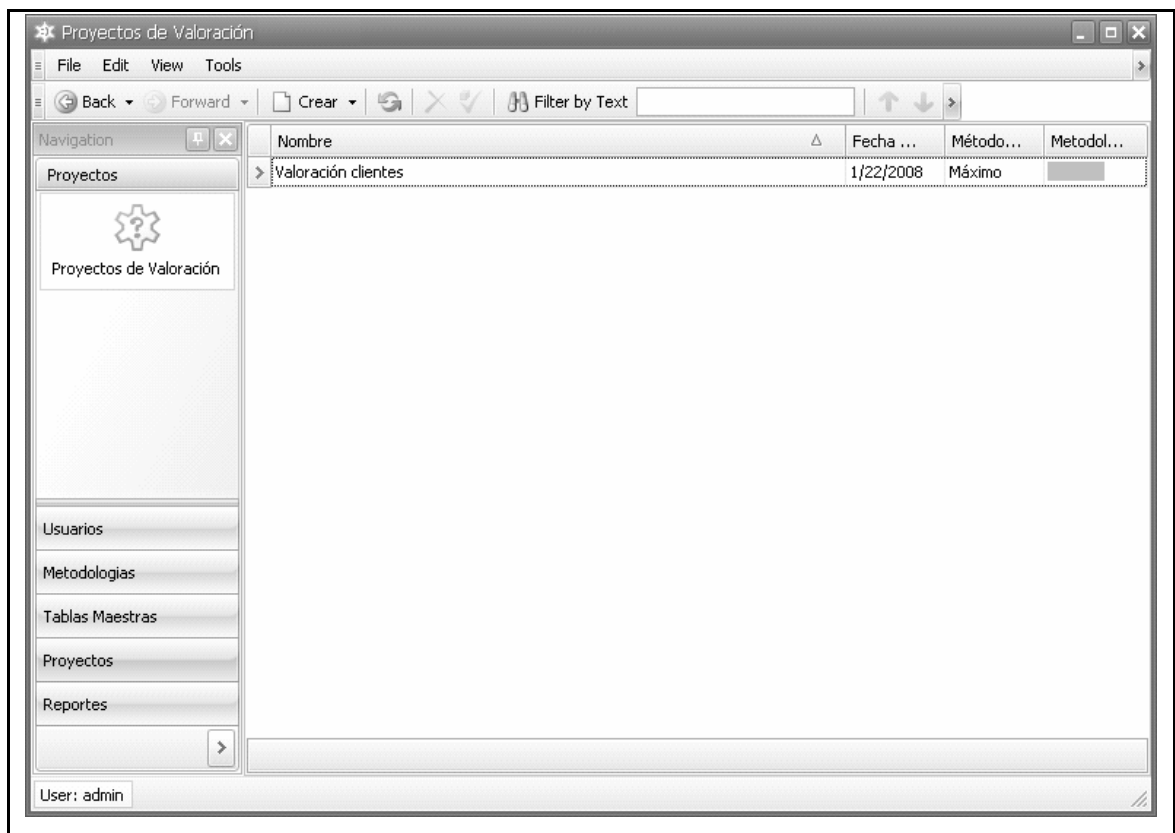


Figura 49: Aplicación final - Gestión de proyectos de análisis de riesgos

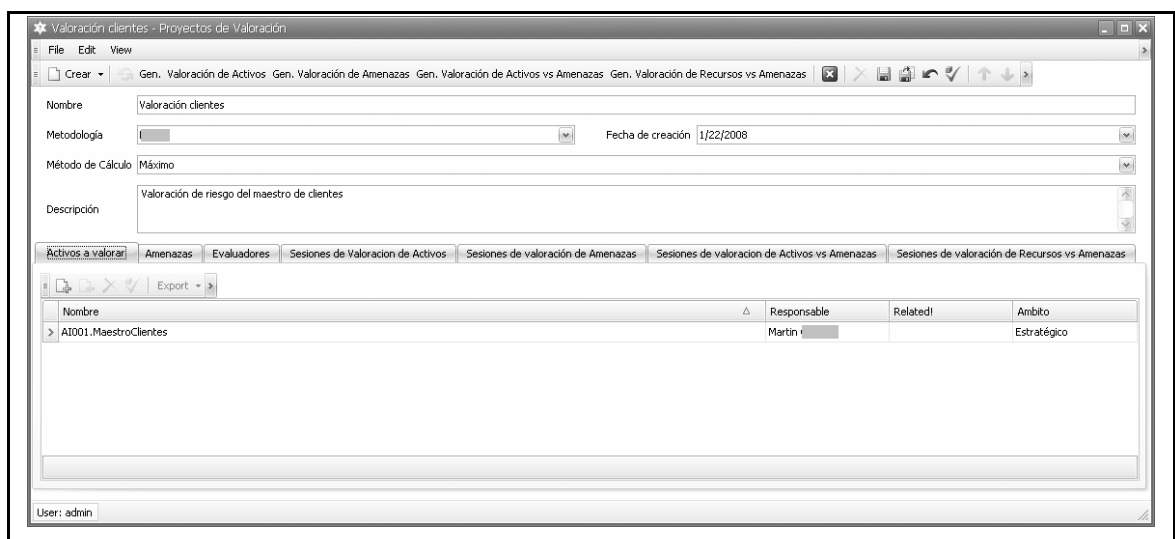


Figura 50: Aplicación final - Proyecto de análisis de riesgos

Módulo valoraciones

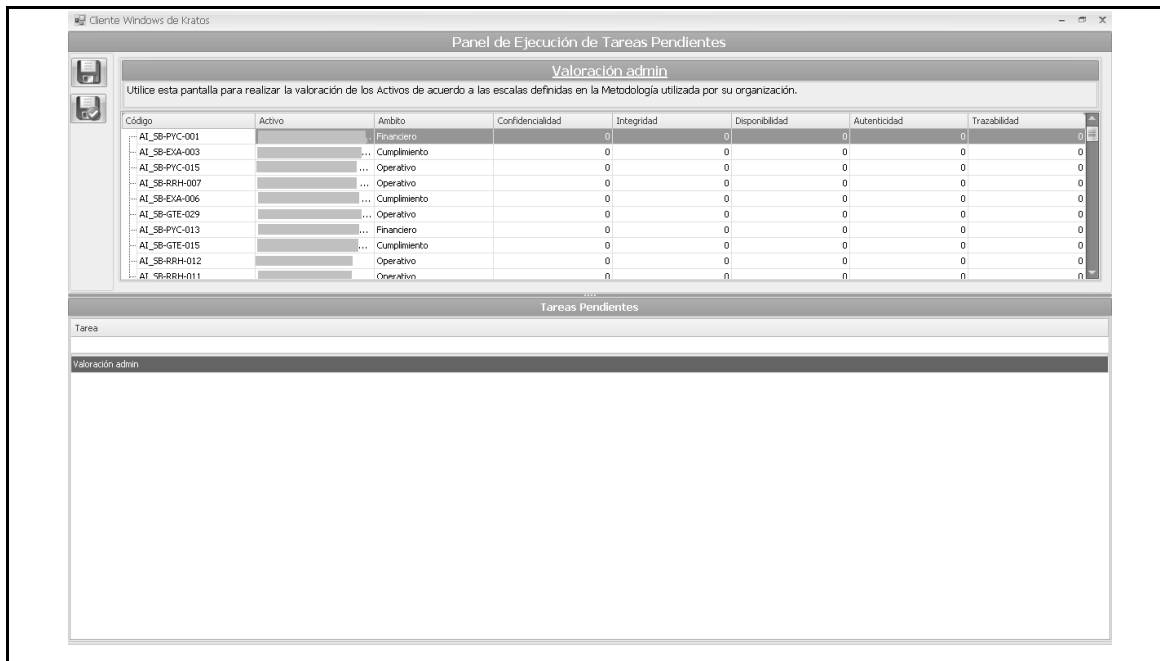


Figura 51: Aplicación final - Valoración de activos

Módulo reporting

Riesgo Intrínseco

Exportar

Riesgo Intrínseco Gráfica

Mostrar detalles

Código	Activo	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
AI_SB-GTE-004		943,67	539,26	1.095,80	181,55	200,67
AI_SB-EXA-001		631,27	733,20	440,10	200,80	203,52
AI_SB-RRH-010		702,92	807,90	890,93	216,25	132,19
AI_SB-GTE-018		943,67	1.078,51	547,90	363,10	200,67
AI_SB-PYC-011		259,53	1.178,32	1.230,15	323,30	390,95
