Universidad Carlos III de Madrid

INGENIERÍA TÉCNICA EN INFORMÁTICA DE GESTIÓN

DEPARTAMENTO DE INFORMÁTICA

PROYECTO FIN DE CARRERA

EL ANÁLISIS DE RIESGOS DENTRO DE UNA AUDITORÍA INFORMÁTICA: PASOS Y POSIBLES METODOLOGÍAS

Autor: Mª del Carmen Crespo Rin

Tutor: Miguel Ángel Ramos González

Leganés, enero de 2013

Título: El Análisis de Riesgos dentro de una Auditoría Informática: pasos y posibles metodologías

Autor: Mª del Carmen Crespo Rin

Tutor: Miguel Ángel Ramos González

EL TRIBUNAL

Presidente:_____

Vocal:_____

Secretario:_____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día __ de _____ de 20__ en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

Agradecimientos

A veces la vida se muestra cruel y te obliga a caminar por los caminos más empinados que te puedas imaginar. Pero a veces, te presenta una cara más amable y te da una segunda oportunidad. Lo que he pretendido es aprovechar una dimensión de esa segunda oportunidad y terminar un sueño que comencé hace mucho tiempo.

Durante este tiempo llegaron personas nuevas a mi vida y otras se marcharon.

Quiero dar las gracias a todas las personas que durante este tiempo han estado a mi lado, me han alentado y me han comprendido.

Quiero dar las gracias a mi familia y mis amigos.

Quiero agradecer especialmente la paciencia de mi tutor, por mis idas y mis venidas; por estar siempre disponible.

Sobre todo y por encima de todo quiero dedicarle este trabajo a mi gran amor, a mi hijo.

Resumen

El presente trabajo se ha estructurado fundamentalmente en dos partes bien diferenciadas. La primera parte comprende desde el capítulo II hasta el capítulo VI y la segunda parte incluye los capítulos VII, VIII y IX.

En la primera parte se ha llevado a cabo un estudio teórico sobre las áreas de conocimiento que están involucradas en este trabajo, es decir, sobre la auditoría informática y el análisis de riesgos. Para ello hemos recurrido a los trabajos publicados por varios autores de reconocido prestigio que nos han permitido estudiar diferentes tipos y modelos de auditoría para diferentes campos de la informática, así como presentar una primera aproximación metodológica al desarrollo de una auditoría. Así mismo, hemos realizado un estudio de las principales metodologías, normas y marcos de trabajo existentes en el campo de la Auditoría de Sistemas de Información; hemos repasado la familia ISO 2700 (incluyendo la ISO 27001, la 27002, la 27004 y la 27007), la ISO/IEC 38500, las normas de auditoría de ISACA, ITIL y por supuesto el marco COBIT.

Con relación al análisis de riesgos, hemos seguido un desarrollo similar al expresado anteriormente para la auditoría. Primero hemos planteado un estudio teórico sobre el concepto de análisis y gestión del riesgo, para a continuación llevar a cabo un estudio de las diferentes metodologías y estándares existentes en el mercado para llevar a cabo un análisis de riesgos. Nos hemos centrado en las siguientes: AS/NZS ISO 31000:2009, UNE 71504:2008, OCTAVE, ISO/IEC 27005:2011, MEHARI, CRAMM y, por supuesto, MAGERIT, que luego hemos utilizado como base en nuestra propuesta metodológica como más adelante explicaremos. Lo anteriormente expuesto formaría lo que hemos denominado marco teórico de trabajo.

A continuación expondremos la segunda parte o propuesta de metodología propia para llevar a cabo una auditoría informática utilizando un análisis de riesgos.

Para ello, lo primero que hemos realizado ha sido unos análisis comparativos de los estándares, marcos de trabajo y guías y normas de la

auditoría informática, por una parte y, por otra parte, un análisis comparativo de estándares y metodologías de análisis de riesgos.

Finalmente, hemos realizado una propuesta metodológica para llevar a cabo una auditoría soportada en el análisis de riesgos, que entendemos susceptible de ser utilizado en entidades pequeñas y medianas. Hemos completado dicha propuesta con unas plantillas en Excel y una página web que podrá servir de mecanismo rápido de consulta para el auditor.

Abstract

This work has been structured mainly in two different parts. The first part covers from chapter II to chapter VI and the second part includes chapters VII, VIII and IX. In the first part, a theoretical study has been carried out on the areas of knowledge that are involved in this work, i.e., on the information technology audit and risk analysis. For this purpose we have resorted to papers published by several renowned authors which have enabled us to study different types and models of audit for different fields of computer science, as well as presenting a first methodological approach to the development of an audit.

Likewise, we have carried out a study of the main methodologies, standards and frameworks existing in the field of the information systems audit: we have reviewed the ISO 2700 family (including ISO 27001, 27002, 27004 and 27007), ISO/IEC 38500, the auditing standards of ISACA, ITIL and, of course, the COBIT framework.

Regarding risk analysis, we have followed a similar development to the one explained previously for the audit. We have first planned a theoretical study on the concept of risk management and analysis, then carried out a research of the different methodologies and standards existing in the market to carry out a risk analysis. We have focused on the following: AS/NZS ISO 31000: 2009, UNE 71504: 2008, OCTAVE, ISO/IEC 27005: 2011, MEHARI, CRAMM and, of course, MAGERIT, that then we have used as a base in our methodological proposal, as explained later. The above would be what we call theoretical framework.

Then, we will expose the second part or proposal of methodology to carry out an information technology audit using a risk analysis.

To do this, we have made several comparative analyses of standards, frameworks and guides and computer auditing standards on the one hand and, on the other hand, a comparative analysis of standards and risk analysis methodologies.

We have finally made a methodological proposal to carry out an audit based on risk analysis, which we believe that can be used in small and medium-

sized entities. We have completed the proposal with a few Excel templates and a web page that can serve as a quick reference for the auditor.

ÍNDICE

CAPÍTULO I: Introducción y objetivos

CAPÍTULO II: La auditoría informática

CAPÍTULO V: Metodologías y/o estándares para el análisis y la gestión de riesgos

CAPÍTULO VIII: Análisis comparativo de estándares y metodologías de análisis de riesgos

CAPÍTULO IX: Propuesta de una guía para llevar a cabo una auditoría informática

Índice de figuras

Índice de Tablas

CAPÍTULO I: Introducción y Objetivos

1. Introducción

El aumento en el uso de los sistemas informáticos por parte de las empresas y la creciente complejidad en dichos sistemas y las infraestructuras que los soportan, han incrementado la complejidad en su control y en el aseguramiento de los mismos frente a amenazas que puedan explotar sus posibles vulnerabilidades.

Por lo anteriormente expuesto, el establecimiento de controles y medidas de protección se ha convertido en una preocupación para todas las empresas que buscan además de proteger sus infraestructuras, proteger uno de sus activos más valiosos: la información y así garantizar su confidencialidad, integridad, trazabilidad y disponibilidad.

Además del establecimiento de controles es necesaria la evaluación de los mismos, por lo tanto se deben diseñar estrategias y planes que proporcionen directrices efectivas de control y que permitan la realización de un proceso de evaluación, revisión y verificación de la información, de los procesos y tecnologías que los soportan.

La auditoría informática y el análisis de riesgos, han sido los métodos usados comúnmente de forma independiente para evaluar los sistemas de información, cada uno con un enfoque diferente. De un lado la auditoría informática es un proceso de revisión y verificación mientras que el análisis de riesgos es un proceso de diagnóstico y revisión.

El concepto de auditoría ha ido evolucionado a la par que han ido evolucionando las tecnologías de la información y comunicación y se ha enfrentado a la necesidad de pasar de un enfoque de verificación, efectuado a posteriori, a un enfoque preventivo y proactivo basado en la valoración de los riesgos y en la evaluación de la eficacia y eficiencia de los procedimientos y los controles establecidos en las organizaciones, orientados a mejorar las características de seguridad, calidad, eficiencia y eficacia de los sistemas de información y las tecnologías asociadas y por lo tanto al mejoramiento de los procesos que sustentan sus negocios.

De la mano de la evolución de los conceptos de control, auditoría, análisis de riesgos y en general de seguridad de la información se han desarrollado normativas, estándares, metodologías y marcos de trabajo ampliamente conocidos, que pueden ser aplicados por las empresas para apoyar y estandarizar el desarrollo de las labores de auditoría y análisis de riesgos. En el caso de la auditoría informática, no se cuenta con una metodología concreta y estandarizada para abordar la auditoría con un enfoque de análisis de riesgos, los diferentes estándares, normativas y marcos de trabajo tocan aspectos puntuales; por lo tanto con el fin de abordar esta problemática, en este trabajo se hace un análisis de la auditoría informática y el análisis de riesgos, inicialmente como mecanismos de evaluación independientes y posteriormente de cómo pueden usarse de forma conjunta dentro de una auditoría informática, para finalmente proponer una guía de auditoría que hace uso del análisis de riesgos.

2. Objetivos

2.1. Objetivo general

El objetivo general de este Proyecto de Fin de Carrera, es realizar un estudio teórico acerca de la auditoría informática y el análisis de riesgos, y posteriormente realizar una propuesta metodológica para llevar a cabo una auditoría informática basada en el análisis de riesgos.

2.2. Objetivos específicos

- Realizar un estudio del estado de la cuestión, de las áreas de conocimiento involucradas en este trabajo, como lo son la auditoría informática y el análisis de riesgos.
- Realizar una evaluación de las principales metodologías existente para la realización de auditorías informáticas y de análisis de riesgos.
- Realizar una propuesta metodológica para llevar a cabo una auditoría informática soportada en el análisis de riesgos, a través del desarrollo de una guía que pueda ser aplicada a empresas pequeñas y medianas.

3. Estructura de la memoria

La estructura que sigue la memoria es la siguiente:

En el **capítulo 1** se presenta la introducción y los objetivos del PFC.

En el **capítulo 2** se hace una introducción a los conceptos generales de la auditoría informática y se tratan diferentes temas relacionados como son: sus objetivos, las diferentes áreas de aplicación, la metodología general para llevar a cabo una auditoría informática y la evolución de la función de auditoría informática.

En el **capítulo 3** se abordan los conceptos generales relacionados con el análisis y la gestión de riesgos, sus objetivos, las fases en un análisis de riesgos, las fases de la gestión de riesgos.

En el **capítulo 4** se presentan diferentes metodologías y estándares para la auditoría informática.

En el **capítulo 5** se presentan diferentes metodologías y estándares para el análisis y la gestión de riesgos.

En el **capítulo 6** se realiza un análisis del papel del análisis de riesgos dentro de una auditoría informática, como tema central del PFC.

En los **capítulos 7 y 8**, se presenta un análisis comparativo de estándares, metodologías, marcos de trabajo, guías y normas de auditoría informática y análisis de riesgos.

En el **capítulo 9**, se desarrolla una propuesta de una guía para llevar a cabo una auditoría informática con un enfoque de análisis de riesgos.

Finalmente se presentan las conclusiones y trabajos futuros y la bibliografía del trabajo.

CAPÍTULO II:
La Auditoría Informática

1. Conceptos generales

En términos generales se puede definir la auditoría informática, tal y como se indica en **[CARI 06]**, como el conjunto de procedimientos y técnicas para evaluar y controlar un sistema informático o de información[1], con el fin de constatar si sus actividades son las adecuadas en relación con las normativas generales de aplicación y los objetivos prefijados por la organización. Dicho de otra manera, una auditoría recoge, agrupa y evalúa evidencias para determinar si un sistema salvaguarda los activos, mantiene la integridad de los datos y lleva a cabo eficazmente los fines de la organización y utiliza eficazmente los recursos, **[OOCI 03]**.

La auditoría informática como se expone en **[OOCI 03],** también es vista como el conjunto de acciones que realiza el personal especializado en las áreas de auditoría y de informática para el aseguramiento continuo de que los recursos de informática operen en un ambiente de seguridad y control eficientes, con la finalidad de proporcionar a la alta dirección o a niveles ejecutivos la certeza de que la información que circula por el área se maneja con los conceptos básicos de integridad, totalidad, exactitud, confiabilidad, etc.

La auditoría como proceso metodológico tiene el propósito principal de evaluar los recursos (humanos, materiales, financieros, tecnológicos, etc.) relacionados con la función de informática para garantizar al negocio que dicho conjunto opere con un criterio de integración y desempeño de niveles altamente satisfactorios, para que a su vez apoyen la productividad y rentabilidad de la organización, **[UCMA 09]**.

[1] A efectos de este trabajo se usarán los términos sistema informático y sistema de información, indistintamente, debido a las diferencias sutiles que existen entre dichos términos y se considerará que se refieren al mismo concepto.

2. Objetivos generales de la auditoría informática

Los objetivos tradicionales de una auditoría informática, tal y como se indica en **[NAVA 10]** son la protección de activos e integridad de datos y la eficacia y eficiencia en la gestión de los mismos. Por tanto, la realización adecuada de la auditoría proporciona información que ayuda a mejorar la rentabilidad, la seguridad y la eficacia de los sistemas.

En lo relativo al control de la seguridad, la auditoría informática debe contemplar tres vertientes:

- **Aspectos generales**. En este caso estamos hablando del control de los elementos que aunque, no se consideran parte intrínseca del sistema sí que su falla afecta al mismo. Estamos hablando por ejemplo de la seguridad en los suministros, de la seguridad física de las instalaciones.
- **Aspectos relativos a la confidencialidad y seguridad de la información**, es decir, el control y el acceso a la información.
- **Aspectos jurídicos y económicos.** En este sentido se habla de la adecuación de los sistemas a la normativa vigente y que sean de aplicación a estos y de su rentabilidad.

La eficacia del sistema informático debe venir determinada por la aportación a la organización de una información válida, exacta, completa, actualizada y disponible en el momento adecuado y para el personal adecuado. La medición debe realizarse en términos de calidad, plazo y coste. Sin el control adecuado, y eso incluye auditorías, no sería posible certificar que se consiguen estos objetivos y podría tener graves repercusiones en la correcta gestión de la organización.

Con relación a la rentabilidad del sistema informático, una auditoría debe revisar que el sistema asegure el equilibrio entre riesgos, costes de seguridad y los costes del propio sistema. Éstos últimos, deben ser valorados en términos económicos mediante el análisis de tres datos:

- Evaluación de los costes reales. Se busca determinar en términos económicos los costes que para una empresa supone el sistema de informático, cuantificando los costes de los distintos elementos que componen el sistema informático (hardware, software, aplicaciones, personal)
- Comparación de los costes reales con magnitudes representativas de la organización. Esto constituye una valiosa información que deberá ser especificada en las conclusiones de la auditoría informática y que deberá tener incidencia en los planteamientos de futuro.
- Comparación de los costes del sistema informático de la empresa con los de empresas similares.

3. Áreas de la auditoría informática

En el momento de llevar a cabo una auditoría informática, debemos entender que puede ser (y en la mayoría de los casos así se hace) una auditoría de algunas de las áreas en las que puede dividirse una auditoría informática y que dependen de la variedad de actividades informáticas que se lleven a cabo dentro de una empresa, y de los procesos que estas ejecutan y que se apoyan en el uso intensivo de tecnología informática

Al revisar la bibliografía, nos encontramos con varias clasificaciones de las áreas de la auditoría informática y que tradicionalmente se han asociado a las funciones llevadas a cabo por el departamento de informática de las empresas. De manera general varios autores sugieren la siguiente clasificación: auditoría de la explotación u operación, auditoría de sistemas, auditoría de desarrollo de proyectos, auditoría de comunicaciones y redes y auditoría de seguridad.

A efectos de este apartado hemos tomado como referencia la clasificación, expuesta en el libro **"Auditoría de tecnologías y sistemas de información, de Mario G Piattini y Emilio del Peso"**, que consideramos ha evolucionado con respecto a las clasificaciones tradicionales y presenta un enfoque más moderno de la auditoría informática y mayor especificidad en sus áreas de aplicación. Dicha

clasificación ha sido tomada de y adaptada de **[PIAT 08]** y se presenta a continuación:

- Auditoría de outsourcing.
- Auditoría física
- Auditoría de la dirección
- Auditoría de explotación
- Auditoría de Bases de Datos
- Auditoría de Técnica de Sistemas
- Auditoría de la seguridad
- Auditoría de redes
- Auditoría de Internet
- Auditoría de Aplicaciones
- Auditoría del desarrollo y mantenimiento de sistemas informáticos
- Auditoría de la video vigilancia.
- Auditoría reglamentaria de los datos de carácter personal.

En los siguientes apartados vamos a desarrollar algunas áreas de auditoría, que nos pueden parecer especialmente significativas o relevantes bien por el área que tocan o bien por el enfoque que utilicen.

3.1. Auditoría Física

La Auditoría Física, al igual que cualquier otra área de una auditoría informática, no difiere de una Auditoría General más que en el alcance de la misma.

La seguridad debe vigilar tres tipos de seguridad: la seguridad lógica, la seguridad física y la seguridad de las comunicaciones, aunque las fronteras que delimitan estas tres seguridades es bastante difusa. En lo que concierne a la seguridad física, debe garantizar la integridad de los activos humanos, lógicos y materiales y para ello, debe tener preparadas las tres medidas -en orden cronológico- que deben ponerse en funcionamiento si se produce un riesgo de fallo: antes, durante y después.

Antes, es decir, el conjunto de acciones que se pueden llevar a cabo para evitar el fallo o, de no ser posible, aminorar las consecuencias que pueda tener.

Durante, ejecutando un Plan de Contingencia adecuado que debe ser el resultado de realizar un Análisis de Riesgos adecuado, de establecer períodos críticos de recuperación y de determinar adecuadamente los objetivos de recuperación.

Después, para que una vez que haya sucedido el fallo, se pueda compensar en la medida de lo posible, las pérdidas, gastos o responsabilidades que se puedan derivar. Esto lo vienen a compensar los contratos de seguro.

Respecto a las áreas que debe tratar una auditoría física, si usamos un orden basado en la lógica "de fuera adentro", el edificio sería la primera área a tener en cuenta en una Auditoría Física. Cabe suponer que el auditor informático no tiene los conocimientos suficientes para detectar el estado actual de la infraestructura y diagnosticar sus defectos y vicios, por lo que se debe prever la ayuda de un perito independiente.