AI_SB-PYC-012		270,14	436,37	352,85	107,90	99,83
AI_SB-EXA-003		631,27	733,20	660,15	200,80	203,52
AI_SB-GTE-024		631,27	733,20	440,10	301,20	101,76
AI_SB-GTE-015		633,37	734,55	458,70	301,80	103,46
AI_SB-IYS-005		420,85	488,80	440,10	200,80	101,76
AI_SB-GTE-019		631,27	733,20	440,10	301,20	101,76
AI_SB-PYC-005		1.045,64	884,57	983,54	324,60	395,65
AI_SB-GTE-003		1.415,50	1.617,77	1.643,69	363,10	200,67
AI_SB-RRH-008		631,27	488,80	660,15	200,80	101,76
AI_SB-GTE-029		784,23	884,57	983,54	243,45	98,91
AI_SB-GTE-016		352,67	652,91	389,23	159,90	64,20
AI_SB-GTE-021		228,08	248,85	269,59	102,45	53,38
AI_SB-GTE-013		270,14	327,28	352,85	53,95	66,55
AI_SB-EXA-007		1.415,50	1.617,77	1.095,80	363,10	200,67
AI_SB-PYC-019		519,06	883,74	615,08	242,48	97,74
AI_SB-GTE-022		356,43	435,82	429,85	107,25	65,38

Figura 52: Aplicación final - Informe de riesgo intrínseco

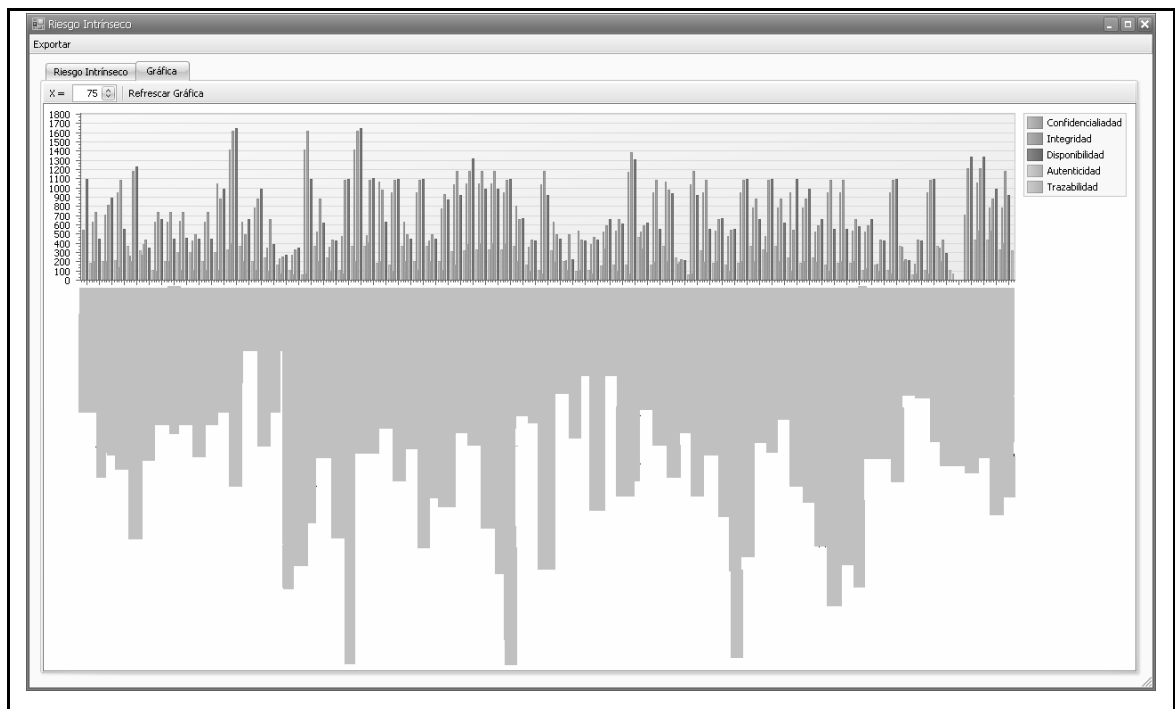


Figura 53: Aplicación final - Gráfico de riesgo intrínseco

Riesgo Efectivo		Mostrar detalles				
Código	Activo	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
AI_SB-GTE-004	...	4,48	2,01	5,08	0,82	1,02
AI_SB-EXA-001	...	3,00	2,73	2,04	0,91	1,03
AI_SB-RRH-010	...	3,34	3,01	4,13	0,98	0,67
AI_SB-GTE-018	...	4,48	4,02	2,54	1,64	1,02
AI_SB-PYC-011	...	1,23	4,39	5,70	1,46	1,98
AI_SB-PYC-012	...	1,28	1,63	1,64	0,49	0,51
AI_SB-EXA-003	...	3,00	2,73	3,06	0,91	1,03
AI_SB-GTE-024	...	3,00	2,73	2,04	1,36	0,52
AI_SB-GTE-015	...	3,01	2,74	2,13	1,36	0,52
AI_SB-IYS-005	...	2,00	1,82	2,04	0,91	0,52
AI_SB-GTE-019	...	3,00	2,73	2,04	1,36	0,52
AI_SB-PYC-005	...	4,96	3,30	4,56	1,47	2,01
AI_SB-GTE-003	...	6,72	6,03	7,62	1,64	1,02
AI_SB-RRH-008	...	3,00	1,82	3,06	0,91	0,52
AI_SB-GTE-029	...	3,72	3,30	4,56	1,10	0,50
AI_SB-GTE-016	...	1,67	2,43	1,80	0,72	0,33
AI_SB-GTE-021	...	1,08	0,93	1,25	0,46	0,27
AI_SB-GTE-013	...	1,28	1,22	1,64	0,24	0,34
AI_SB-EXA-007	...	6,72	6,03	5,08	1,64	1,02
AI_SB-PYC-019	...	2,46	3,30	2,85	1,09	0,50
AI_SB-GTE-022	...	1,69	1,63	1,99	0,48	0,33
AI_SB-GTE-007	...	2,24	4,02	5,08	1,64	1,02
AI_SB-EXA-002	...	6,72	6,03	7,62	1,64	2,04
AI_SB-EXA-005	...	2,27	4,04	5,12	0,82	1,02
AI_SB-RRH-002	...	5,06	3,66	2,89	0,72	0,49
AI_SB-EXA-004	...	4,48	4,02	5,08	1,64	1,02
AI_SB-EXA-006	...	3,00	1,82	2,04	0,91	0,52
AI_SB-EXA-009	...	4,48	4,02	5,08	1,64	1,02
AI_SB-GTE-020	...	2,00	1,82	2,04	0,91	0,52
AI_SB-GTE-027	...	3,69	3,45	4,03	1,39	0,85
AI_SB-PYC-007	...	4,93	4,39	4,28	1,46	1,98
AI_SB-PYC-006	...	4,96	4,40	6,08	1,47	2,01
AI_SB-PYC-009	...	4,96	4,40	4,56	1,47	2,01