Las áreas que el auditor sí que debe analizar personalmente, siempre considerando el aspecto físico de la seguridad, son:

- Organigrama de la empresa
- Auditoría interna
- Administración de la seguridad
- Centros de procesos de datos e instalaciones
- Equipos y comunicaciones
- Ordenadores personales
- Seguridad física del personal

3.2. Auditoría de la Dirección

Esta área de auditoría debe revisar que la dirección de informática de cualquier organismo y/o entidad funcione de manera adecuada, es decir, planifique, organice, coordine y controle adecuadamente.

Planificación: La auditoría, deberá examinar el proceso de planificación de sistemas de información y evaluar si se cumplen los objetivos del mismo. Para ello deberá evaluar:

- Si el proceso de planificación está alineado con el plan estratégico de la empresa, estableciendo mecanismos de sincronización entre los hitos empresariales y los proyectos informáticos que estén asociados. Así mismo, se deberá evaluar si se presta la consideración necesaria a las nuevas tecnologías informáticas.
- Si se ha realizado una adecuada asignación de recursos para llevar a cabo las tareas y actividades recogidas en el Plan

- **Organización y coordinación:** En este punto, la auditoría de dirección debe revisar la existencia de flujos de información con el resto de las áreas del organismo y/o entidad así como aspectos intrínsecos de la propia función de dirección.
- **Control y seguimiento**: La tarea de dirigir no puede considerarse completa sin esta última fase, que es parte indisoluble de esta responsabilidad. Se debe vigilar y controlar que se cumplen todos los puntos que se han tratado anteriormente. Para poder hacer esta labor, se convierte en recomendable la existencia de estándares de rendimiento con los que comparar cada una de las tareas. La dirección de informática no debe dejar nunca de lado, que el cumplimiento de sus actividades se lleve a cabo dentro del respeto a la normativa legal de aplicación.

3.3. Auditoría de la Explotación

Podemos considerar que un sistema de información (SI) es un conjunto de componentes que interactúan para que una organización pueda alcanzar sus objetivos de manera satisfactoria.

Utilizando la clasificación del proyecto CoBiT, podemos concluir que los componentes de un SI son:

- **Datos**.- Se consideran datos tanto los estructurados como los no estructurados, es decir, imágenes, sonidos, etc.
- **Aplicaciones**.- Tanto las manuales como las informativas.
- **Tecnología**.- Software y hardware; sistemas operativos, de gestión de bases de datos, de redes,…
- **Instalaciones**.- Donde se ubican y mantienen los SI.
- **Personal**.- Los conocimientos específicos que deben tener para planificar, organizar, administrar y gestionar los SI.

Estos recursos se deben utilizar de forma y manera que posibiliten la eficacia y eficiencia de la organización de la empresa y que asegura la confidencialidad de los datos.

Para poder hacer el seguimiento y comprobar que el SI funciona como se debe, éste deberá disponer de un control interno que prevenga los eventos no deseados o si esto no es posible los detecte y los corrija.

Según las recomendaciones que se incluyen en la Guía del Proyecto CoBiT, el objetivo general de la auditoría consiste en: "Asegurarse que las funciones que

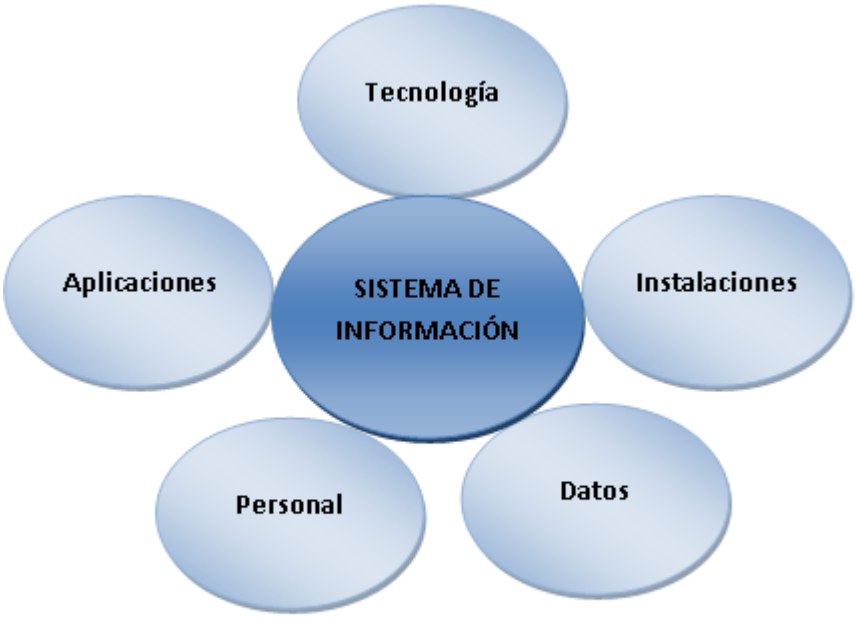


Figura 2.1. Componentes de un Sistema de Información

sirven de apoyo a las Tecnologías de la Información se realizan con regularidad, de forma ordenada y satisfaciendo los requisitos empresariales."

En función de la importancia de los riesgos que se hayan detectado, se determinarán los objetivos de auditoría, que se deberán determinar concretamente para definir con claridad el alcance de la misma.

3.3.1. Control interno

Vamos a hacer en este apartado una mención especial a la definición de control interno dentro de un SI. Todo SI debe disponer de un control interno que prevenga los eventos no deseados o si esto no es posible, los detecte y los corrija.

Tradicionalmente se ha distinguido entre controles generales y controles de aplicación.

LA AICPA (American Institute of Charter Public Accountants), publicó en la Norma número 48 (1984) la definición de **controles generales** como "aquellos que están relacionados con todas o con la mayoría de las actividades contables informatizadas, que generalmente incluyen controles del desarrollo de las modificaciones y del mantenimiento de programas informáticos y controles de la utilización y modificación de los datos que se mantienen en ficheros informáticos".

El Registro de Economistas y Auditores publicó en enero de 1996 el informe «El estudio y evaluación del control interno en entornos informatizados», en el que dice que: "Los controles generales son una parte del entorno general de control y son aquellos que afectan a toda la información por igual y a la continuidad de servicio de la organización. La debilidad o ausencia de estos controles puede tener un impacto significativo en la integridad y exactitud de los datos. También se consideran controles generales aquellos relacionados con la protección de los activos: la información resultante, los elementos físicos del hardware y el software."

Por otra parte, los **controles de aplicación** son aquellos relacionados con la captura, entrada y registro de datos en un sistema informático y los relacionados con su procesamiento, cálculo, salida de información y su distribución.

En el proceso de auditoría se deberá evaluar el nivel de control interno así como juzgar si los procedimientos establecidos son adecuados para salvaguardar el SI.

Se define control, según el informe COSO, como "el conjunto de normas, procedimientos, prácticas y estructuras organizativas diseñadas para proporcionar seguridad razonable de que los objetivos de las empresas se alcanzarán y que los eventos no deseados se preverán, se detectarán y se corregirán."

3.4. Auditoría de Bases de Datos

Queremos hacer especial mención en este apartado, a la manera en que el profesor Mario Piattini plantea la realización de una auditoría de Bases de Datos.

Para auditar un entorno de base de datos, o cualquier otro entorno o área podemos emplear una metodología tradicional basada en el uso de checklist, como herramienta básica de trabajo o bien utilizar una metodología de evaluación de riesgos (objetivos de control, técnicas de control, pruebas de cumplimiento y pruebas sustantivas), que es la que se propone en ISACA y que es el objeto final de este trabajo.

3.4.1. Objetivos de control en el ciclo de vida de una Base de Datos

En la siguiente figura reflejamos el ciclo de vida de una base de datos, según los modelos propuestos por ISACA, Menkus y CoBiT, que vamos a desarrollar brevemente.

Figura 2.2. Ciclo de vida de una Base de Datos

Fase I: Estudio previo y plan de trabajo

En esta primera fase se debe elaborar un estudio de viabilidad que contemple las distintas alternativas existentes, incluyendo la no realización del proyecto o la posibilidad de comprar en lugar de desarrollar, que contemple un análisis de coste-beneficio.

El auditor deberá comprobar la existencia de este estudio, además de si son revisados por la dirección, que es la que decide si se sigue con el proyecto o no.

En caso en que se decida seguir adelante con el proyecto, el auditor verificará que se establece un plan de trabajo (plan director), y que además se emplea para el seguimiento y la gestión del proyecto.

Fase II: Concepción de la base de datos y selección del equipo

En el proceso de auditoría se deberá analizar la metodología de diseño y verificar si es adecuada o no, así como comprobar su correcta utilización.

Fase III: Diseño y carga

El proceso de auditoría deberá verificar que los diseños –lógico y físico de la base de datos- se han realizado correctamente. Se deberá comprobar si la definición de los datos contempla no sólo la estructura de los mismos, sino las asociaciones y las restricciones que les afecten, así como las cuestiones relativas a su seguridad. En el proceso de auditoría se deberá comprobar también, en el caso en el que las definiciones sean correctas, que han sido aprobadas por el usuario.

Fase IV: Explotación y mantenimiento

En esta cuarta fase, el proceso de auditoría debe verificar que existen los mecanismos de explotación y mantenimiento que aseguren que los datos son tratados de manera congruente y que el contenido sólo se modifica una vez conseguida la autorización adecuada.

Fase V: Revisión post-implantación

Esta última fase, que no se lleva a cabo en bastantes organizaciones, deberá establecer el desarrollo de un plan que evalúe si se han conseguido los resultados esperados, si se han satisfecho las necesidades de los usuarios y si la relación coste/beneficio coincide con la prevista.

3.5. Auditoría del outsourcing de los Sistemas de Información

El outsourcing de los Sistemas de Información, se ha ido convirtiendo en un proceso más en la actividad habitual de cualquier organización a la hora de gestionar las Tecnologías de la Información.

Es por lo tanto, un área más que se debe auditar y cuya necesidad de llevar a cabo un proceso de auditoría en el ámbito de una organización, vendrá dado por el resultado que se obtenga del análisis de riesgos que se lleve a cabo, que debe ser el que detecte los procesos que se encuentren en un régimen de outsourcing.

Además, tal y como indica la Ley Sarbanes-Oxley: “los servicios que se desarrollan bajo outsourcing tecnológico son parte del conjunto de operaciones y responsabilidades de las empresas y necesitan ser consideradas dentro del marco de control interno”.

En un outsourcing de los SI, se formaliza un pacto o convenio entre partes que se recoge en un contrato, en el que se obligan al cumplimiento de una serie

de servicios sobre una materia determinada (en el caso que nos ocupa sería servicios informáticos, de información o tecnológicos). En el contrato deberá figurar un Acuerdo de Nivel de Servicio, que recoge el nivel de servicios que deben prestarse y que se considerarán como adecuados por ambas. Es decir, deben posibilitar una medida objetiva de la calidad de la prestación de los servicios contratados. A estas medidas objetivas, es a lo que se llama Indicadores de Nivel de Servicio.

4. Metodología general de auditoría informática

La auditoría informática como proceso formal, el cual es ejecutado por especialistas del área de auditoría tal y como se expone en **[UCMA 09]**, es un proceso metodológico, que tiene el propósito de evaluar los recursos – humanos, tecnológicos, materiales, financieros – que están relacionados con la función de informática, para garantizar que se opere con criterios de integración y desempeño altamente satisfactorios y que también apoyen la productividad y la rentabilidad de la organización.

4.1. Proceso metodológico en una auditoría informática

Anteriormente nos hemos referido a la auditoría informática como un proceso formal, el cual debe llevar a cabo los procesos, tareas y actividades mediante una metodología.

No es recomendable basar el proceso de auditoría únicamente en la experiencia, habilidades y criterios sin que exista una referencia metodológica. Esta metodología debe ser entendida y aceptada por todas las partes implicadas en el proceso de auditoría.

No obstante, tampoco el uso de una metodología garantiza por sí sola el éxito de los proyectos de auditoría, también se requiere un buen dominio y uso constante de los siguientes aspectos complementarios, como se indica en **[UCMA 09]**:

- Técnicas
- Herramientas de productividad
- Habilidades personales
- Conocimientos técnicos y administrativos
- Experiencia en los campos de auditoría e informática
- Conocimiento de los factores de negocio y del medio externo al mismo
- Actualización permanente
- Comunicación con asociaciones relacionadas

4.2. Etapas de la metodología de auditoría

A continuación presentamos una ruta posible a seguir en una metodología de auditoría, la cual ha sido sugerida en **[UCMA 09], [HERN 00] y [ECHE 97].**

Es importante mencionar que la metodología que se describe a continuación es de ámbito general y que existen metodologías específicas y reconocidas para realizar una auditoría informática, al igual que estándares y normativa asociada; esta metodología se presenta como un marco de trabajo que permite abordar una auditoría.

Cada una de las etapas indicadas a continuación se ha tomado de **[UCMA 09], [HERN 00] y [ECHE 97].**

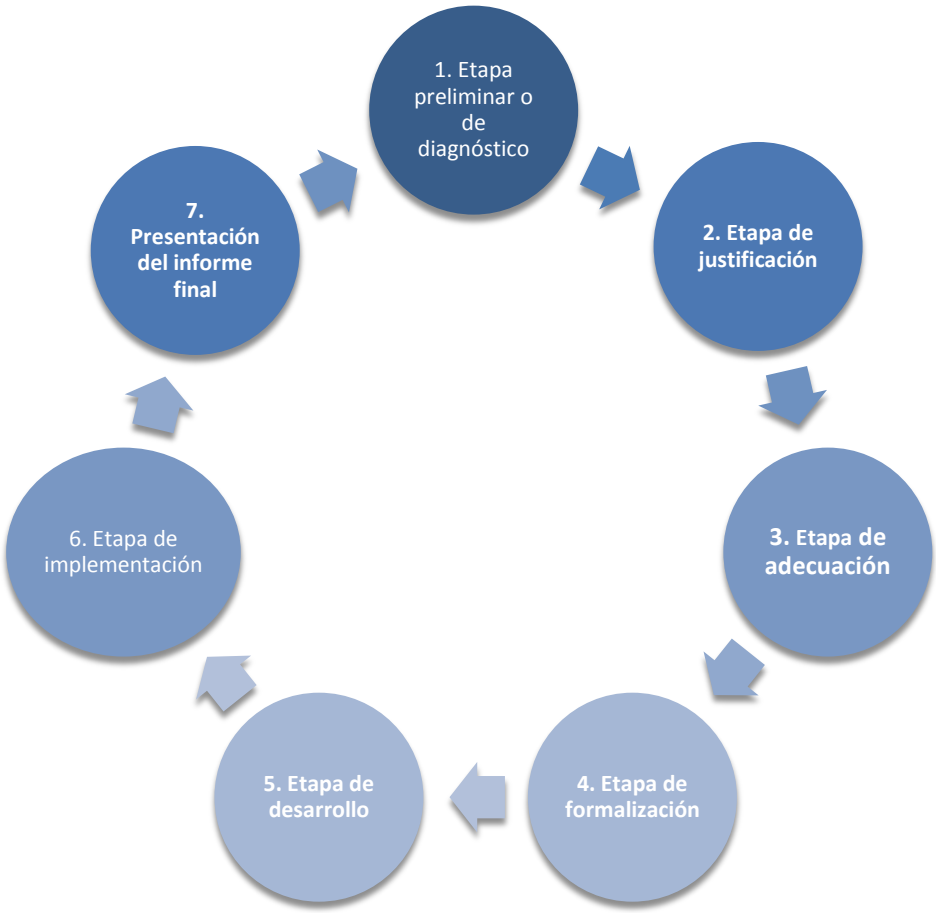


Figura 2.3. Etapas de una metodología de auditoría

4.2.1. Etapa preliminar o de diagnóstico

En este primer paso, se hace un diagnóstico del negocio, que incluye a la dirección y las áreas usuarias.

De la dirección, se intenta poder saber el grado de satisfacción y confianza que tiene en los productos, servicios y recursos informáticos. Este primer paso, también sirve para detectar las fortalezas, aciertos y apoyos que brinda la función de informática y las oportunidades de negocio que ésta puede ofrecer para hacerle más competitivo.

4.2.2. Etapa de justificación

En esta segunda etapa, se elabora el documento que va a ser fundamental para la aprobación del proyecto de auditoría.

Este documento contendrá el resultado de las siguientes tres tareas:

- La matriz de riesgo: que contempla las áreas a auditar,
- El tiempo sugerido para hacerlo: plan de auditoría informática y
- El visto bueno o compromiso ejecutivo.

4.2.3. Etapa de adecuación

Esta etapa puede definirse como un conjunto de tareas estructuradas para que el proyecto de auditoría informática se adapte a las necesidades de la empresa que se está evaluando, sin olvidar en ningún caso la referencia a los estándares, políticas y procedimientos de auditoría que son siempre aceptados y recomendados por las asociaciones relacionadas con el proceso.

4.2.4. Etapa de formalización

Al término del desarrollo de las etapas ejecutadas hasta el momento –preliminar, justificación y adecuación-, el auditor habrá obtenido una "fotografía" de la situación actual de la empresa y de la función de informática, que refleje las debilidades y fortalezas más relevantes. Así mismo, se ha definido la planificación y proyección de las áreas que se van a auditar y se han documentado las actuaciones. Es en esta etapa en la que la dirección da su aprobación y apoyo formal para el desarrollo del proyecto de auditoría.

4.2.5. Etapa de desarrollo

En esta etapa, el auditor va a ejercer su función de manera práctica, es decir, comienza la ejecución propia de las tareas y, aplicando sus conocimientos y experiencias, de acuerdo con el plan aprobado en la etapa anterior, conseguirá un informe final cuyo seguimiento suponga beneficios tangibles para el negocio.