Figura 54: Aplicación final - Informe riesgo efectivo

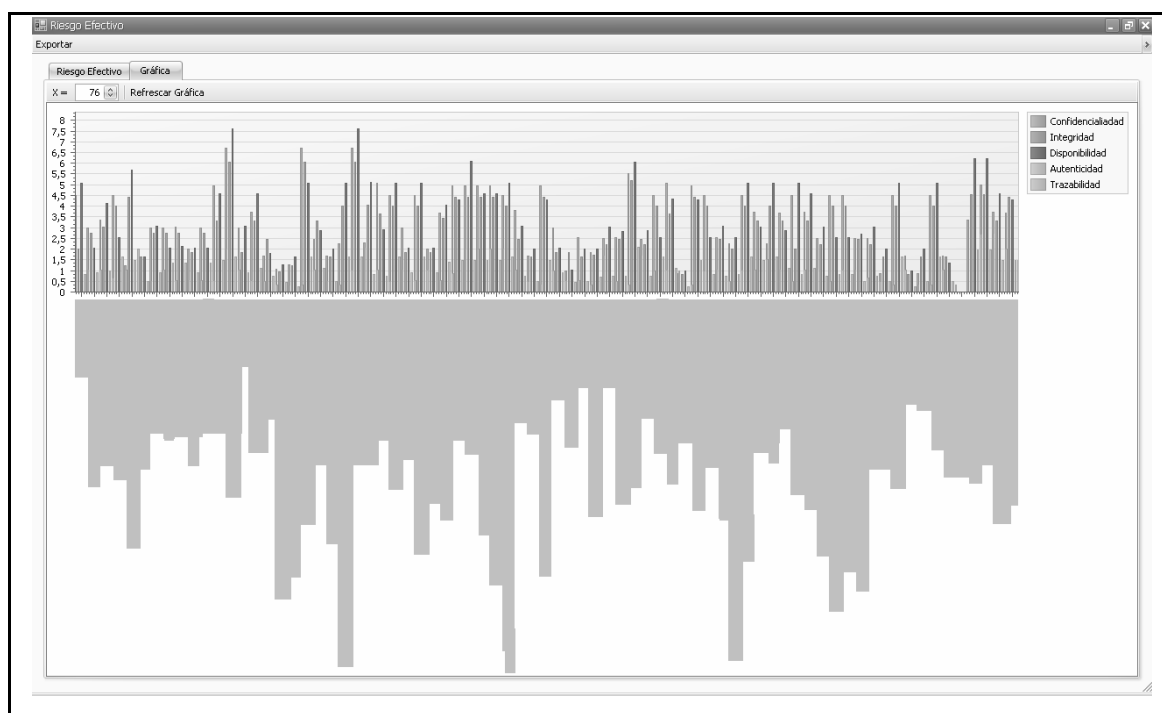


Figura 55: Aplicación final - Gráfico riesgo efectivo

ANEXO VIII: CUESTIONARIOS

En este anexo se describen los cuestionarios desarrollados para soportar la toma de datos para la aplicación de la metodología de análisis de riesgos.

Documentación Análisis de Riesgos de Seguridad de la Información																																					
Identificación de Activos de Información																																					
xxxxx – Análisis de Riesgos de Seguridad de la Información																																					
<table><tr><td>Proyecto:</td><td colspan="2">xxxxx</td><td>Descripción:</td><td colspan="2">Análisis de Riesgos de Seguridad de la Información</td></tr><tr><td>Código:</td><td colspan="2">xxxxx-xxx-000-01</td><td>Fecha emisión:</td><td>xx/xx/xxxx</td><td>Versión:</td><td>01</td></tr><tr><td>Responsable:</td><td colspan="5">Gestión de Riesgos Tecnológicos</td></tr><tr><td>Elaborado por:</td><td colspan="5">AAAAA</td></tr><tr><td>Revisado por:</td><td colspan="5">BBBBB</td></tr><tr><td>Aprobado por:</td><td colspan="5">CCCCC</td></tr></table>	Proyecto:	xxxxx		Descripción:	Análisis de Riesgos de Seguridad de la Información		Código:	xxxxx-xxx-000-01		Fecha emisión:	xx/xx/xxxx	Versión:	01	Responsable:	Gestión de Riesgos Tecnológicos					Elaborado por:	AAAAA					Revisado por:	BBBBB					Aprobado por:	CCCCC				
Proyecto:	xxxxx		Descripción:	Análisis de Riesgos de Seguridad de la Información																																	
Código:	xxxxx-xxx-000-01		Fecha emisión:	xx/xx/xxxx	Versión:	01																															
Responsable:	Gestión de Riesgos Tecnológicos																																				
Elaborado por:	AAAAA																																				
Revisado por:	BBBBB																																				
Aprobado por:	CCCCC																																				

Figura 56: Cuestionarios - Portada

	Código XXXXX-XXX-000-01	Tipo Cuestionario	Versión 01	Fecha emisión xx/xx/xxxx	Página 2 / 14
	Descripción Identificación de Activos de Información				

CONTROL DE DOCUMENTACIÓN

LISTA DE DISTRIBUCIÓN

Destinatario	Ámbito del destinatario

CONTROL DE CAMBIOS DEL DOCUMENTO

Ver.	Fecha	Descripción cambios	Páginas afectadas
01	26/03/2007	1ª versión	Todas

CONTROL DE FIRMAS DEL DOCUMENTO

Elaborado por	Revisado por	Aprobado por
AAAAA	BBBBB	CCCCC
Firma	Firma	Firma
Fecha	Fecha	Fecha

Figura 57: Cuestionarios - Control de documentación

	Código XXXXX-XXX-000-01	Tipo Cuestionario	Versión 01	Fecha emisión xx/xx/xxxx	Página 3 / 14
	Descripción Identificación de Activos de Información				

ÍNDICE	
--------	--

1. OBJETIVO	4
2. DESCRIPCIÓN GENERAL	5
3. ORGANIZACIÓN.....	6
4. PROCESOS DE NEGOCIO	7
5. ACTIVOS DE INFORMACIÓN / DATOS.....	8
6. RECURSOS DE INFORMACIÓN	9
7. ANEXO I: DOCUMENTACIÓN	10
8. ANEXO II: VALORACIÓN	11
9. ANEXO III: RECURSOS DE INFORMACIÓN.....	12
10. ANEXO IV: AMENAZAS.....	13
11. ANEXO V: TIPOS DE CONTROLES.....	14

Gestión de Riesgos Tecnológicos	Fecha Impresión : 09/04/09
---------------------------------	----------------------------

Figura 58: Cuestionarios - Índice

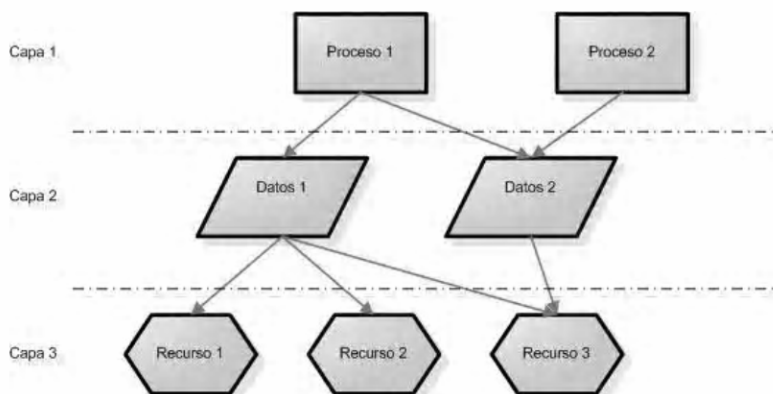
	Código XXXXX-XXX-000-01	Tipo Cuestionario	Versión 01	Fecha emisión xx/xx/xxxx	Página 4 / 14
	Descripción Identificación de Activos de Información				

1. OBJETIVO

El objetivo de este cuestionario es identificar los **activos de información** necesarios para el funcionamiento de los procesos críticos de negocio y sus requisitos de seguridad. Esta información es necesaria para realizar el análisis de los riesgos a los que éstos se ven sometidos.

Como **activo de información** entendemos cualquier información valiosa para la compañía, sin importar el medio en que se almacene, procese o comunique.

A continuación se describe gráficamente la relación entre los diferentes elementos involucrados en este análisis:



La metodología para la identificación de los activos de información relevantes para el análisis se puede resumir en los siguientes pasos:

- En primer lugar se realiza una identificación de los **procesos de negocio** de cada compañía, unidad o departamento, y se seleccionan los procesos que se consideran críticos.
- En segundo lugar, para aquellos procesos considerados críticos se identifican los **activos de información** necesarios para el correcto funcionamiento del proceso, y cuáles son sus requerimientos de seguridad.
- En tercer lugar, se identifican los **recursos de información** que se utilizan para el manejo (adquisición, almacenamiento, tratamiento, salida) de los activos de información, sean tecnológicos (aplicaciones, sistemas, bases de datos, etc.) o de otros tipos (personas, servicios, soporte papel, etc.)