4.2.6. Etapa de implementación

Finalizadas todas las tareas anteriores, se ha llegado al arranque de la etapa de implantación. En este punto, finaliza la tarea del auditor propiamente dicha y empieza para los responsables de las áreas usuarias afectadas y el responsable de la función informática. Estas personas son las responsables de poner en marcha las acciones recomendadas y aprobadas por la dirección. La función del auditor pasa a ser la de seguimiento y apoyo.

4.2.7. Presentación del informe final

La función de auditoría se materializa única y exclusivamente por escrito. Por tanto, el informe final es el exponente de la calidad de la misma.

El informe final de auditoría debe comenzar con la fecha de inicio de la auditoría y la fecha de redacción del mismo. Tiene como destinatario exclusivo al responsable máximo de la empresa, o la persona o personas que encargaron la auditoría y se deberán entregar tantas copias como solicite el cliente.

4.3. Principales pruebas y herramientas para efectuar una auditoría informática

En la realización de una auditoría informática el auditor puede realizar las siguientes pruebas, de acuerdo a lo expuesto en **[OOCI 03]**, **[CARI 06]**:

Pruebas clásicas: Consisten en probar las aplicaciones / sistemas con datos de prueba, observando la entrada, la salida esperada, y la salida obtenida. Existen paquetes que permiten la realización de estas pruebas.

Pruebas sustantivas: Aportan al auditor suficientes evidencias para que se pueda realizar un juicio imparcial. Se suelen obtener mediante observación, cálculos, muestreos, entrevistas, técnicas de examen analítico, revisiones y conciliaciones. Verifican asimismo la exactitud, integridad y validez de la información obtenida.

Pruebas de cumplimiento: Determinan si el sistema evaluado funciona adecuadamente, de acuerdo a la documentación revisada, según declaran los auditados y según las políticas y procedimientos de la organización.

Las principales herramientas de las que dispone un auditor informático para la realización de estas pruebas son:

- Observación
- Realización de cuestionarios
- Entrevistas a auditados y no auditados
- Muestreo estadístico
- Flujogramas
- Listas de comprobación de realización de requisitos
- Mapas conceptuales
- Software

5. Evolución de la función de auditoría informática

Tal y como se sugiere en **[NAVA 10]**, cada vez con mayor frecuencia las empresas y organismos, someten sus sistemas informáticos a auditorías, entre otras cosas debido a la obligatoriedad que establece (en algunos casos), por ejemplo en España, la Ley Orgánica de Protección de Datos –LOPD- .

En un principio, la informática se orientó al apoyo de áreas tales como contabilidad, nóminas, finanzas; a partir de la necesidad de conocer y medir el apoyo que la misma realizaba en las áreas antes mencionadas y, en el entorno organizacional en general, se originó el proceso que se denominó auditoría de sistemas de información o auditoría de sistemas.

Con el desarrollo de las tecnologías de la información y su creciente incorporación en las actividades empresariales, los profesionales encargados de llevar a cabo las auditorías de sistemas se vieron abocados a cambiar el enfoque con el cual se llevaban hasta ahora las auditorias.

De esta manera, surgió la necesidad del replanteamiento de la auditoría de sistemas y pasar al concepto de auditoría informática. Ésta además de encargarse de la auditoría de sistemas –como antes definida- se encargaría también de evaluar y verificar políticas, controles, procedimientos y seguridad en los recursos dedicados al manejo de la información.

CAPÍTULO III: El Análisis y la Gestión de Riesgos

1. Conceptos generales

Para iniciar el estudio del análisis y la gestión de riesgos es preciso comenzar definiendo lo que es riesgo; quizás podemos tener una definición "intuitiva" de lo que en términos generales es un riesgo, pero cuando hablamos de seguridad y de análisis de riesgos debemos ir más allá y acudir a fuentes que nos ofrezcan una buena definición.

Podemos empezar haciendo mención a la definición que hace la Real Academia Española de la Lengua; en su primera acepción lo define como "contingencia o proximidad de un daño" y en la segunda como "cada una de las contingencias que pueden ser objeto de un contrato de seguro".

En el contexto empresarial se define riesgo como: "los factores, acontecimientos, tanto internos como externos, a los que está expuesta la empresa y, que ponen en peligro la consecución de los objetivos."

También podemos definirlo como: "incertidumbre de la ocurrencia de un suceso con efectos negativos y de la magnitud de dichos efectos". Otras variedades de interpretación hablan de: "posibilidad de que exista un daño o contratiempo", "conjunto de circunstancias de pueden disminuir el beneficio", "eventualidad que imposibilita el cumplimiento de un objetivo" y así seguramente podríamos seguir durante algunos párrafos más.

Si centramos la definición de riesgo en el campo del presente trabajo, la tecnología informática (sistemas de información), cuando se habla de riesgo se plantea como amenaza, determinando el grado de exposición a la ocurrencia de una pérdida (el riesgo de perder la información de un disco duro por un virus, por ejemplo).

Si bien existen múltiples definiciones abordadas por diferentes normas y estándares nos quedaremos con las siguientes definiciones para continuar en nuestro estudio:

- **Magerit** define riesgo como: "La estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización."

- Por su parte el Centro Superior de Información de la Defensa, "Glosario de Términos de Criptología", del Ministerio de Defensa, define riesgo como: "La probabilidad de que una vulnerabilidad propia de un sistema de información sea explotada por las amenazas a dicho sistema, con el objetivo de penetrarlo"

En las definiciones anteriores se pueden identificar varios elementos comunes, que se deben comprender adecuadamente para poder entender y valorar en su integridad el concepto de riesgo.

Dichos elementos son: **activo, amenaza, impacto, probabilidad y vulnerabilidad**, de los cuales presentamos su definición a continuación, de acuerdo a algunas normas y/o estándares y entidades oficiales:

- **Activo [MAGE 06]:** "Recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección."
- **Amenaza [MAGE 06]:** "Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos."

En el Esquema Nacional de Seguridad encontramos la siguiente definición: "Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos"

- **Impacto [MAGE 06]:** Consecuencia que sobre un activo tiene la materialización de una amenaza.
- **Probabilidad**: según el diccionario de la Real Academia Española de la Lengua, sería la razón entre el número de casos favorables (yo diría tratándose de riesgos que desfavorables) y el número de casos posibles. Estamos ante el estudio cuantitativo y/o cualitativo del número de veces que la amenaza puede materializarse.

- **Vulnerabilidad [MAGE 06]:** Estimación de la exposición efectiva de un activo a una amenaza. Se determina por dos medidas: frecuencia de ocurrencia y degradación causada.

Figura 3.1 Relación conceptos riesgo [AVEL 08]

Una vez expuestos los conceptos básicos relacionados con los riesgos, ahora pasamos a realizar un estudio del análisis de riesgos como proceso, para lo cual empezaremos definiendo el análisis de riesgos, como lo hemos hecho hasta ahora, basados en conceptos emitidos por organizaciones oficiales.

2. El análisis de riesgos. Definición

En Magerit Versión 2.0, el análisis de riesgos se ha definido como: "Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización". **[MAGE 06]**

Dentro de Magerit versión 1.0, encontramos una definición un poco más amplia, que agrupa varios de los conceptos estudiados hasta ahora, y define el análisis de riesgos como: "Identificación de las amenazas que acechan a los distintos componentes pertenecientes o relacionados con el sistema de información (conocidos como 'activos'); para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización, obteniendo cierto conocimiento del riesgo que se corre", **[MAGE 97]**.

En la norma ISO 27002 **[ISO/IEC 05]**, se define como: "Proceso mediante el cual se identifican las amenazas y las vulnerabilidades en una organización, se valora su impacto y la probabilidad de que ocurran".

Si bien son definiciones presentadas por diferentes organizaciones y estándares, podemos observar que su esencia es similar y que nos dan los elementos necesarios para abordar el análisis de riesgos como el proceso que nos permitirá identificar y evaluar los riesgos a los que está expuesta una organización.

2.1. Objetivo del análisis de riesgos

Es importante para una organización tener claridad en cuanto a lo que espera al llevar a cabo un análisis de riesgos. Para ello se han identificado los principales objetivos que se persiguen al realizar un análisis de riesgos de acuerdo a lo expuesto en, **[GOME 03]**:

- Identificar, evaluar y manejar los riesgos de seguridad.
- Estimar la exposición de un activo a una amenaza determinada.

- Determinar cuál combinación de medidas de seguridad proporcionará un nivel de seguridad razonable a un costo aceptable.
- Tomar mejores decisiones en seguridad informática.
- Enfocar recursos y esfuerzos en la protección de los activos.

2.2. Fases del análisis de riesgos

Si bien existen diferentes metodologías que indican cómo llevar a cabo un análisis de riesgos, de forma general y sin hacer referencia a ninguna metodología en particular, el proceso de análisis de riesgos debe contemplar las siguientes fases según lo expuesto en, **[GOME 03]**:

- Determinar los activos relevantes para la Organización
- Valorar los activos identificados
- Determinar las amenazas a las que están expuestos los activos
- Estimar el impacto de la amenaza
- Calcular el nivel de riesgo. Estimar el riesgo.

El análisis de riesgos clasifica los riesgos identificados y proporciona datos para la evaluación y el tratamiento de los mismos. En el análisis del riesgo no sólo se tienen en cuenta las fuentes del riesgo sino que también deben considerarse las consecuencias que puedan provocar la materialización del riesgo y las probabilidades de que dicha materialización ocurra.

El análisis de riesgos (o del riesgo) tiene como objetivo identificar los riesgos (mediante la identificación de sus elementos) y lograr establecer el Riesgo Total (o exposición bruta al riesgo) y el Riesgo Residual (Riesgo remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información **[MAGE 06]**), bien sea en términos cuantitativos o en términos cualitativos.

Realizar un correcto análisis de riesgos es indispensable para lograr una gestión adecuada de los mismos. Los riesgos necesitan ser analizados para decidir cuáles son los factores de riesgo que potencialmente tendrían un mayor efecto y por tanto necesitan ser tratados o gestionados.

Una vez llevadas a cabo las fases del análisis de riesgos se obtendrá un mapa de los riesgos a los que está expuesta una organización y se procederá a su gestión o tratamiento.

En la figura 3.2, se puede observar el marco del análisis de riesgos.

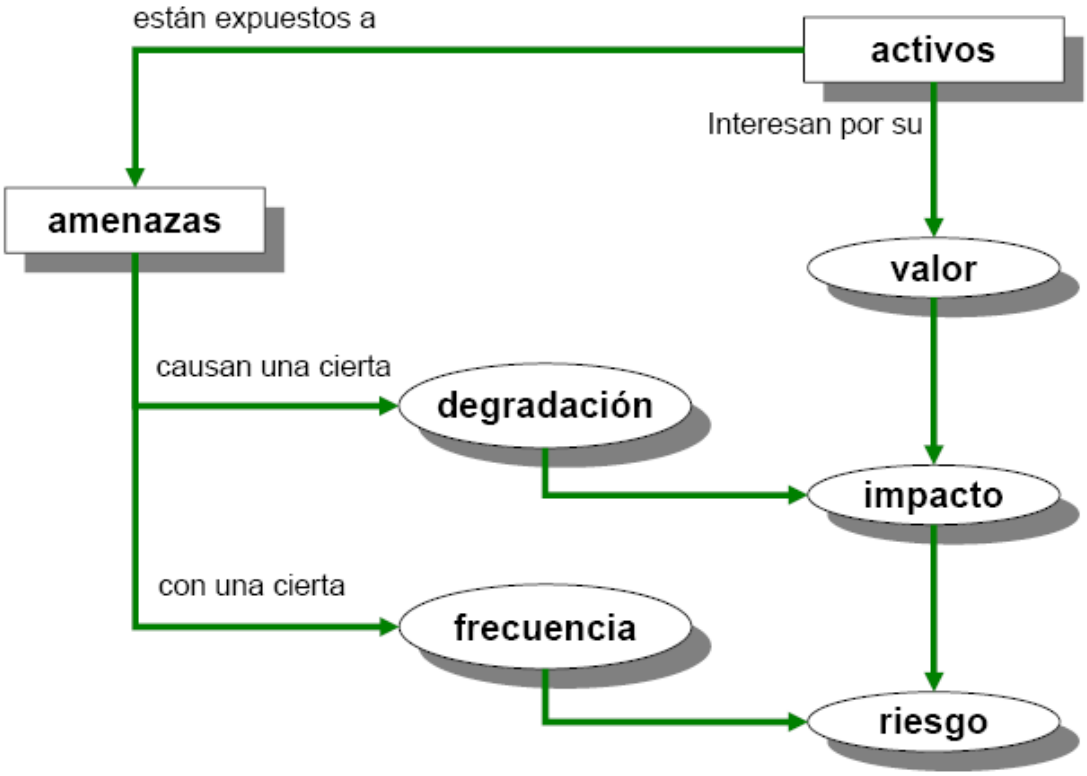


Figura 3.2. Marco del análisis de riesgos. [MAGE 06]

3. La gestión de riesgos

Una vez conceptualizado el análisis de riesgos, ahora entraremos a definir lo que es la gestión de riesgos, como el proceso que nos permitirá tratar los riegos identificados y mitigar su impacto.

En Magerit **[MAGE 06]**, se define la gestión de riesgos como la "Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados."

Selección e implantación de las medidas o 'salvaguardas' de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios. La gestión de riesgos se basa en los resultados obtenidos en el análisis de los riesgos.

3.1. Fases de la gestión de riesgos

De forma general, la gestión de riesgos sigue las siguientes fases:

- Determinación de los criterios de aceptación del riesgo
- Determinación de las medidas de seguridad necesarias (establecimiento de salvaguardas).
- Estimación del impacto residual
- Estimación del nivel de riesgo residual

La gestión de riesgos permite tomar las decisiones necesarias para el tratamiento de los riesgos, definiendo las salvaguardas necesarias para mitigar o impedir los riesgos identificados.

Pero no basta solo con determinar dichas salvaguardas, es necesario evaluarlas para lo cual, se debe evaluar el impacto de las amenazas identificadas en el análisis de riesgos, tras aplicar las medidas de seguridad o salvaguardas, lo cual determinará el impacto residual, que es el impacto remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información, **[MAGE 06]**), si las salvaguardas aplicadas son eficaces, el impacto residual en este punto debería ser despreciable.

De igual forma se debe realizar una estimación del nivel de riesgo residual, que es el riesgo remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información, **[MAGE 06]**. De igual forma que con el impacto residual, si las salvaguardas aplicadas son eficaces, el riesgo residual en este punto debería ser despreciable.

Si tanto el impacto como el riesgo residual tuviesen un nivel importante, es necesario revisar el análisis de riesgos efectuado y repetir el proceso.

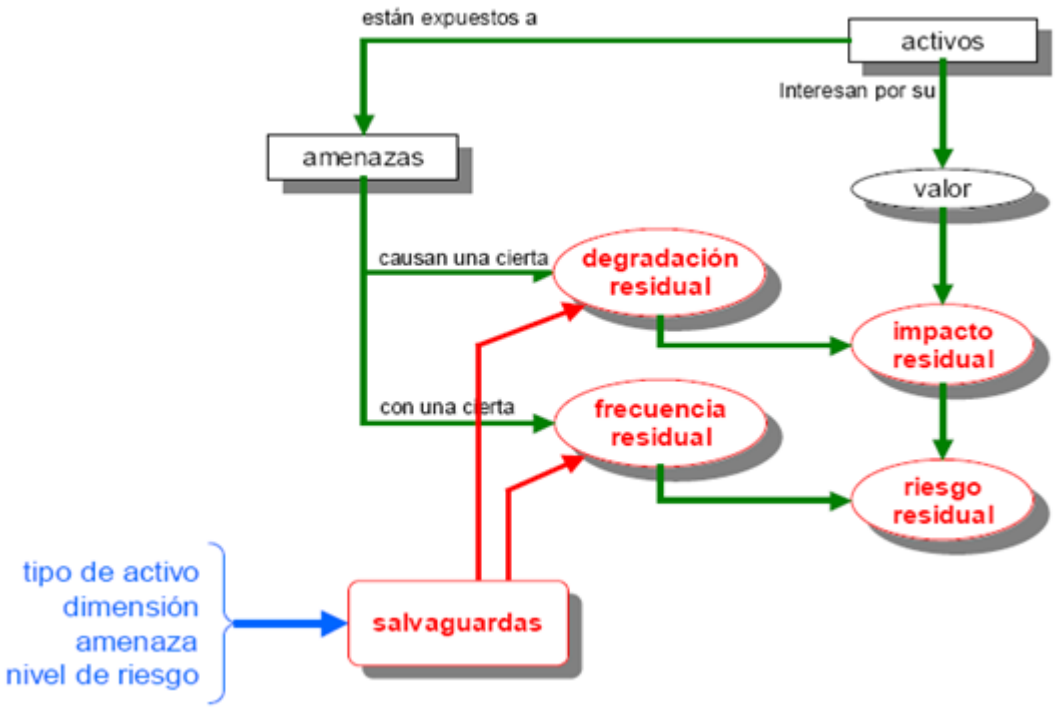


Figura 3.3. Marco de la gestión de riesgos. [MAGE 06]

4. El análisis y gestión de riesgos en su contexto

Tal y como se indica en **[MAGE 06]**, las tareas de análisis y gestión de riesgos no son un fin en sí mismas sino que se encajan en la actividad continua de gestión de la seguridad.

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

La implantación de los controles de seguridad requiere una organización gestionada y la participación informada de todo el personal que trabaja con el

sistema de información. Es este personal el responsable de la operación diaria, de la reacción ante incidencias y de la monitorización en general del sistema para determinar si satisface con eficacia y eficiencia los objetivos propuestos.

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

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

5. Cuándo procede analizar y gestionar los riesgos

Conforme a lo expuesto en **[MAGE 06]**, realizar un análisis de riesgos es laborioso y costoso. Levantar un mapa de activos y valorarlos requiere la colaboración de muchos perfiles dentro de la Organización, desde los niveles de gerencia hasta los técnicos. Y no solo es que haya que involucrar a muchas personas, sino que hay que lograr una uniformidad de criterio entre todos pues, si importante es cuantificar los riesgos, más importante aún es relativizarlos. Y esto es así porque típicamente en un análisis de riesgos aparecen multitud de datos. La única forma de afrontar la complejidad es centrarse en lo más importante (máximo impacto, máximo riesgo) y obviar lo que es secundario o incluso despreciable.