Figura 59: Cuestionarios - Objetivo

	Código XXXXX-XXX-000-01	Tipo Cuestionario	Versión 01	Fecha emisión xx/xx/xxxx	Página 5 / 14
	Descripción Identificación de Activos de Información				

2. DESCRIPCIÓN GENERAL

Por favor, incluya aquí una descripción general de la compañía/unidad/departamento, incluyendo:

- Ubicación en la estructura organizativa del Grupo xxxxxxxx
- Misión

Figura 60: Cuestionarios - Descripción general

	Código XXXXX-XXX-000-01	Tipo Cuestionario	Versión 01	Fecha emisión xx/xx/xxxx	Página 6 / 14
	Descripción Identificación de Activos de Información				

3. ORGANIZACIÓN

Por favor, describa en el siguiente cuadro la organización de la compañía, unidad o departamento.

Si dispone de documentación relativa a la organización (Por ejemplo: organigrama, descripción de puestos de trabajo, etc.), por favor, indíquelo en el anexo I de este documento.

Id.	Unidad organizativa ¹	Descripción/Funciones
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		

¹ **Unidad organizativa:** Dirección, gerencia, área, unidad, departamento, grupo, etc.

Figura 61: Cuestionarios - Organización

Código	XXXXX-XXX-000-01	Tipo	Cuestionario	Versión	01	Fecha emisión	xx/xx/xxxx	Página	7 / 14
Descripción		Identificación de Activos de Información							

4. PROCESOS DE NEGOCIO

Por favor, indique en el siguiente cuadro los procesos de negocio necesarios para el cumplimiento de la misión de la compañía, unidad o departamento. Las casillas sombreadas incluyen un ejemplo de la cumplimentación de los datos solicitados.

Si dispone de documentación relativa a estos procesos de negocio (Por ejemplo: mapa de procesos, carta de servicios, plan de continuidad de negocio, documentación de procesos, etc.), por favor, indíquelo en el anexo I de este documento.

Nombre	Descripción	Participantes ²	Crítico ³	Activos de Información/Datos ⁴
Producto A	Elaboración del producto A	RA- Departamento de Producción C- Departamento de Diseño	SI	<ul style="list-style-type: none"> Diseño Plan de producción
Servicio B	Prestación del servicio B	RA- Departamento de Postventa C- Departamento de Producción	SI	<ul style="list-style-type: none"> Pedidos Estado proyectos Sugerencias de clientes

Observaciones:

² **Participantes:** Unidad organizativa o persona que participa en el proceso. Indicar el grado de involucración de cada área, utilizando el modelo RACI: **R**- Realiza / **A**- Responsable / **C**- Colabora / **I**- Es informada.

³ **Crítico:** Indicar si el proceso incluye tratamiento de datos críticos desde el punto de vista de la seguridad: disponibilidad, integridad, confidencialidad, autenticidad o trazabilidad.

⁴ **Datos/Información:** Datos que se deben utilizar para el funcionamiento del proceso. Enumerar el/los conjuntos de datos necesarios.

Gestión de Riesgos Tecnológicos Fecha Impresión : 09/04/09

Figura 62: Cuestionarios - Procesos de negocio

Código	XXXXX-XXX-000-01	Tipo	Cuestionario	Versión	01	Fecha emisión	xx/xx/xxxx	Página	8 / 14
Descripción		Identificación de Activos de Información							

5. ACTIVOS DE INFORMACIÓN / DATOS

Por favor, complete en el siguiente cuadro la descripción de los activos de información identificados en el apartado anterior.

Las casillas sombreadas incluyen un ejemplo de la cumplimentación de los datos solicitados.

Si dispone de documentación relativa a los activos de información (Por ejemplo, mapas de aplicaciones, diccionarios de datos, diagramas de flujo de datos, documentación de procesos, etc.), por favor, indíquelo en el anexo I.

Dato/Información	Descripción/Finalidad	Requerimientos de Seguridad (1-10) ⁵					Recursos de información ⁶			
		D	I	C	A	T	Origen	Almacenamiento	Procesamiento	Destino
Diseño	Especificaciones del producto	5	8	8	7	9	Proceso de diseño	PCs diseñadores Planos en papel Aplicación control maquinaria	Aplicación control maquinaria	Oficina de patentes
Pedidos	Peticiones de servicio	4	5	3	6	8	Call center Formularios en papel	Aplicación CRM	Aplicación CRM Correo electrónico	Departamento Comercial Datawarehouse

Observaciones:

⁵ **Requerimientos de seguridad:** **D**: Disponibilidad / **I**: Integridad / **C**: Confidencialidad / **A**: Autenticidad / **T**: Trazabilidad. Una guía para la valoración de los requerimientos de seguridad puede encontrarse en el anexo II de este documento.

⁶ **Recursos de información:** Todos los elementos involucrados en el manejo de la información. Un listado de tipos de recursos de información a considerar puede encontrarse en el anexo III.