Un análisis de riesgos es recomendable en cualquier Organización que dependa de los sistemas de información y comunicaciones para el cumplimiento de su misión. En particular en cualquier entorno donde se practique la tramitación electrónica de bienes y servicios, sea en contexto público o privado. El análisis de riesgos permite tomar decisiones de inversión en tecnología, desde la adquisición de equipos de producción hasta el despliegue de un centro alternativo para

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

El análisis de riesgos es una herramienta de gestión que permite tomar decisiones. Las decisiones pueden tomarse antes de desplegar un servicio o con éste funcionando. Es muy deseable hacerlo antes, de forma que las medidas que haya que tomar se incorporen en el diseño del servicio, en la elección de componentes, en el desarrollo de las aplicaciones y en los manuales de usuario. Todo lo que sea corregir riesgos imprevistos es costoso en tiempo propio y ajeno, lo que puede ir en detrimento de la imagen prestada por la Organización y puede suponer, en último extremo, la pérdida de confianza en su capacidad.

CAPÍTULO IV: Estándares, Marcos de Trabajo y Guías y Normas para la Auditoría de Sistemas de Información

1. Introducción

En el campo de la auditoría informática existen diversas metodologías, estándares y marcos de trabajo, que ofrecen las pautas necesarias de un lado para asegurar estos sistemas a través del establecimiento de controles, y por otro para realizar tareas de auditoría. En este trabajo abordaremos aquellos de mayor relevancia tanto en el ámbito nacional como internacional y que se ajustan a los objetivos y ámbito del trabajo.

Iniciaremos nuestro estudio con la familia ISO 27000 que ofrece un conjunto de estándares que permite el aseguramiento, control y adecuada gestión de la seguridad de la información y de los sistemas a través de los cuales esta es procesada y transmitida; de especial interés para el trabajo son los estándares ISO/ IEC 27001, 27002, 27002, 27005 (que será tratado en el capítulo V) y 27007, este último estándar específico para auditoría de un Sistema de Gestión de Seguridad de la Información.

Abordaremos dos marcos de trabajo y de buenas prácticas como son CoBiT e ITIL, el primero de interés como marco de trabajo de control interno para Tecnologías de la Información y el segundo ofrece un conjunto de mejores prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información de forma eficaz, segura y controlada.

También estudiaremos la auditoría de sistemas de información, dentro del Esquema Nacional de Seguridad, como un referente de prácticas recomendadas a ser aplicadas dentro de la administración pública.

Finalmente abordaremos las guías de auditoría sugeridas y recomendadas por instituciones reconocidas como son ISACA y “The Institute of Internal Auditors -IIA-”, las cuales ofrecen directrices generales para llevar a cabo una auditoría informática.

2. La familia ISO/IEC 27000

ISO/IEC 27000 es un conjunto de estándares desarrollados (algunos en fase de desarrollo) por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. Los rangos de numeración reservados por ISO para esta serie van de 27000 a 27019 y de 27030 a 27044.

A continuación se listan las normas que componen dicha serie, con una breve descripción de cada una. Posteriormente ampliaremos aquellas que sean de particular importancia para el ámbito de este trabajo, **[AIFC 08]**.

- **ISO 27000:** Contiene términos y definiciones que se emplean en toda la serie 27000.
- **ISO 27001:** Es la norma principal de la serie y contiene los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI). Tiene su origen en la BS 7799-2:2002 y es la norma con la cual se certifican, por auditores externos, los SGSI de las organizaciones.
- **ISO 27002:** Es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.
- **ISO 27003:** Guía de implementación de SGSI e información acerca del uso del modelo PDCA (Plan-Do-Check-Act) y de los requerimientos de sus diferentes fases.
- **ISO 27004:** Guía de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Do” (Implementar y Utilizar) del ciclo PDCA.
- **ISO 27005:** Guía de técnicas para la gestión del riesgo de la seguridad de la información y servirá, por tanto, de apoyo a la ISO 27001 y a la implantación de un SGSI. Recoge partes de ISO/IEC TR 13335.

- **ISO 27006:** Requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.
- **ISO 27007:** Guía de auditoría de un SGSI.
- **ISO 27011:** Guía de gestión de seguridad de la información específica para telecomunicaciones.
- **ISO 27012:** Guía de gestión de seguridad de la información específica para la industria automotriz.
- **ISO 27013:** Guía de gestión de seguridad de la información específica para la asociación mundial de loterías.
- **ISO 27014:** Guía de gestión de seguridad de la información específica para sistemas de información en los transportes.
- **ISO 27031:** Guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.
- **ISO 27032:** Guía relativa a la ciberseguridad.
- **ISO 27033:** Es una norma consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante gateways, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes. Proviene de la revisión, ampliación y renumeración de ISO 18028.
- **ISO 27034:** Guía de seguridad en aplicaciones.
- **ISO 27799:** Estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 17799 (actual ISO 27002).

2.1. ISO/IEC 27001: Tecnologías de la información – Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos

La norma ISO/IEC 27001, **[ISO/IEC 05a]**, especifica los requisitos para establecer, implantar, documentar y evaluar un Sistema de Gestión de la Seguridad de la Información (SGSI), de acuerdo a la Norma ISO 27002, dentro del

contexto de los riesgos identificados por la Organización, **[INTE 10]**. Esta norma es aplicable a cualquier tipo de organización.

La norma ISO/IEC 27001 está basada en un enfoque por procesos y en la mejora continua. Es, por lo tanto, compatible e integrable con el resto de sistemas de gestión que ya existan en una organización.

ISO 27001 está basada en el modelo de proceso Plan-Do-Check-Act (Planificar-Hacer-Chequear-Actuar), también conocido como círculo de Deming y que se resume en la figura 4.1.

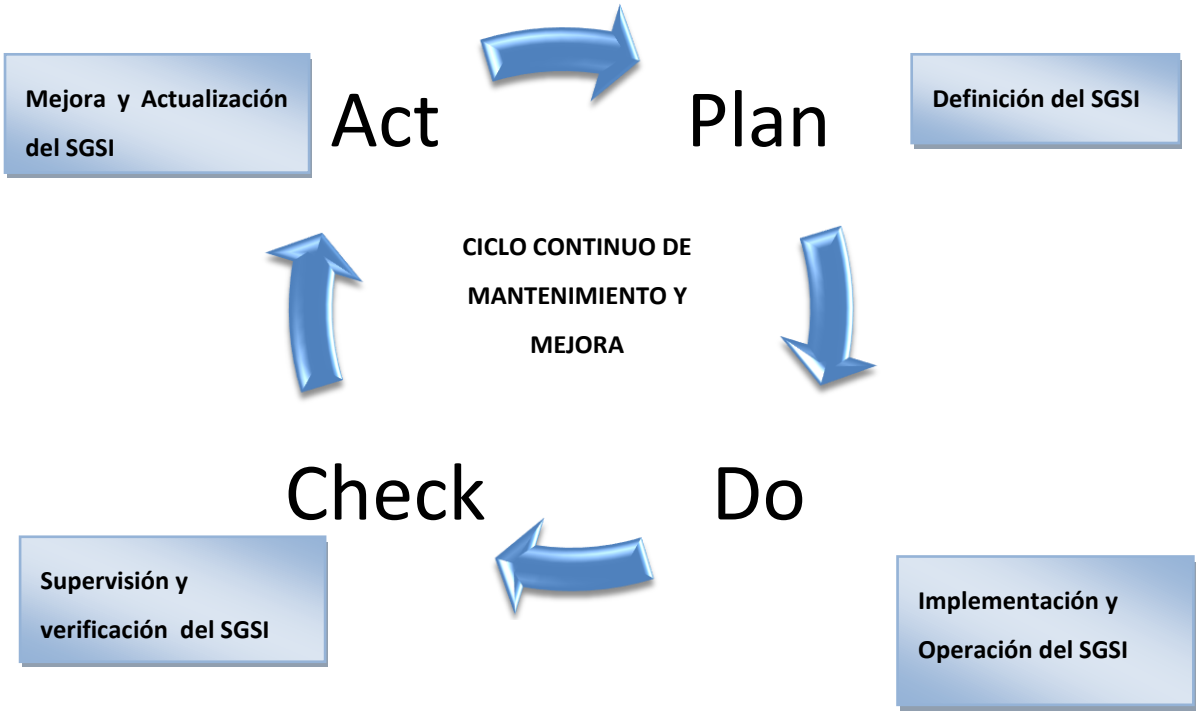


Figura 4.1. Ciclo Deming en la ISO/IEC 27001

De acuerdo al modelo PDCA mencionado, las etapas del SGSI definido por la ISO 27001 son las que se relacionan a continuación:

1. **Plan (planificar):** Definición del SGSI:
   - Delimitación del escenario que cubre el SGSI.
   - Definición de la política de seguridad incluyendo objetivos y estrategia de gestión de riesgos.

- Diseño del método de gestión de riesgos.
- Evaluación de riesgos inicial, delimitación de riesgo residual.
- Estado de aplicabilidad, definición de controles y excepciones.

2. **Do (hacer):** Implementación y operación del SGSI:
   - Plan de acción para el tratamiento de los riesgos.
   - Implementación de los controles.
   - Formación y adiestramiento.
3. **Check (chequear):** Supervisión y verificación del SGSI
   - Seguimiento de los objetivos marcados.
   - Adaptación de buenas prácticas.
   - Programas de revisiones y auditorías.
4. **Act (actuar):** Mejora y actualización del SGSI
   - Adoptar acciones preventivas.
   - Adoptar acciones correctivas.

La norma ISO/IEC 27001, **[ISO/IEC 05a]**, está estructurada en 9 capítulos y 3 anexos:

Capítulo 1. Introducción: Generalidades e introducción al método PDCA.

Capítulo 2. Alcance y campo de aplicación: En este capítulo se especifica el alcance de la norma, la aplicación y el tratamiento de exclusiones.

Capítulo 3. Referencias Normativas: Se mencionan aquellas normas que sirven de referencia y que son necesarias para la aplicación de esta norma.

Capítulo 4. Términos y definiciones: Breve descripción de los términos más usados en la norma.

Capítulo 5. Sistema de Gestión de la Seguridad de la Información: Capítulo que aborda aspectos de cómo crear, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI, así como establecer los requisitos de documentación y el control de la misma.

Capítulo 6. Responsabilidad de la dirección: Indica la responsabilidad de la dirección en cuanto a compromiso con el SGSI, gestión y provisión de recursos y concienciación, formación y capacitación del personal.

Capítulo 7. Auditorías internas del SGSI: Este capítulo trata de cómo realizar las auditorías internas de control y cumplimiento.

Capítulo 8. Revisión del SGSI por la dirección: En este capítulo se proporcionan las claves de actuación para gestionar el proceso periódico de revisión del SGSI por parte de la dirección.

Capítulo 9. Mejoramiento del SGSI: Acciones de mejora continua, acciones correctivas y acciones preventivas.

Anexo A. Objetivos de control y controles: Anexo normativo que enumera los objetivos de control y controles que se encuentran detallados en la norma ISO 27002:2005.

Anexo B. Relación con los Principios de la OCDE: Anexo informativo con la correspondencia entre los apartados de la ISO 27001 y los principios de buen gobierno de la OCDE.

Anexo C. Correspondencia con otras normas: Anexo informativo con una tabla de correspondencia de cláusulas con ISO 9001 e ISO 14001.

2.2. ISO/IEC 27002:2005: Tecnologías de la información – Técnicas de Seguridad - Código de buenas prácticas para la Gestión de la Seguridad de la Información.

ISO/IEC 27002:2005, **[ISO/IEC 05]**, es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios que cubren aspectos específicos de la seguridad de la información. Anteriormente esta guía era conocida como ISO 17799:2005, a partir del 1 de Julio de 2007 es renombrada, manteniendo 2005 como año de edición, esta norma no es certificable.

La norma está estructurada en 16 capítulos de los cuales, los capítulos del 0 al 4 tratan aspectos generales de la norma y los capítulos del 5 al 15 tratan cada uno de los 11 dominios, centrándose en un determinado aspecto de la seguridad de la información. En la siguiente figura se muestra la distribución de dichos dominios y el aspecto de seguridad que cubren:

Figura 4.2. Distribución de los dominios de la Norma ISO 27002. [INTE10]

A continuación se presenta una breve descripción de cada uno de los capítulos de la norma y se indican los objetivos de control y los controles para cada dominio, los cuales han sido tomados y adaptados de **[RUBI 09]** y de **[ISO/IEC 05a]**:

Capítulo 0. Introducción: conceptos generales de seguridad de la información y SGSI.

Capítulo 1. Campo de aplicación: Se especifica el objetivo de la norma y su campo de aplicación.

Capítulo 2. Términos y definiciones: Breve descripción de los términos más usados en la norma.

Capítulo 3. Estructura del estándar: Descripción de la estructura de la norma.

Capítulo 4. Evaluación y tratamiento del riesgo: Indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.

Capítulo 5. Política de seguridad: El objetivo de este dominio es establecer controles que permitan brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes, a través de la elaboración y aprobación de un documento de política de seguridad, el cual debe darse a conocer a toda la organización y a los interesados externos.

- **Política de seguridad de la información. Controles**
  - Documento de política de seguridad de la información.
  - Revisión de la política de seguridad de la información.

Capítulo 6. Aspectos organizativos de la seguridad de la información: El objetivo de este dominio es establecer controles a través de los cuales se pueda gestionar la seguridad de la información dentro de la organización y mantener la seguridad de la información y de los servicios de procesamiento de información de la organización a los cuales tienen acceso partes externas o que son procesados, comunicados o dirigidos por éstas.

- **Organización interna**.
  - Compromiso de la Dirección con la seguridad de la información.
  - Coordinación de la seguridad de la información.
  - Asignación de responsabilidades relativas a la seguridad de la información.
  - Proceso de autorización de recursos para el tratamiento de la información.
  - Acuerdos de confidencialidad.
  - Contacto con las autoridades.

- Contacto con grupos de especial interés.
- Revisión independiente de la seguridad de la información.

- **Terceros.**
  - Identificación de los riesgos derivados del acceso de terceros.
  - Tratamiento de la seguridad en la relación con los clientes.
  - Tratamiento de la seguridad en contratos con terceros.

Capítulo 7. Gestión de activos: Este dominio busca establecer controles que permitan lograr y mantener la protección adecuada de los activos de la organización, definiendo responsabilidad sobre los activos y realizando clasificación de la información.

- **Responsabilidad sobre los activos.**
  - Inventario de activos.
  - Propiedad de los activos.
  - Uso aceptable de los activos.
- **Clasificación de la información.**
  - Directrices de clasificación.
  - Etiquetado y manipulado de la información.

Capítulo 8. Seguridad ligada a los recursos humanos: Con este dominio se pretende establecer controles que conduzcan a asegurar que los empleados, contratistas y usuarios de terceras partes, entienden sus responsabilidades y sean aptos para las funciones para las cuales están considerados, y reducir el riesgo de robo, fraude, o uso inadecuado de las instalaciones. De igual forma se busca que sean conscientes de las amenazas y preocupaciones respecto a la seguridad de la información, sus responsabilidades y sus deberes, y que estén equipados para apoyar la política de seguridad de la organización en el transcurso de su trabajo normal, y así ayudar a reducir el riesgo de error humano. Todos estos han de tenerse en cuenta antes del empleo; durante el empleo; una vez ha cesado el empleo o cuando hay un cambio de puesto de trabajo.

- **Antes del empleo:** funciones y responsabilidades; investigación de antecedentes; términos y condiciones de contratación.
- **Durante el empleo:** Responsabilidades de la Dirección; concienciación, formación y captación en seguridad de la información; proceso disciplinario.
- **Cese del empleo o cambio de puesto de trabajo:** Responsabilidad de cese o cambio; devolución de activos: retirada de los derechos de acceso.

Capítulo 9. Seguridad física y ambiental: Con este dominio se busca establecer controles que permitan evitar el acceso físico no autorizado, el daño o la interferencia en las instalaciones y a la información de la organización, de igual forma evitar la pérdida, daño, robo o puesta en peligro de los activos, y la interrupción de las actividades de la organización

- **Áreas seguras.**
  - Perímetro de seguridad física.
  - Controles físicos de entrada.
  - Seguridad de oficinas, despachos e instalaciones.
  - Protección contra las amenazas externas y de origen ambiental.
  - Trabajo en áreas seguras.
  - Áreas de acceso público y de carga y descarga.
- **Seguridad de los equipos.**
  - Emplazamiento y protección de equipos.
  - Instalaciones de suministro.
  - Seguridad del cableado.
  - Mantenimiento de los equipos.
  - Seguridad de los equipos fuera de las instalaciones.
  - Reutilización o retirada segura de equipos.
  - Retirada de materiales propiedad de la empresa.

Capítulo 10. Gestión de comunicaciones y operaciones: Este dominio está orientado al establecimiento de controles que permitan asegurar la operación correcta y segura de los servicios de procesamiento de información, e implementar y mantener un grado adecuado de seguridad de la información de la prestación del servicio, de conformidad con los acuerdos de prestación del servicio por terceros.

- **Responsabilidades y procedimientos de operación.**
  - Documentación de los procedimientos de operación.
  - Gestión de cambios.
  - Segregación de tareas.
  - Separación de los recursos de desarrollo, prueba y operación.
- **Gestión de la provisión de servicios por terceros.**
  - Provisión de servicios.
  - Supervisión y revisión de los servicios prestados por terceros.
  - Gestión del cambio en los servicios prestados por terceros.
- **Planificación y aceptación del sistema.**
  - Gestión de capacidades.
  - Aceptación del sistema.
- **Protección contra el código malicioso y descargable.**
  - Controles contra el código malicioso.
  - Controles contra el código descargado en el cliente.
- **Copias de seguridad.**
  - Copias de seguridad de la información.
- **Gestión de la seguridad de las redes.**
  - Controles de red.
  - Seguridad de los servicios de red.
- **Manipulación de los soportes.**
  - Gestión de soportes extraíbles.
  - Retirada de soportes.
  - Procedimientos de manipulación de la información.

- Seguridad de la documentación del sistema.

- **Intercambio de información.**
  - Políticas y procedimientos de intercambio de información.
  - Acuerdos de intercambio.
  - Soportes físicos en tránsito.
  - Mensajería electrónica.
  - Sistemas de información empresariales.
- **Servicios de comercio electrónico.**
  - Comercio electrónico.
  - Transacciones en línea.
  - Información públicamente disponible.
- **Supervisión.**
  - Registros de auditoría.
  - Supervisión del uso del sistema.
  - Protección de la información de los registros.
  - Registros de administración y operación.
  - Registro de fallos.
  - Sincronización del reloj.

Capítulo 11. Control de acceso: El objetivo de este dominio es permitir controlar el acceso a la información de la organización con base en los requisitos de seguridad y del negocio, asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información.

- **Requisitos de negocio para el control de acceso.**
  - Política de control de acceso.
- **Gestión de acceso de usuario.**
  - Registro de usuario.
  - Gestión de privilegios.
  - Gestión de contraseñas de usuario.
  - Revisión de los derechos de acceso de usuario.
- **Responsabilidades de usuario.**

- Uso de contraseñas.
- Equipo de usuario desatendido.
- Política de puesto de trabajo despejado y pantalla limpia.

- **Control de acceso a la red.**
  - Política de uso de los servicios en red.
  - Autenticación de usuario para conexiones externas.
  - Identificación de los equipos en las redes.
  - Protección de los puertos de diagnóstico y configuración remotos.
  - Segregación de las redes.
  - Control de la conexión a la red.
  - Control de encaminamiento (routing) de red.
- **Control de acceso al sistema operativo.**
  - Procedimientos seguros de inicio de sesión.
  - Identificación y autenticación de usuario.
  - Sistema de gestión de contraseñas.
  - Uso de los recursos del sistema.
  - Desconexión automática de sesión.
  - Limitación del tiempo de conexión.
- **Control de acceso a las aplicaciones y a la información.**
  - Restricción del acceso a la información.
  - Aislamiento de sistemas sensibles.
- **Ordenadores portátiles y teletrabajo.**
  - Ordenadores portátiles y comunicaciones móviles.
  - Teletrabajo.

Capítulo 12. Adquisición, desarrollo y mantenimiento de los sistemas de información: Este dominio busca establecer controles que permitan: mantener la seguridad en los procesos de adquisición, mantenimiento y desarrollo del software, garantizando que la seguridad es parte integral de los sistemas de información; evitar errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones; proteger la confidencialidad, autenticidad o integridad de la información por medios criptográficos; garantizar

la seguridad de los archivos del sistema, y de la información de los sistemas de aplicaciones.

- **Requisitos de seguridad de los sistemas de información.**
  - Análisis y especificación de los requisitos de seguridad.
- **Tratamiento correcto de las aplicaciones.**
  - Validación de los datos de entrada.
  - Control del procesamiento interno.
  - Integridad de los mensajes.
  - Validación de los datos de salida.
- **Controles criptográficos.**
  - Política de uso de los controles criptográficos.
  - Gestión de claves.
- **Seguridad de los archivos de sistema.**
  - Control del software en explotación.
  - Protección de los datos de prueba del sistema.
  - Control de acceso al código fuente de los programas.
- **Seguridad en los procesos de desarrollo y soporte.**
  - Procedimientos de control de cambios.
  - Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - Restricciones a los cambios en los paquetes de software.
  - Fugas de información.
  - Externalización del desarrollo de software.
- **Gestión de la vulnerabilidad técnica.**
  - Control de las vulnerabilidades técnicas.

Capítulo 13. Gestión de incidentes de seguridad de la información: El objetivo de este dominio es establecer controles que permitan asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información, se comunican de forma tal que permitan tomar las acciones correctivas oportunamente.

- **Notificación de eventos y puntos débiles de seguridad de la información.**
  - Notificación de los eventos de seguridad de la información.
  - Notificación de puntos débiles de seguridad.
- **Gestión de incidentes y mejoras de seguridad de la información.**
  - Responsabilidades y procedimientos.
  - Aprendizaje de los incidentes de seguridad de la información.
  - Recopilación de evidencias.

Capítulo 14. Gestión de la continuidad del negocio: Con este dominio se busca establecer controles orientados a contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallos importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.

- **Aspectos de seguridad de la información en la gestión de la continuidad del negocio.**
  - Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
  - Continuidad del negocio y evaluación de riesgos.
  - Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.
  - Marco de referencia para la planificación de la continuidad del negocio.
  - Pruebas, mantenimiento y revaluación de planes de continuidad.

Capítulo 15. Cumplimiento: El objetivo de este dominio es el establecimiento de controles tendentes a evitar el incumplimiento de cualquier ley, de obligaciones estatuarias reglamentarias o contractuales y de cualquier requisito de seguridad.

- **Cumplimiento de los requisitos legales.**
  - Identificación de la legislación aplicable.

- Derechos de propiedad intelectual (DPI).
- Protección de los documentos de la organización.
- Protección de datos y privacidad de la información de carácter personal.
- Prevención del uso indebido de recursos de tratamiento de la información.
- Regulación de los controles criptográficos.

- **Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.**
  - Cumplimiento de las políticas y normas de seguridad.
  - Comprobación del cumplimiento técnico.
- **Consideraciones sobre las auditorías de los sistemas de información.**
  - Controles de auditoría de los sistemas de información.
  - Protección de las herramientas de auditoría de los sistemas de información.

2.3. ISO/IEC 27004:2009: Tecnologías de la información – Técnicas de Seguridad – Mediciones para la Gestión de la Seguridad de la Información

El estándar ISO/IEC 27004:2009, es una guía para el desarrollo y uso de métricas para evaluar la efectividad de un Sistema de Gestión de Seguridad de la Información (SGSI) y sus controles o grupo de controles, como se especifica en ISO/IEC 27001. Es un estándar que se aplica para cualquier tipo de organización, y permite desarrollar criterios para la medición de la eficacia y eficiencia de un SGSI, implementado a través del estándar ISO/IEC 27001.

Tal y como se indica en el documento oficial de la norma, **[ISO/IEC 09]**: "El empleo de este estándar permitirá a las organizaciones dar respuesta a los interrogantes de cuán efectivo y eficiente es el SGSI y qué niveles de implementación y madurez han sido alcanzados. Estas mediciones permitirán comparar los logros obtenidos en seguridad de la información sobre períodos de

tiempo en áreas de negocio similares de la organización y como parte de continuas mejoras".

Los objetivos de las mediciones a realizar a través de esta estándar son:

- Evaluar la eficiencia del SGSI
- Evaluar la efectividad de la implementación de la ISO/IEC 27001 sobre los controles de seguridad.
- Comunicar a la organización valores de seguridad
- Proporcionar estados de seguridad que guíen las revisiones del SGSI
- Servir como entradas al plan de análisis y tratamiento de riesgos

Esta norma, tal y como se indica en **[ISO/IEC09]**, ofrece recomendaciones sobre las actividades que deben desarrollarse para que una organización cumpla con los requisitos de medición especificados en la norma ISO / IEC 27001 y que citamos a continuación:

a) Desarrollo de medidas: medidas de base, medidas derivadas e indicadores.
b) Implementación y operación de un programa de medición de seguridad de la Información.
c) Recogida y análisis de datos.
d) Elaboración de resultados de la medición.
e) Comunicación de resultados de las medidas desarrolladas a las partes interesadas.
f) Utilizar los resultados de medición como factores que contribuyen a las decisiones relacionadas con el SGSI.
g) Utilizar los resultados de la medición para determinar las necesidades para mejorar el SGSI implementado, incluyendo su ámbito de aplicación, las políticas, objetivos, controles, procesos y procedimientos.
h) Facilitar la mejora continua de la seguridad de la información

El estándar ISO/IEC 27004, al igual que ISO/IEC 27001 está orientado a procesos y se basa en el modelo Plan-Do-Check-Act, consistente en una relación

cíclica de entrada y salida de las actividades de medición, cuyos fundamentos para esta norma resumimos en la figura 4.3.:

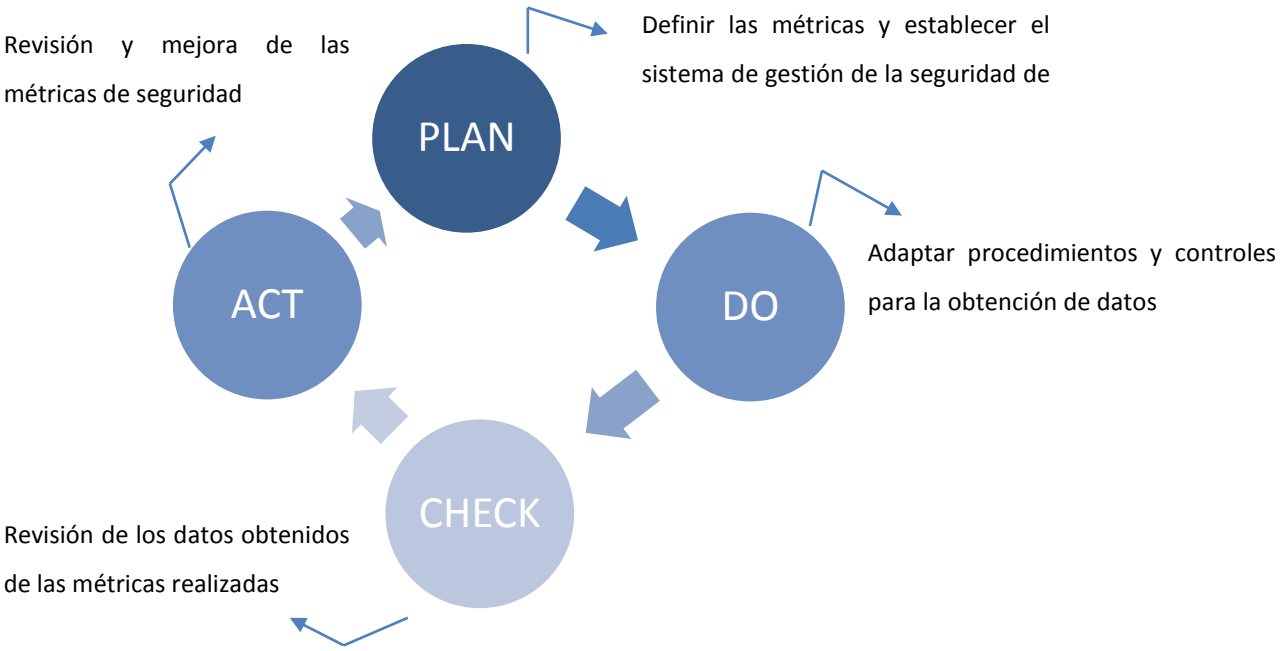


Figura 4.3. Ciclo PDCA ISO/IEC 27004

La norma se encuentra estructurada en 11 capítulos y dos anexos, que describimos a continuación[2]:

0. **Introduction**: Generalidades e introducción a la norma.
1. **Scope:** En este capítulo se especifica el alcance de la norma y su ámbito de aplicación.

[2] Hemos conservado el título de cada capítulo en inglés extraído del documento oficial, al no encontrar una traducción oficial de estos, las descripciones que presentamos han sido extractadas y adaptadas de **[ISO/IEC 09], [DIAZ 10], [LARR 09], [ISSA 11a]**.

2. **Normative References:** En este capítulo de indican los estándares que sirven de referencia y que son necesarios para la aplicación de este estándar, que en este caso son la ISO/IEC 27000:2009 y la ISO/IEC 27001:2005.
3. **Terms and Definitions:** En este capítulo se hace una descripción de los términos fundamentales usados en el estándar.
4. **Structure of this International Standard:** En este capítulo se describe la estructura general del estándar.
5. **Information security measurement overview:** Consideraciones generales sobre la medición de la seguridad, factores de éxito y modelo de medición.
6. **Management responsibilities:** Responsabilidades de la Dirección para medir la eficacia del SGSI. La dirección es responsable de establecer el programa de medición de seguridad de la información, con la participación de las partes interesadas en las actividades de medición; la aceptación de los resultados de medición para el análisis de la gestión y el uso de medición de los resultados en la mejora de las actividades dentro del SGSI.
7. **Measures and measurement development**: Desarrollo de métricas y la forma de medición. Consiste en la identificación y desarrollo de las medidas y la medición para la evaluación de la eficacia del SGSI implementado. Las actividades necesarias para desarrollar las métricas y la medición incluyen las siguientes:
    a) Definición de los procesos
    b) El desarrollo de mediciones aplicables.
    c) La implementación del programa.
    d) Revisión de mediciones.
8. **Measurement operation**: Actividades imprescindibles para asegurar que los resultados obtenidos proporcionan información precisa para la medición de la eficacia del sistema y para la adopción de acciones de mejora. Incluye operaciones que son esenciales para asegurar que los resultados obtenidos en la medición proporcionen información precisa con respecto a la eficacia de una aplicación SGSI, controles o grupo de controles y la necesidad de acciones de mejora apropiadas. Las actividades que se incluyen son las siguientes:

1. La integración de los procedimientos de medición en el funcionamiento general de SGSI.
2. Reunir, almacenar y verificar los datos.

9. **Analysis and measurement results reporting:** Análisis de los datos recogidos y reporte y comunicación de los mismos. Las actividades a seguir son las que siguen:
    a) El análisis de los datos y el desarrollo de resultados de la medición,
    b) Comunicar resultados de las mediciones a las partes interesadas.
10. **Information Security Measurement Programme Evaluation and Improvement:** Revisión periódica del programa de medición de cara a verificar su corrección y vigencia, así como las mejoras a implementar en el mismo. La organización debe evaluar a intervalos planificados lo siguiente:
    a) La eficacia de la aplicación de medición de seguridad de la información para asegurarse de que:
        i. Produce resultados de medición de una manera eficaz.
        ii. Se ejecuta según lo previsto.
    b) Los cambios de direcciones en el SGSI implementado y / o controles.
    c) Cambios de direcciones en el entorno (por ejemplo, los requisitos, la legislación o la tecnología),
    d) Utilidad de los resultados de medición desarrollados para garantizar que se satisfagan las necesidades de información pertinentes. La administración debe especificar la frecuencia de dicha evaluación, el plan de revisiones periódicas y establecer los mecanismos para hacer posibles revisiones. Las actividades correspondientes son las que siguen:
        i. Determinar los criterios de evaluación para la medición de la seguridad de la información.
        ii. Supervisar, revisar y evaluar la medición.
        iii. Implementar mejoras

Anexo A: Template for an information security measurement construct: Este anexo consiste en una plantilla para la elaboración de métricas.

Anexo B: Measurement construct examples: En este anexo se encuentran ejemplos de métricas realizadas con la plantilla mencionada anteriormente.

2.4. ISO/IEC 27007:2011: Information technology — Security Techniques — Guidelines for Information Security Management Systems Auditing [3]

Este estándar publicado en noviembre de 2011, proporciona una guía sobre el programa de auditoría para un sistema de gestión de seguridad de la información (SGSI), sobre la realización de las auditorías y de la competencia de los auditores de SGSI (además de las directrices contenidas en la norma ISO 19011).

Esta norma es aplicable a aquellos que necesitan comprender o realizar auditorías internas o externas de un SGSI o para administrar un programa de auditoría del SGSI.

2.4.1. Características y ventajas principales[4]

ISO/IEC 27007 proporciona orientación sobre la realización de auditorías de un SGSI, además esta guía ayudará a los auditores a asegurarse de que están llevando a cabo una auditoría de SGSI en la forma correcta.

Los auditores pueden utilizar las pautas establecidas por este estándar en cualquier tipo de organización. Es ampliamente aplicable, y su uso garantiza un enfoque de mejores prácticas a seguir al llevar a cabo auditorías de SGSI.

La auditoría de un SGSI siguiendo las directrices de esta norma, permitirá a una organización identificar las deficiencias que se puedan tener y que es preciso abordar antes de someterse a una auditoría de certificación formal.

El estándar abarca los aspectos específicos del SGSI para la auditoría de cumplimiento y que tienen que ver con:

[3] Guía para auditar Sistemas de Gestión de Seguridad de la Información

[4] La información que aparece en este apartado ha sido obtenida de **[FORU 11], [ITGO 11]** y **[WIKI 11]**

- Gestión del programa de auditoría del SGSI, esto incluye: determinar qué auditar, cuándo y cómo; asignar los auditores correspondientes, gestionar los riesgos de la auditoría, la mejora continua de los procesos.
- Realización de una auditoría de SGSI, esto incluye: planeación de los procesos de auditoría, dirección, las principales actividades de auditoría incluyendo el trabajo de campo, análisis, presentación de informes y seguimiento.
- Gestión de los auditores del SGSI, esto incluye: gestión de competencias y habilidades y evaluación.

2.4.2. Estructura del estándar[5]

- Introduction to this Standard
- Scope
- Normative References
- Terms and Definitions
- Principles of Auditing
- General
- Audit Activities
- Competence and Evaluation of Auditors

[5] Tal y como figura en el original

3. ISO/IEC 38500:2008*:* "Corporate governance of information technology"[6]

La norma ISO/IEC 38500:2008 fue publicada en junio de 2008 en base a la norma australiana AS8015:2005. Es la primera de una serie sobre normas de gobierno de Tecnologías de la Información y Comunicación – TIC.

Su objetivo tal y como se indica en [BALL 10], es proporcionar un marco de principios para que la dirección de las organizaciones lo utilice al evaluar, dirigir y monitorizar el uso de las TIC.

De acuerdo con lo expuesto en **[BALL 10]**, esta norma viene a complementar el conjunto de estándares ISO que afectan a los sistemas y tecnologías de la información (ISO/IEC 27000, ISO/IEC 20000, ISO/IEC 15504, ISO/IEC 24762, etc.) y otros marcos de trabajo como CoBiT e ITIL y fija los estándares para un buen gobierno de los procesos y decisiones empresariales relacionadas con los servicios de información y comunicación que, suelen estar gestionados tanto por especialistas en TIC internos o ubicados en otras unidades de negocio de la organización, como por proveedores de servicios externos.