Gestión de Riesgos Tecnológicos Fecha Impresión : 09/04/09

Figura 63: Cuestionarios - Activos de información

Código	XXXX-XXX-000-01	Tipo	Cuestionario	Versión	01	Fecha emisión	xx/xx/xxxx	Página	9 / 14
Descripción		Identificación de Activos de Información							

6. RECURSOS DE INFORMACIÓN

Por favor, complete en el siguiente cuadro la descripción de los recursos de información identificados en el apartado anterior.

Las casillas sombreadas incluyen un ejemplo de la cumplimentación de los datos solicitados.

Si dispone de documentación relativa a los recursos de información (Por ejemplo, mapas de aplicaciones, inventario de aplicaciones, diccionarios de datos, documentación de procesos, etc.), por favor, indíquelo en el anexo I.

Nombre	Tipo de recurso ⁷	Responsable	Descripción	Amenazas ⁸	Controles ⁹
Planos en papel	Soporte papel	Dpto. Diseño	Planos para la fabricación del producto.	Robo Destrucción	Almacenamiento en caja fuerte Copia de respaldo en caja de seguridad
Aplicación control maquinaria	Aplicación	Dpto. Producción	Aplicación que controla las máquinas de producción.	Avería del servidor Corrupción de datos	Sistema redundado Sistema de control de calidad del producto

Observaciones:

⁷ Tipo de recurso: Una guía de tipos de recursos de información puede encontrarse en el anexo III de este documento.

⁸ Amenazas: Una taxonomía para la identificación de amenazas puede encontrarse en el anexo IV de este documento.

⁹ Controles: Una taxonomía para la identificación de controles puede encontrarse en el anexo V de este documento.

Gestión de Riesgos Tecnológicos Fecha Impresión : 09/04/09

Figura 64: Cuestionarios - Recursos de información

Código	XXXX-XXX-000-01	Tipo	Cuestionario	Versión	01	Fecha emisión	xx/xx/xxxx	Página	10 / 14
Descripción		Identificación de Activos de Información							

7. ANEXO I: DOCUMENTACIÓN

Por favor, indicar a continuación los documentos referenciados en las tablas anteriores:

- ☐ Organigrama
- ☐ Descripción de puestos de trabajo
- ☐ Mapa de procesos de negocio
- ☐ Análisis de riesgos de negocio
- ☐ Carta de servicios
- ☐ BIA / Plan de Continuidad de Negocio
- ☐ Documentación de procesos
- ☐ Mapa / Inventario de aplicaciones
- ☐ Diccionario/Inventario de datos
- ☐ Diagramas de flujo de datos
- ☐ Auditorías
- ☐ Otros (Indicar)

- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

Gestión de Riesgos Tecnológicos Fecha Impresión : 09/04/09

Figura 65: Cuestionarios - Anexo I Documentación

Código	XXXX-XXX-000-01	Tipo	Cuestionario	Versión	01	Fecha emisión	xx/xx/xxxx	Página	11 / 14
Descripción		Identificación de Activos de Información							

8. ANEXO II: VALORACIÓN

Importancia: el valor del activo es la estimación del coste inducido por la materialización de una amenaza sobre el mismo. A continuación se muestra el criterio de Importancia del activo por cada una de las dimensiones:

Valor	Criterio
10	Muy alto
7-9	Alto
4-6	Medio
1-3	Bajo
0	Despreciable

Los activos pueden ser valorados basándose en diversas dimensiones (características o atributos que hacen valioso un activo) como son las siguientes:

Disponibilidad: Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados. ¿Qué importancia tendría que el activo no estuviera disponible?

Integridad de los datos: Garantía de la exactitud y completitud de la información y los métodos de su procesamiento. ¿Qué importancia tendría que los datos fueran modificados fuera de control?

Confidencialidad de los datos: Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso. ¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?

Autenticidad: Aseguramiento de la identidad u origen. ¿Qué importancia tendría que quien accede al servicio no sea realmente quien se cree? ¿Qué importancia tendría que los datos no fueran realmente imputables a quien se cree?

Trazabilidad: Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. ¿Qué importancia tendría que no quedara constancia fehaciente del uso del servicio? ¿Qué importancia tendría que no quedara constancia del acceso o modificación a los datos?

Gestión de Riesgos Tecnológicos Fecha Impresión : 09/04/09

Figura 66: Cuestionarios - Anexo II Valoración

Código	XXXX-XXX-000-01	Tipo	Cuestionario	Versión	01	Fecha emisión	xx/xx/xxxx	Página	12 / 14
Descripción		Identificación de Activos de Información							

9. ANEXO III: RECURSOS DE INFORMACIÓN

A continuación se muestra un listado no exhaustivo de tipos de recursos de información que se deben considerar para cada activo de información identificado:

<input type="checkbox"/> Procesos y servicios <ul style="list-style-type: none"> o Procesos o Servicios internos o Servicios externos <input type="checkbox"/> Personas <ul style="list-style-type: none"> o Directivos o Usuarios internos o Usuarios contratas o Administradores de sistemas o Clientes o Proveedores o Accionistas o Reguladores/supervisores <input type="checkbox"/> Aplicaciones informáticas	<input type="checkbox"/> Redes de comunicaciones <ul style="list-style-type: none"> o Redes locales o Enlaces de telecomunicaciones o Redes inalámbricas <input type="checkbox"/> Soportes de información <ul style="list-style-type: none"> o Papel o Cintas o Discos magnéticos o CD/DVD o Memorias flash o Tarjetas de memoria o Tarjetas inteligentes o Memorias internas dispositivos hardware <input type="checkbox"/> Equipamiento auxiliar <ul style="list-style-type: none"> o Sistemas de alimentación eléctrica o Sistemas de aire acondicionado o Sistemas de detección/extinción de incendios o Sistemas de alarma o Sistemas de videovigilancia o Sistemas de control de acceso <input type="checkbox"/> Software de sistemas <ul style="list-style-type: none"> o Sistemas operativos o Bases de datos <input type="checkbox"/> Dispositivos de hardware <ul style="list-style-type: none"> o Servidores o Puestos de trabajo o Ordenadores portátiles o Agendas electrónicas o Teléfonos inteligentes o Impresoras o Scanners o Modems o Hubs o Switches o Routers 	<input type="checkbox"/> Dispositivos de seguridad <ul style="list-style-type: none"> o IDS/IPS o Firewall o Antivirus o Accionistas o Reguladores/supervisores
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Gestión de Riesgos Tecnológicos Fecha Impresión : 09/04/09

Figura 67: Cuestionarios - Anexo III Recursos de información

	Código XXXXX-XXX-000-01	Tipo Cuestionario	Versión 01	Fecha emisión xx/xx/xxxx	Página 13 / 14
Descripción Identificación de Activos de Información					

10. ANEXO IV: AMENAZAS

A continuación se muestra una taxonomía para la identificación de amenazas a los recursos de información:

<input type="checkbox"/> Desastres naturales <ul style="list-style-type: none"> o Fuego o Agua o Otros desastres naturales <input type="checkbox"/> De origen industrial <ul style="list-style-type: none"> o Fuego o Agua o Contaminación mecánica o Contaminación electromagnética o Avería de origen físico o lógico o Corte del suministro eléctrico o Condiciones inadecuadas de temperatura y/o humedad o Fallo de servicios de comunicaciones o Interrupción de otros servicios y suministros esenciales o Degradación de los soportes de almacenamiento de la información o Emanaciones electromagnéticas o Otros desastres industriales <input type="checkbox"/> De origen regulatorio <ul style="list-style-type: none"> o Incumplimiento legal o Incumplimiento contractual o Incumplimiento normativa interna 	<input type="checkbox"/> Errores y fallos no intencionados <ul style="list-style-type: none"> o Errores de los usuarios o Errores del administrador o Errores de monitorización (log) o Errores de configuración o Deficiencias en la organización o Difusión de software dañino o Errores de [re]-encaminamiento o Errores de secuencia o Escapes de información o Alteración de la información o Introducción de información incorrecta o Degradación de la información o Destrucción de información o Divulgación de información o Vulnerabilidades de los programas (software) o Errores de mantenimiento / actualización de programas (software) o Errores de mantenimiento / actualización de equipos (hardware) o Caída del sistema por agotamiento de recursos o Indisponibilidad del personal 	<input type="checkbox"/> Errores y fallos intencionados <ul style="list-style-type: none"> o Manipulación de la configuración o Suplantación de la identidad del usuario o Abuso de privilegios de acceso o Uso no previsto o Difusión de software dañino o [Re]-encaminamiento de mensajes o Alteración de secuencia o Acceso no autorizado o Análisis de tráfico o Repudio o Interceptación de información (escucha) o Modificación de la información o Introducción de falsa información o Corrupción de la información o Destrucción la información o Divulgación de información o Manipulación de programas o Denegación de servicio o Robo o Ataque destructivo o Ocupación enemiga o Indisponibilidad del personal o Extorsión o Ingeniería social
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Gestión de Riesgos Tecnológicos Fecha Impresión : 09/04/09

Figura 68: Cuestionarios - Anexo IV Amenazas

	Código XXXXX-XXX-000-01	Tipo Cuestionario	Versión 01	Fecha emisión xx/xx/xxxx	Página 14 / 14
Descripción Identificación de Activos de Información					

11. ANEXO V: TIPOS DE CONTROLES

A continuación se muestra una taxonomía para la identificación de controles que protegen los recursos de información:

- ☐ Políticas, normas y procedimientos
- ☐ Organización y estructura
- ☐ Control de activos
- ☐ Control de empleados
- ☐ Control de seguridad física
- ☐ Control de comunicaciones
- ☐ Control de operaciones de sistemas de información
- ☐ Control de acceso lógico
- ☐ Adquisición, desarrollo y mantenimiento de aplicaciones
- ☐ Gestión de incidentes de seguridad
- ☐ Gestión de la continuidad
- ☐ Cumplimiento regulatorio

Gestión de Riesgos Tecnológicos Fecha Impresión : 09/04/09

Figura 69: Cuestionarios - Anexo V Tipos de controles