La norma se aplica al gobierno de los procesos de gestión de las TIC en todo tipo de organizaciones que utilicen las tecnologías de la información, facilitando las bases para la evaluación objetiva del gobierno de las mismas. **[BALL 10]**.

La aplicación de esta norma trae consigo el poder contar con un buen gobierno de TIC, lo que conllevaría como beneficios, según lo expuesto en [BALL 10], la conformidad de la organización con:

- Los estándares de seguridad
- Legislación de privacidad
- Legislación sobre el spam
- Legislación sobre prácticas comerciales
- Derechos de propiedad intelectual, incluyendo acuerdos de licencia de software
- Regulación medioambiental

[6] Gobierno Corporativo de las Tecnologías de la Información

- Normativa de seguridad y salud laboral
- Legislación sobre accesibilidad
- Estándares de responsabilidad social

También la búsqueda de un buen rendimiento de las TIC mediante:

- Apropiada implementación y operación de los activos de TIC
- Clarificación de las responsabilidades y rendición de cuentas en lograr los objetivos de la organización
- Continuidad y sostenibilidad del negocio
- Alineamiento de las TIC con las necesidades del negocio
- Asignación eficiente de los recursos
- Innovación en servicios, mercados y negocios
- Buenas prácticas en las relaciones con los interesados (stakeholders)
- Reducción de costes
- Materialización efectiva de los beneficios esperados de cada inversión en TIC

3.1. Definiciones, Principios y Tareas

La norma incluye 19 definiciones de términos, entre los que se pueden destacar los siguientes, extraídos de **[BALL 10]**:

- **Gobierno corporativo de TIC** (Corporate Governance of IT). El sistema mediante el cual se dirige y controla el uso actual y futuro de las tecnologías de la información
- **Gestión** (Management). El sistema de controles y procesos requeridos para lograr los objetivos estratégicos establecidos por la dirección de la organización. Está sujeta a la guía y monitorización establecida mediante el gobierno corporativo.
- **Interesado** (Stakeholder). Individuo, grupo u organización que puede afectar, ser afectado, o percibir que va a ser afectado, por una decisión o una actividad

- **Uso de TIC** (Use of IT). Planificación, diseño, desarrollo, despliegue, operación, gestión y aplicación de TI para cumplir con las necesidades del negocio. Incluye tanto la demanda como la oferta de servicios de TIC por unidades de negocio internas, unidades especializadas de TI, proveedores externos y "utility services" (como los que se proveen de software como servicio).
- **Factor humano** (Human Behavior). La comprensión de las interacciones entre personas y otros elementos de un sistema con la intención de asegurar el bienestar de las personas y el buen rendimiento del sistema. Incluye la cultura, necesidades y aspiraciones de las personas como individuos y como grupo.

La norma define seis principios para un buen gobierno corporativo de las TIC, y que relacionamos a continuación, **[BALL 10]**:

- **Responsabilidad:** Los individuos y grupos dentro de la organización deben comprender y aceptar sus responsabilidades en la oferta o demanda de TI. La responsabilidad sobre una acción conlleva la autoridad para su realización.
- **Estrategia:** La estrategia de negocio de la organización tiene en cuenta las capacidades actuales y futuras de las TIC. Los planes estratégicos de las TIC satisfacen las necesidades, actuales y previstas, derivadas de la estrategia de negocio.
- **Adquisición**: Las adquisiciones de TI se hacen por razones válidas, en base a un análisis apropiado y continuo, con decisiones claras y transparentes. Hay un equilibrio adecuado entre beneficios, oportunidades, costes y riesgos tanto a corto como a largo plazo.
- **Rendimiento**: La TI está dimensionada para dar soporte a la organización, proporcionando los servicios con la calidad adecuada para cumplir con las necesidades actuales y futuras.

- **Conformidad**: La función de TI cumple todas las legislaciones y normas aplicables. Las políticas y prácticas al respecto están claramente definidas, implementadas y exigidas.
- **Factor humano**: Las políticas de TIC, prácticas y decisiones demuestran respeto al factor humano, incluyendo las necesidades actuales y emergentes de toda la gente involucrada.

La norma propone un modelo a través del cual, la dirección ha de gobernar las TIC mediante tres tareas principales, **[BALL 10]**:

- **Evaluar**: Examinar y juzgar el uso actual y futuro de las TIC, incluyendo estrategias, propuestas y acuerdos de aprovisionamiento (internos y externos).
- **Dirigir**: Dirigir la preparación y ejecución de los planes y políticas, asignando las responsabilidades al efecto. Asegurar la correcta transición de los proyectos a la producción, considerando los impactos en la operación, el negocio y la infraestructura. Impulsar una cultura de buen gobierno de TIC en la organización.
- **Monitorizar**: Mediante sistemas de medición, vigilar el rendimiento de la TIC, asegurando que se ajusta a lo planificado.

El modelo se resume gráficamente en la siguiente figura:

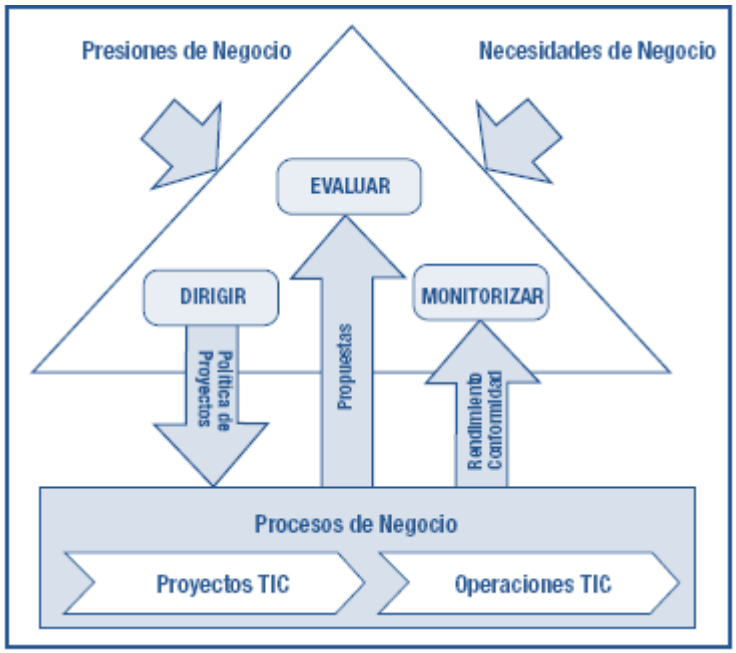


Figura 4.4. Modelo de Gobierno Corporativo de TIC. [BALL 10].

3.2. Orientaciones y Prácticas

Para cada uno de los principios citados anteriormente, la norma proporciona una breve guía u orientación sobre como evaluar, dirigir y monitorizar la función de TIC, los cuales se resumen en la figura 4.5.

Tal y como se indica en **[BALL 10]**, estas orientaciones dadas por la norma son muy generales, ya que no incluyen mecanismos, técnicas o herramientas concretas a utilizar.

Principios	Dirigir	Monitorizar	Evaluar
Responsabilidad	Planes con responsabilidad asignada	Mecanismos establecidos gobierno de TIC	Asignación responsabilidades
	Recibir información y rendir cuentas	Asignación responsabilidades (entendimiento)	Competencias de responsables
		Desempeño responsables gobierno TIC	
Estrategia	Creación y uso de planes y políticas	Progreso propuestas aprobadas	Desarrollo de TIC y procesos negocio
	Alentar propuestas innovadoras	Alcanzar objetivos en plazos establecidos	Evaluar actividades de TIC y alineamiento
		Utilizar recursos asignados	Mejores prácticas
		Uso de TIC, alcanzando beneficios esperados	Satisfacción interesados
			Valoración y evaluación riesgos
Adquisición	Activos TI adquieren manera apropiada	Inversiones y capacidades requeridas	Alternativas propuestas
	Documentos capacidad requerida	Entendimiento interno/externo necesidad negocio	Propuestas aprobadas
	Acuerdos de provisión respalden necesidades negocio		Análisis de riesgo/valor
			Inversiones
Rendimiento	Asignación recursos suficientes	Grado TIC sustenta negocio	TIC sustenta procesos de negocio dimensionado y capacidad
	Asignar prioridades y restricciones	Recursos e inversiones priorizados necesidades negocio	Riesgos: continuidad de operaciones
	Satisfacer necesidades de negocio	Políticas precisión datos	Riesgos: integridad de información, protección de activos
	Datos correctos, actualizados, protegidos	Políticas uso eficiente TIC	Decisiones uso TIC apoyo al negocio
			Eficacia y desempeño de gobierno de TIC
Cumplimiento	TI cumple obligaciones, normas y directrices	Cumplimiento y conformidad (auditorías/informes)	TIC cumple obligaciones, normas y directrices
	Establecer y aplicar políticas (uso TI interno)	Oportunos, completos, adecuados (necesidades negocio)	Conformidad gobierno TIC
	Personal TIC cumple directrices desarrollo y conducta	Actividades de TIC	
	Ética rija acciones relacionadas TIC		
Factor Humano	Actividades TI compatibles factor humano	Actividades TIC, identificar, prestar atención	Actividades de TIC, identificar
	Informar cualquier individuo (riesgos, problemas)	Prácticas de trabajo consistente uso apropiado de TIC	Actividades de TIC, considera debidamente
	Administración riesgos según políticas y procedimientos		
	Escalado a las decisiones		

Figura 4.5. Guía sobre cómo dirigir, monitorizar y evaluar la función de TIC.

[BALL 10].

4. CoBiT 4.1: Objetivos de control para la Información y la Tecnología relacionada

CoBiT, siglas en inglés de "Control Objectives for Information and related Technology", es un marco de trabajo de control interno para TI (Tecnologías de la Información), que ofrece una serie de mejores prácticas, las cuales están orientadas al control de la información y tecnología relacionada y que se ha convertido en un marco de referencia general para el gobierno de TI en las organizaciones.

CoBiT ha sido desarrollado por el Instituto de Administración de las Tecnologías de la Información – ITGI – (IT Governance Institute) en 1996. En la actualidad se encuentra disponible de manera gratuita la versión 4.1 y su actualización a la versión 5.0, también está disponible pero aún de pago.

CoBiT está formado por un grupo de productos que citamos a continuación:

• El resumen informativo al consejo sobre el gobierno de TI, 2ª Edición. Diseñado para ayudar a los ejecutivos a entender por qué el gobierno de TI es importante, cuáles son sus intereses y cuáles son sus responsabilidades para administrarlo.

• Directrices Gerenciales / Modelos de madurez. Ayudan a asignar responsabilidades, medir el desempeño, llevar a cabo benchmarks y manejar brechas en la capacidad.

• Marco de Referencia. Explica cómo CoBiT organiza los objetivos de gobierno y las mejores prácticas de TI basándose en dominios y procesos de TI y los alinea a los requerimientos del negocio.

• Objetivos de control. Brindan objetivos a la dirección basados en las mejores prácticas genéricas para todos los procesos de TI.

• Guía de Implementación de Gobierno de TI: Usando CoBiT y Val TI 2ª Edición. Proporciona un mapa de ruta para implementar gobierno TI utilizando los recursos CoBiT y Val TI.

• Prácticas de Control de CoBiT: Guía para Conseguir los Objetivos de Control para el Éxito del Gobierno de TI 2ª Edición. Proporciona una guía del porqué vale la pena implementar controles y cómo implementarlos.

• Guía de Aseguramiento de TI: Usando CoBiT. Proporciona una guía de cómo CoBiT puede utilizarse para soportar una variedad de actividades de aseguramiento junto con los pasos de prueba sugeridos para todos los procesos de TI y objetivos de control.

En este apartado vamos a abordar los aspectos fundamentales del marco de trabajo de CoBiT, como modelo para auditar la gestión y control de los sistemas de información y tecnología.

CoBiT, tal y como se indica en **[COBIT 07]**, se fundamenta en cuatro pilares que son la base de todo el marco de trabajo y que enumeramos a continuación:

- Orientado a negocios
- Orientado a procesos
- Basado en controles
- Impulsado por mediciones

CoBiT pretende con estos pilares dar respuesta a la necesidad que tienen las organizaciones de contar con un marco de trabajo para su gobierno y control de TI y que permita:

- la alineación de sus estrategias de negocio y de TI
- contar con un enfoque de procesos que facilite la definición del alcance y el nivel de cobertura y con estructura claramente definida
- ser generalmente aceptado
- ser consistente con otros estándares e independiente de tecnologías
- proveer un lenguaje simple y comprensible para todos los interesados
- cumplir con requerimientos de entidades reguladoras

En la figura 4.6, se puede observar el principio básico en que se fundamenta CoBiT.

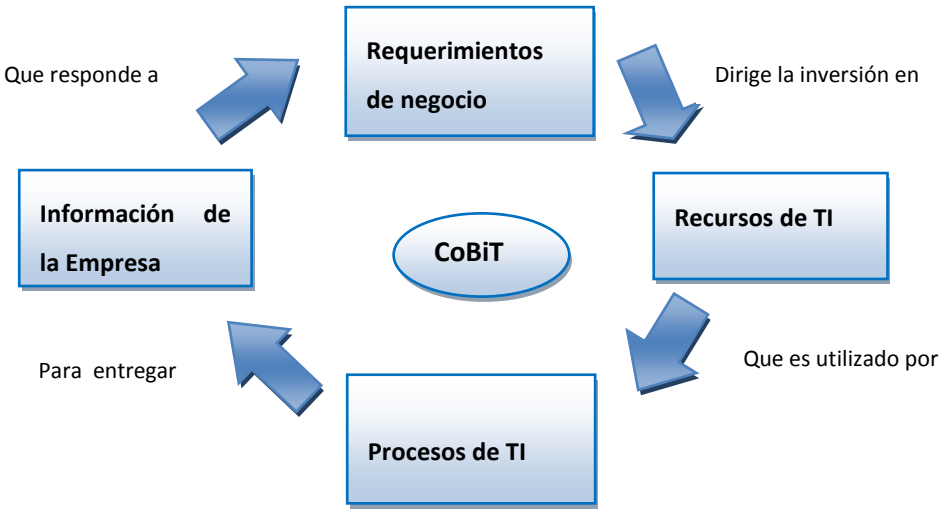


Figura 4.6. Principio básico de CoBiT. [COBIT 07]

4.1. Orientado a negocios

Tal y como se indica en **[COBIT 07]**, la orientación a negocios es uno de los pilares principales de CoBiT, por lo cual está diseñado para ser utilizado no sólo por proveedores de servicios, usuarios y auditores de TI, sino también y principalmente, como guía integral para la gerencia y para los responsables de los procesos de negocio. Con el objetivo de garantizar dicha alineación con los requerimientos del negocio CoBiT ofrece las siguientes herramientas:

4.1.1. Criterios de Información de CoBiT

Con el fin de satisfacer los objetivos de negocio, la información necesita adaptarse a determinados criterios de control, es lo que CoBiT ha llamado requerimientos de información del negocio. Con este objetivo se definen siete criterios de información, que se describen a continuación, **[COBIT 07]**:

- **Efectividad,** tiene que ver con que la información sea relevante y pertinente a los procesos del negocio y se proporcione de una manera oportuna, correcta, consistente y utilizable.

- **Eficiencia,** se refiere a que la información sea generada con el óptimo (más productivo y económico) uso de los recursos.
- **Confidencialidad,** se refiere a la protección de información sensible contra revelación no autorizada.
- **Integridad,** está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.
- **Disponibilidad,** se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas.
- **Cumplimiento,** tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales están sujetos los procesos de negocio, es decir, criterios de negocios impuestos externamente, así como políticas internas.
- **Confiabilidad,** se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno.

4.1.2. Metas de negocios y de TI

Si bien los criterios de información vistos anteriormente proporcionan un método genérico para definir los requerimientos del negocio, como se indica en [COBIT 07], la definición de un conjunto de metas genéricas de negocio y de TI ofrece una base más refinada y relacionada con el negocio para el establecimiento de requerimientos de negocio y para el desarrollo de métricas que permitan la medición con respecto a estas metas.

CoBiT ofrece en su Apéndice I una matriz de metas genéricas de negocios y metas de TI y se asocian con los criterios de la información. Estos ejemplos genéricos se pueden utilizar como guía para determinar los requerimientos, metas y métricas específicas del negocio para la empresa.

4.1.3. Recursos de TI

Estos recursos son la base sobre la cual se desarrollan los procesos que permiten cumplir las metas de TI y por ende de la organización. Dichos recursos tienen que ver con las personas y la infraestructura de tecnología de la organización. El conjunto de los procesos y la infraestructura constituyen la arquitectura empresarial para TI.

Los recursos de TI identificados en CoBiT **[COBIT 07]** son los siguientes:

- **Las aplicaciones**. Incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.
- **La información.** Son los datos en todas sus formas, de entrada, procesados y generados por los sistemas de información, en cualquier forma en que sean utilizados por el negocio.
- **La infraestructura**. Es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el entorno que los soporta) que permiten el procesamiento de las aplicaciones.
- **Las personas**. Son el personal requerido para planificar, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Estas pueden ser internas o externas (por outsourcing o contratadas), de acuerdo a como se requieran.

En la figura 4.7.se puede ver la relación existente entre las metas de TI y los recursos de TI:

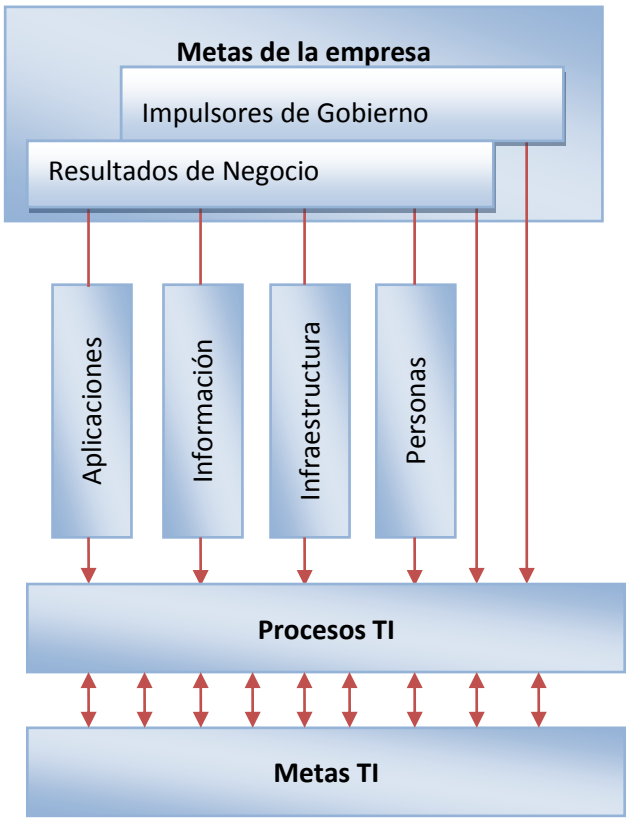


Figura 4.7. Gestión de los Recursos de TI para Alcanzar Metas de TI. [COBIT07]

4.2. Orientado a procesos

CoBiT **[COBIT 07]**, define las actividades de TI en un modelo genérico de procesos organizado en cuatro dominios, que en CoBiT 4.1 se denominan como se indica a continuación:

- **Planificar y Organizar (PO).** Proporciona dirección para la entrega de soluciones (AI) y la entrega de servicio (DS).
- **Adquirir e Implementar (AI).** Proporciona las soluciones y las implanta para convertirlas en servicios.
- **Entregar y Dar Soporte (DS).** Recibe las soluciones y las hace utilizables por los usuarios finales.

- **Monitorear y Evaluar (ME).** Monitorea todos los procesos para asegurar que se sigue la dirección prevista.

Dicho modelo de procesos es ofrecido por CoBiT como un modelo de referencia y un lenguaje común para que todos en la empresa visualicen y administren las actividades de TI. Además brinda un marco de trabajo para la medición y monitoreo del desempeño de TI.

En la figura 4.8., se pueden observar los dominios y su interrelación.

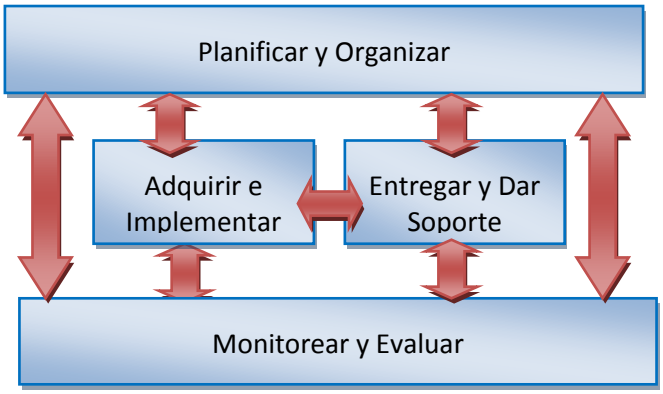


Figura 4.8. Los cuatro dominios interrelacionados de CoBiT. [COBIT 07]

Dentro de estos cuatro dominios, CoBiT ha identificado 34 procesos de TI generalmente usados. CoBiT proporciona una lista completa de procesos que puede ser utilizada para verificar que se completan las actividades y responsabilidades. Sin embargo, no es necesario que se apliquen todas, y, aun más, se pueden combinar como se necesite por cada empresa. A continuación se presenta la lista de dichos procesos para cada dominio:

- **Planificar y Organizar (PO)**
  - PO1 Definir un Plan Estratégico de TI
  - PO2 Definir la Arquitectura de la Información
  - PO3 Determinar la Dirección Tecnológica
  - PO4 Definir los Procesos, Organización y Relaciones de TI

- PO5 Administrar la Inversión en TI
- PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia
- PO7 Administrar los Recursos Humanos de TI
- PO8 Gestionar la Calidad
- PO9 Evaluar y Administrar los Riesgos de TI
- PO10 Administrar Proyectos

- **Adquirir e Implementar (AI)**
  - AI1 Identificar soluciones automatizadas
  - AI2 Adquirir y mantener software aplicativo
  - AI3 Adquirir y mantener infraestructura tecnológica
  - AI4 Facilitar la operación y el uso
  - AI5 Adquirir recursos de TI
  - AI6 Administrar cambios
  - AI7 Instalar y acreditar soluciones y cambios
- **Entregar y dar Soporte (DS)**
  - DS1 Definir y administrar los niveles de servicio
  - DS2 Administrar los servicios de terceros
  - DS3 Administrar el desempeño y la capacidad
  - DS4 Garantizar la continuidad del servicio
  - DS5 Garantizar la seguridad de los sistemas
  - DS6 Identificar y asignar costos
  - DS7 Formar y entrenar a los usuarios
  - DS8 Administrar la atención a usuarios (help desk) y los incidentes
  - DS9 Administrar la configuración
  - DS10 Administrar los problemas
  - DS11 Administrar los datos
  - DS12 Administrar el ambiente físico
  - DS13 Administrar las operaciones
- **Monitorear y Evaluar (ME)**
  - ME1 Monitorear y Evaluar el Desempeño de TI
  - ME2 Monitorear y Evaluar el Control Interno

- ME3 Garantizar el Cumplimiento Regulatorio
- ME4 Proporcionar Gobierno de TI

Es importante resaltar que para cada uno de estos 34 procesos, se tiene un enlace a las metas de negocio y TI que soporta. Además se proporciona información de cómo se pueden medir las metas, también se proporcionan cuáles son sus actividades clave y entregables principales y quién es el responsable de ellas.

4.3. Basado en controles

CoBiT **[COBIT 07]**, define el control como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar la seguridad razonable de que los objetivos de negocio se alcanzarán y los eventos no deseados serán prevenidos o detectados y corregidos.

Como hemos visto hasta ahora, CoBiT brinda un modelo genérico que representa todos los procesos que normalmente se encuentran en las funciones de TI, proporcionando un modelo de referencia general y entendible para la gerencia de operaciones de TI y para la gerencia de negocios. Dicho modelo de procesos debe tener mecanismos claros de control para lo cual CoBiT define objetivos de control para los 34 procesos, así como para el proceso general y los controles de aplicación. Cada proceso tiene un objetivo de control de alto nivel y varios objetivos de control detallados; además el marco de trabajo de CoBiT brinda vínculos claros entre los requerimientos de gobierno de TI, los procesos de TI y los controles de TI, a través de un modelo de control. La figura 4.9 que se presenta a continuación, representa gráficamente lo expuesto anteriormente.

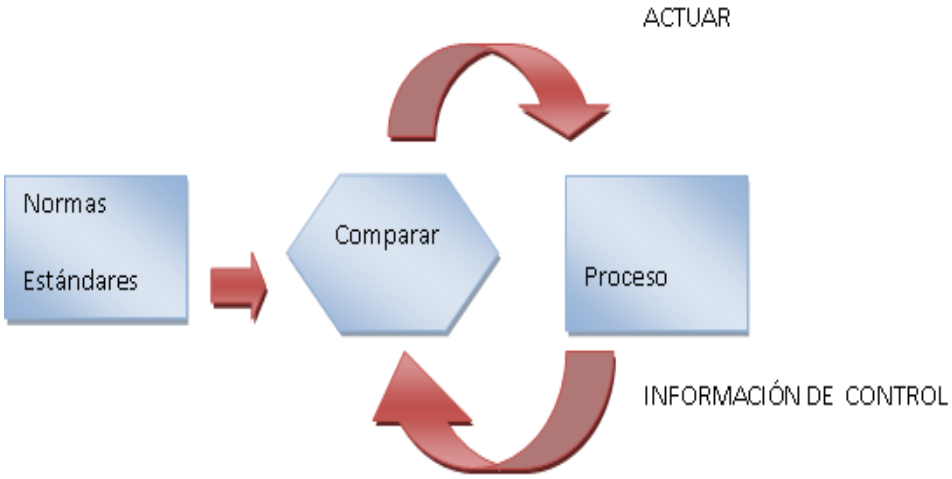


Figura 4.9. Modelo de Control. [COBIT 07]

Los objetivos de control definidos por CoBiT pueden ser consultados en su documentación oficial, **[COBIT 07]**.

4.4. Impulsado por mediciones

Dentro de cualquier tipo de organización es necesario realizar mediciones que le permitan determinar cuál es su estado actual y qué tipo de mejoras se requieren, además es necesario monitorear permanentemente su desempeño. CoBiT ofrece tres herramientas que permiten llevar a cabo estas mediciones y realizar monitoreo permanente:

- **Modelos de madurez** que facilitan la evaluación por medio de benchmarking y la identificación de las mejoras necesarias en la capacidad. El modelo de madurez para la administración y el control de los procesos de TI, propuesto por CoBiT **[COBIT 07]**, se basa en un método de evaluación de la organización, de tal forma que se pueda evaluar a sí misma desde un nivel de no-existente (0) hasta un nivel de optimizado (5). Este enfoque se deriva del modelo de madurez que el Software Engineering Institute definió para la madurez de la capacidad del desarrollo de software.

CoBiT ha desarrollado para cada uno de sus 34 procesos un modelo de madurez.

- **Metas y mediciones de desempeño para los procesos de TI**, que demuestran cómo los procesos satisfacen las necesidades del negocio y de TI, y cómo se usan para medir el desempeño de los procesos internos basados en los principios de un marcador de puntuación balanceado (balanced scorecard).

  Las métricas y las metas se definen en CoBiT a tres niveles:

  a) Las metas y métricas de TI que definen lo que el negocio espera de las TI (lo que el negocio usaría para medir a TI)
  b) Metas y métricas de procesos que definen lo que el proceso de TI debe generar para dar soporte a los objetivos de TI.
  c) Métricas de desempeño de los procesos (miden como de bien se desempeña el proceso para indicar si es probable alcanzar las metas).

- **Metas de actividades** para facilitar el desempeño efectivo de los procesos.

A manera de resumen en la figura 4.10, se puede observar el marco de trabajo de CoBiT completo.

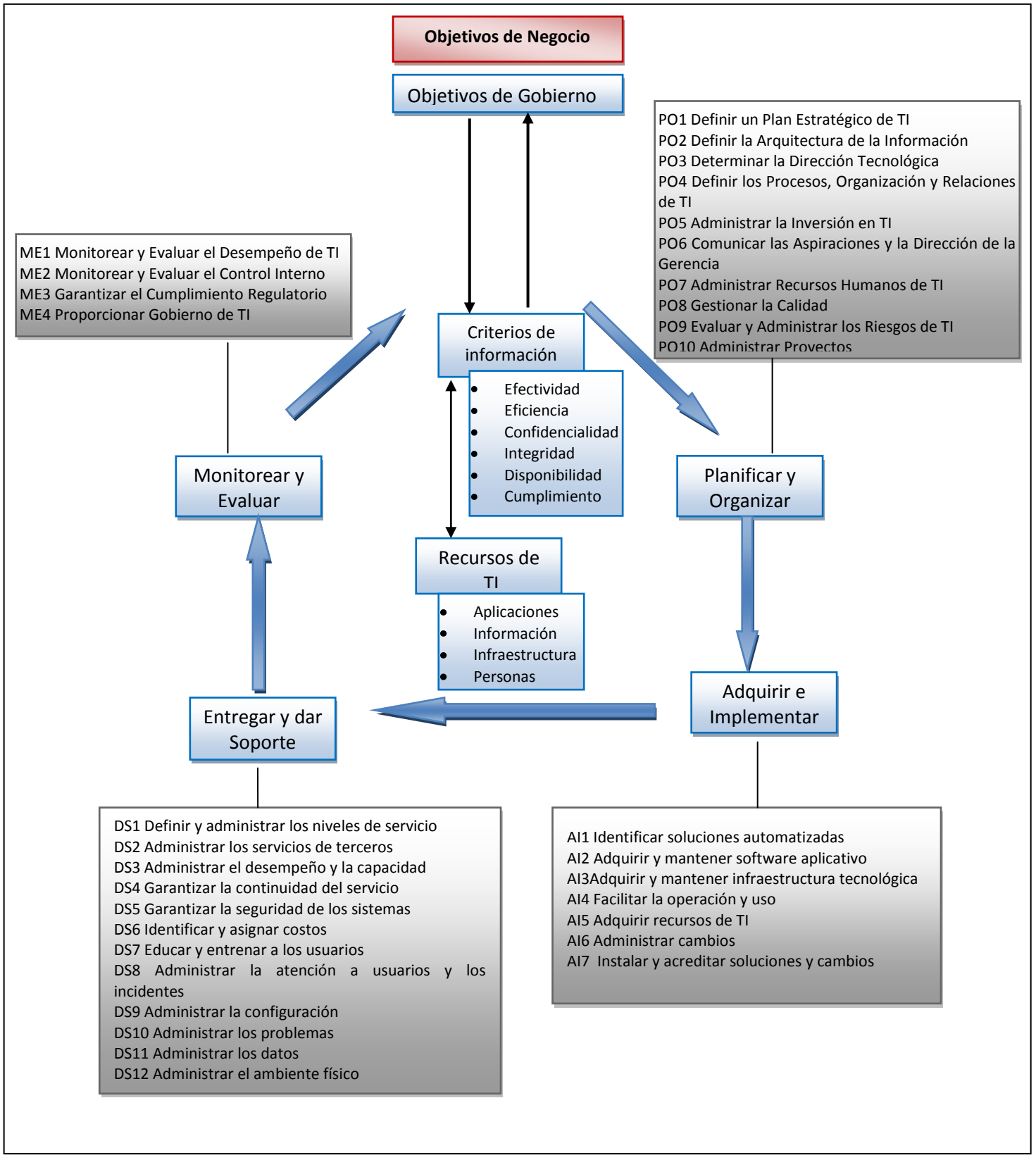


Figura 4.10. Resumen del marco. [COBIT 07]

5. GTAG -Global Technology Audit Guide[7]

Las guías GTAG - Global Technology Audit Guide-, han sido elaboradas por The Institute of Internal Auditors -IIA-. Esta serie de guías ha sido creada para proporcionar información de alto nivel sobre aspectos tecnológicos desde un punto de vista no demasiado técnico, de forma que puedan ayudar a los auditores internos (principales destinatarios de las guías) y externos a comprender mejor los diferentes riesgos, los controles y los temas del buen gobierno relacionados con aspectos tecnológicos.

Cada guía sirve como fuente de recursos para auditores e informáticos en distintos aspectos relacionados con los riesgos de las tecnologías de la información y las mejores prácticas aplicables. Las guías desarrolladas hasta el momento son, **[GTAG 09]**:

GTAG 1: Information Technology Controls

GTAG-2:Change and Patch Management Controls: Critical for Organizational Success

GTAG-3: Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment

GTAG-4: Management of IT Auditing

GTAG-5: Managing and Auditing Privacy Risks

GTAG-6: Managing and Auditing IT Vulnerabilities

GTAG-7: Information Technology Outsourcing

GTAG-8: Auditing Application Controls

GTAG-9: Identity and Access Management

GTAG-10: Business Continuity Management

GTAG-11: Developing the IT Audit Plan

GTAG-12: Auditing IT Projects

GTAG-13: Fraud Prevention and Detection in an Automated World

GTAG-14: Auditing User-developed Applications

GTAG-15: Information Security Governance

[7] Guía de Auditoría Tecnológica Global

GTAG-16: Data Analysis Technologies

A continuación se presenta una breve descripción de cada guía, a excepción de la GTAG 16 que sólo es accesible para miembros de la IIA. Dichas descripciones han sido tomadas y adoptadas de su web oficial, **[GTAG 09]**:

GTAG 1: Information Technology Controls

Esta primera guía cubre temas generales de tecnología de la información y auditoría, así como temas relacionados con la gestión, seguridad, control, aseguramiento y gestión de riesgos.

GTAG 2: Change and Patch Management Controls: Critical for Organizational Success

El objetivo de esta guía es transmitir la idea de cómo una efectiva y eficiente gestión de cambios en las TI contribuye al éxito de una organización, teniendo en cuenta que la gestión de los cambios de TI es un proceso fundamental que puede causar problemas a toda la organización y fácilmente interrumpir las operaciones, si dicha gestión no se realiza bien.

Esta guía proporciona un conocimiento práctico de los procesos y riesgos de la gestión del cambio en TI.

GTAG 3: Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment

Esta guía se centra en ayudar a los CAE (Chief Audit Executive). Tiene como misión identificar lo que se debe hacer para usar de manera efectiva la tecnología en apoyo de la "auditoría continua". Así mismo, se destacan las áreas que requieren mayor atención.

GTAG 4: Management of IT Auditing

El propósito de esta guía es ayudar a los CAE y gerentes de auditoría interna como responsables de la supervisión de las auditorías de TI, a organizar su trabajo a través de aspectos estratégicos relativos a la planificación, ejecución y

presentación de informes de las auditorías de TI, de tal forma que se pueda llevar un trabajo de forma ordenada.

GTAG 5: Managing and Auditing Privacy Risks

Esta guía abarca conceptos, principios y marcos de trabajo relacionados con la privacidad, que ayudarán a los CAE, auditores internos y directores a encontrar fuentes apropiadas para guiarse en materia de privacidad. Ofrece la visión de riesgos de privacidad que debería tener la organización, cuando se recopila, utiliza, mantiene o divulga información personal. Esta guía explica detalladamente cómo tratar la privacidad en el proceso de auditoría y también proporciona un esquema genérico para un programa de auditoría de privacidad.

GTAG 6: Managing and Auditing IT Vulnerabilities

Esta guía fue desarrollada para ayudar a los CAE y auditores internos a formular las preguntas correctas al personal de seguridad de TI al evaluar la eficacia de sus procesos de administración de vulnerabilidades. La guía recomienda prácticas específicas de gestión para ayudar a una organización a alcanzar y mantener niveles más altos de eficacia y eficiencia, e ilustra las diferencias entre un alto y un bajo desempeño en la gestión de vulnerabilidad. La guía cubre los siguientes aspectos:

a) Definición del ciclo de vida de gestión de vulnerabilidades
b) Definición del alcance de una auditoría de gestión de vulnerabilidades
c) Definición del nivel de madurez de la organización

GTAG 7: IT Outsourcing

Esta guía provee al CAE, los auditores internos y la dirección la información sobre los tipos de actividades de outsourcing de TI, el ciclo de vida de outsourcing y cómo las actividades de outsourcing deben ser administradas a través de la aplicación de planes bien definidos y que estén respaldados por un marco de trabajo de riesgos, control, cumplimiento y gobierno.

GTAG 8 - Auditing Application Controls

Esta guía proporciona orientación sobre el desarrollo y ejecución periódica de auditorías de control de aplicaciones (business application systems), para determinar si los controles a las aplicaciones están diseñados de manera adecuada y operando de manera efectiva.

GTAG 9 - Identity and Access Management – IAM

El propósito de esta guía es dar una idea de lo que significa IAM para una organización y sugerir áreas de auditoría interna para su investigación. Esta guía puede ayudar a los CAE y auditores internos a entender, analizar y supervisar sus procesos de Gestión de Identidad y Acceso. Se incluye en esta guía una lista de verificación para la revisión de la Gestión de Identidad y Acceso.

GTAG 10 - Business Continuity Management

Esta guía se centra en cómo la gestión de la continuidad del negocio (BCM) debe ser diseñada para permitir que los líderes de negocio gestionen el nivel de riesgo en que la organización podría encontrarse, en el caso de que un evento destructivo natural o provocado por el hombre, afecte a la operatividad de la organización. La guía incluye la planificación de la recuperación de desastres para la continuidad de la infraestructura de tecnología de información crítica y de los sistemas de aplicaciones de negocios.

GTAG 11: Developing the IT Audit Plan

Esta guía está orientada a apoyar a los CAE y auditores internos en el desarrollo de un plan de auditoría de TI.

La guía propone los siguientes aspectos a tener en cuenta para desarrollar el plan de auditoría de TI:

- Comprender la organización y cómo TI la soporta
- Comprender el entorno de TI y definir el universo de auditoría de TI
- Priorizar temas de auditoría a través de la evaluación de riesgos
- Desarrollar el plan de auditoría de TI

GTAG 12: Auditing IT Projects

Esta guía ofrece una visión general de las técnicas para la participación efectiva entre equipos de proyectos y la dirección en la evaluación de los riesgos relacionados con los proyectos de TI. Esta guía incluye:

- Los principales riesgos de gestión de proyectos.
- Expone cómo la actividad de auditoría interna puede participar activamente en la revisión de los proyectos, mientras mantiene la independencia.
- Presenta cinco componentes claves de los proyectos de TI, para ser considerados por los auditores internos, en la construcción de un enfoque de auditoría.
- Indica tipos de auditorías de los proyectos.
- Presenta una lista de sugerencias de preguntas para su uso en la evaluación de proyectos de TI

GTAG 13: Fraud Prevention and Detection in an Automated World

Esta guía se centra en los riesgos de TI relacionados con el fraude y en las evaluaciones de estos riesgos y en cómo el uso de la tecnología puede ayudar a los auditores internos y otros actores clave en la organización a direccionar el fraude y los riesgos asociados.

También tiene como objetivo informar y orientar a los CAE y auditores internos sobre cómo utilizar la tecnología para ayudar a prevenir, detectar y responder al fraude.

GTAG 14: Auditing User-developed Applications (UDAs)

Esta guía ofrece pautas para la realización de auditoría al desarrollo de aplicaciones, “User-developed Applications”. Esta guía proporciona:

- Direccionamiento sobre el alcance de una auditoría interna de la UDA.
- Orientación sobre cómo el rol del auditor interno como asesor se puede aprovechar para asistir a la dirección en el desarrollo de un marco efectivo para el control de UDA.
- Consideraciones que los auditores internos deben tener en cuenta cuando se realizan auditorías de UDA.
- Un ejemplo de un flujo de proceso de UDA, así como un programa de auditoría interna de UDA y soporte de hojas de trabajo para ayudar a los auditores internos a organizar y ejecutar una auditoría.

GTAG 15: Information Security Governance

Esta guía proporciona pautas para ayudar al CAE en la incorporación de una auditoría de gobierno de la seguridad de la información (ISG) en el plan de auditoría, se centra en si la actividad de ISG de la organización ofrece las conductas, prácticas y ejecución de la Seguridad de la Información correctas. Esta guía permite:

1. Definir el ISG.
2. Ayudar a los auditores internos a entender las preguntas correctas y saber que documentación es requerida.
3. Describir el rol de las actividades de auditoría interna (IAA) en el ISG.

6. El Esquema Nacional de Seguridad

El Esquema Nacional de Seguridad (ENS) es el encargado de establecer las políticas de seguridad en la utilización de medios electrónicos en las Administraciones Públicas. Está formado por un conjunto de principios básicos y de requisitos mínimos que permitan una protección adecuada de la información. (Fuente: II jornadas Asticnet)

La regulación de ENS viene determinada en el Real Decreto 3/2010, de 8 de enero y que se prevé en el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

El ENS es el resultado del trabajo conjunto de todas las Administraciones Públicas con el apoyo del Centro Criptológico Nacional, a los que hay que sumar la aportación de profesionales externos.

El objetivo fundamental del ENS es que "todos los órganos superiores de las administraciones públicas dispongan de una política de seguridad que garantice el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos."

Como objetivos fundamentales del ENS, podemos reseñar:

- Creación de las condiciones necesarias en el uso de medios electrónicos.
- Aportar un lenguaje común para la interacción entre las administraciones públicas.

En el ENS se categorizan los sistemas para que la adopción de medidas de seguridad sean proporcionales a la naturaleza de la información y de los sistemas y servicios a proteger. Para que el principio de proporcionalidad se aplique correctamente, se categorizan los sistemas en tres escalones, en función de la valoración del impacto que un incidente tendría en la seguridad de la información o de los servicios.

La auditoría de seguridad que verifica el cumplimiento del ENS se debe llevar a cabo al menos cada dos años en el caso de sistemas de categoría Media y Alta.

6.1. Guía de Auditoría

El Centro Criptológico Nacional, tiene entre sus funciones la de "elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIIC" (STIC), tal y como consta en la Guía de Seguridad CCN-STIC-802) **[STIC 10]**.

La guía CCN-STIC-802, hecha por y para las Administraciones Públicas, define un marco de referencia para poder llevar a cabo auditorías de sistemas de las tecnologías de la información y como tal, establece pautas de carácter general que puedan ser aplicadas a entidades con diferente tipología.

Esta guía de auditoría **[STIC 10]**, se encuadra dentro de lo previsto en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, y específicamente dentro del artículo 34 (Auditoría de Seguridad) y del Anexo III (Auditoría de la Seguridad) del Real Decreto 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

La guía **[STIC 10]** tiene como objetivo establecer unas premisas mínimas de ejecución de auditorías, que asegure una realización lo más homogénea posible sin que ello implique la utilización de una metodología determinada.

6.2. El objeto de la auditoría

La guía **[STIC 10]**, propone como objeto de una auditoría dar cumplimiento a lo que se establece en el artículo 34 y en el anexo III del Real Decreto 3/2010.

El resultado de la auditoría, según **[STIC 10]**, emitirá una opinión independiente y objetiva sobre el cumplimiento de las normas, que permita a los

responsables de la entidad u organismo, la toma de decisiones adecuadas para la subsanación de las deficiencias identificadas y para alcanzar el nivel de seguridad adecuado.

Por tanto, el objetivo final de la auditoría, será certificar la seguridad del sistema que haya sido objeto de la misma y poder asegurar la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de los servicios prestados y de la información tratada.

6.3. Desarrollo y ejecución de la auditoría

La guía [STIC 10], presenta un esquema tradicional para la realización de una auditoría:

- Alcance y objetivo de la auditoría
- Composición del equipo auditor
- Planificación preliminar de la auditoría
- Programa de auditoría
- Revisiones y pruebas de auditoría
- Elaboración y presentación de resultados y pruebas de auditoría
- Presentación del informe de auditoría

6.3.1. Alcance y objetivo de la auditoría

La guía [STIC 10], presenta de manera esquematizada los puntos que se deben recoger en este primer paso de ejecución de una auditoría:

- El alcance y el objetivo de la auditoría debe estar claramente definido, documentado y consensuado entre el equipo auditor y el órgano (Administración Pública, entidad de derecho público,…) que haya solicitado la auditoría.
- Se deberá establecer claramente el límite hasta donde se audita.
- Dado que las medidas de seguridad objeto de la auditoría, pueden abarcar medidas de diversa naturaleza (física, lógica, organizativa,…),

será necesario identificar los elementos que forman parte del alcance de la auditoría (ej. Políticas de seguridad, tipo de datos que se manejan, personal afectado por la auditoría, conexiones externas con otros organismos públicos y/o privados, legislación que afecta al sistema de información objeto de la auditoría,…)

- Por último, la guía **[STIC 10]** deja claro que no debe ser objeto de auditoría la ejecución de cualquier acción que pueda ser considerada como responsabilidad de consultoría o similar, para poder garantizar la independencia y objetividad del auditor.

6.3.2. Composición del equipo auditor

En este segundo punto, la guía **[STIC 10]** relaciona como debe ser la composición del equipo auditor y qué requisitos son los que debe cumplir:

- El equipo auditor deberá estar compuesto por un conjunto de profesionales, que disponga de los conocimientos suficientes para asegurar la correcta ejecución de la auditoría.
- El equipo puede estar compuesto sólo por auditores internos, sólo por auditores externos o bien puede ser un equipo de trabajo mixto. En cualquier caso, será necesario cumplir los siguientes requisitos:
  - Si es un equipo de auditores internos, deberá ser totalmente independiente de la organización, sistemas o servicios que sean objeto de la auditoría **[STIC 10]**.
  - Si en el equipo participan auditores externos e internos, debe quedar claro el equipo que es responsable de la auditoría así como establecer con claridad las responsabilidades y funciones de cada uno de los integrantes del equipo auditor.
  - Se deberá determinar con claridad, la propiedad de la documentación de trabajo y de las evidencias de auditoría, independientemente de la composición del equipo. Así mismo, debe establecerse de manera inequívoca la responsabilidad del informe de auditoría.

  - En el caso en que la auditoría se lleve a cabo por un equipo de auditores externos o bien por auditores internos en los que se haya incorporado a expertos externos, se deberán firmar las cláusulas de confidencialidad necesarias.
- Con relación a la responsabilidad del equipo auditor, sus pruebas y revisiones no deben limitarse a la revisión de documentos, sino a la obtención de evidencias eficaces que sustenten el informe final.

6.3.3. Planificación preliminar de la auditoría

La guía **[STIC 10]**, en la planificación preliminar de la auditoría relaciona las tareas habituales descritas en los modelos clásicos de ejecución de una auditoría, que consiste básicamente en el establecimiento de los requisitos de información y documentación necesarios para desarrollar el programa de auditoría, definir las pruebas a auditar, las entrevistas y revisiones.

La aportación que hace la guía **[STIC 10]**, con relación a otros marcos de referencia y/o metodologías tradicionales es el hecho de especificar cuál debe ser la documentación mínima necesaria para concretar la planificación de la auditoría del cumplimiento del Real Decreto 3/2010:

- Documentos firmados por el órgano superior correspondiente, que muestren el conocimiento y la aprobación formal de las decisiones en materia de política de seguridad.
- Organigrama de las áreas afectadas.
- Identificación de los responsables.
- Descripción detallada del sistema a auditar.
- Identificación de la categoría del sistema según el Anexo I del RD 3/2010.
- Política de seguridad, de firma electrónica, normativa de seguridad.
- Descripción detallada del sistema de gestión de la seguridad.
- Informe de Análisis de Riesgos.
- Decisiones adoptadas para gestionar los riesgos.

6.3.4. Programa de auditoría

Dado que la guía **[STIC 10]**, como dijimos al comienzo de este apartado, funciona como marco de referencia, en este paso de ejecución de auditoría se señala en primer lugar que en cada contexto de auditoría se deberán diseñar las revisiones y pruebas de validación, definiendo en qué consistirán cada una de ellas y estableciendo los recursos necesarios para llevarlas a cabo **[STIC 10]**.

6.3.5. Elaboración y presentación de resultados y pruebas de auditoría

Para la guía **[STIC 10]**, el objetivo principal en este momento de la auditoría es la presentación de los resultados de las revisiones y pruebas, con carácter previo a la emisión y presentación del informe de auditoría, y que servirá para reforzar la eficacia del mismo, ya que, al confirmar la veracidad de los resultados de las pruebas y sin existir ninguna otra consideración no tenida en cuenta, se puede cambiar la evaluación del cumplimiento de un requisito de seguridad.

La especificidad que presenta esta guía, con relación a otros posibles marcos de referencia y/o metodologías de auditoría, se refiere al estricto cumplimiento de lo establecido en el RD 3/2010 y en el Título VIII del RD 1720/2007, ya que en el caso de observarse alguna deficiencia que pueda implicar riesgos en la protección de la información, debe ser señalado.

6.3.6. Presentación del informe de auditoría

Concluidas las anteriores etapas, la presentación del informe de auditoría, según la guía de seguridad **[STIC 10]**, deberá incluir una opinión sobre: la política de seguridad, los procedimientos de resolución de conflictos, si existe un sistema de gestión de la seguridad de la información regulado y documentado, si se ha realizado análisis de riesgos y si existe un sistema de gestión de mejora continua.

En comparación con otras metodologías y/o marcos de referencia la guía de seguridad **[STIC 10]** presenta como diferencia, el obligado cumplimiento en cada una de las etapas de la auditoría de lo especificado en la normativa (Real Decreto 3/2010 y la Ley 11/2007).

6.4. Anexos

Por último, la guía **[STIC 10]**, presenta un conjunto de anexos –que relacionamos a continuación - que definen diferentes requisitos, modelos y glosario de términos.

Anexo A. Requisitos para el equipo auditor

Anexo B. Incorporación de expertos al equipo de auditoría

Anexo C. Concurrencia con el título VIII del RD 1720/2007

Anexo D. Modelo de acuerdo de confidencialidad

Anexo E. Glosario de términos.

Anexo F. Bibliografía de referencia

7. Normas de Auditoría de Sistemas de Información de ISACA

Information Systems Audit and Control Association (ISACA) es una asociación reconocida mundialmente, dedicada al desarrollo de los conocimientos relacionados con la seguridad y auditoría de los sistemas de información, el gobierno TI de la empresa, los riesgos relacionados con las TI y el cumplimiento. Fundada en 1969, ISACA desarrolla estándares internacionales de auditoría y normas de control.

ISACA aprobó las Normas de Auditoría de Sistemas de Información **[ISAC 07]**, de aplicación obligatoria para los auditores de sistemas de información con la certificación CISA (Certified Information Systems Auditor) que gestiona y concede la propia asociación ISACA.

Los objetivos de estas normas **[ISAC 07]**, son los de informar a los auditores del nivel mínimo de rendimiento aceptable para satisfacer las responsabilidades profesionales establecidas en el Código de Ética Profesional y de informar a la gerencia y a otras partes interesadas de las expectativas de la profesión con respecto al trabajo de aquellos que la ejercen.

En la actualidad existen 16 normas publicadas **[ISAC 07]**, las cuales citamos a continuación:

- S1 Estatuto de Auditoría
- S2 Independencia
- S3 Ética y normas profesionales
- S4 Competencia profesional
- S5 Planeación
- S6 Realización de labores de auditoría
- S7 Reporte
- S8 Actividades de seguimiento
- S9 Irregularidades y acciones ilegales
- S10 Gobernabilidad de TI
- S11 Uso de la evaluación de riesgos en la planeación de auditoría
- S12 Materialidad de la auditoría
- S13 Uso del trabajo de otros expertos
- S14 Evidencia de auditoría
- S15 Controles de TI
- S16 Comercio electrónico

Cada una de estas normas puede ser consultada y descargada del sitio web de ISACA, **[ISAC 07].**

8. ITIL: Information Technology Infrastructure Library[8]

ITIL fue desarrollada a finales de los 80 como una guía para el gobierno británico y se ha acabado convirtiendo en un estándar mundial para la Gestión de Servicios Informáticos. Su estructura ha demostrado ser útil para todas las organizaciones y para todos los sectores mediante su adopción por innumerables compañías como base para la consulta, formación y soporte de herramientas de software.

ITIL es una guía de las mejores prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información. ITIL está formado por un conjunto de procedimientos que permiten a las organizaciones conseguir la calidad y la

[8] Biblioteca de infraestructura de Tecnologías de la Información

eficiencia en las operaciones de TI. Todos los procedimientos son independientes del proveedor y abarcan toda la infraestructura, el desarrollo y las operaciones de TI.

8.1. ITIL v 3.0

Cuando fue creada en los 80's, ITIL constaba de 10 libros centrales que cubrían las dos principales áreas de Soporte del Servicio y de Prestación del Servicio; libros que fueron más tarde soportados por 30 libros complementarios. Desde el año 2000, se ha ido acometiendo una revisión de la biblioteca, intentando conseguir un acceso más simple a la información. En la actualidad ITIL se encuentra en su versión 3.0 y está formada por cinco libros [http://www.itil-officialsite.com/], que relacionamos a continuación:

Libro 1. "Estrategia del Servicio": Trata sobre el alineamiento del negocio y la TI para que cada uno de ellos obtenga lo mejor del otro. Abunda en las claves de las estrategias de gestión de los servicios y la planificación del valor, es decir, en la relación de la estrategia del servicio informático con las necesidades de la organización y en la planificación e implementación de la estrategia del servicio.

Libro 2. "Diseño del Servicio": Este libro se centra en la generación y mantenimiento de las políticas informáticas así como en la creación de la arquitectura y documentación necesaria para el diseño de los procesos y que las soluciones de servicios de infraestructuras sea acertados e innovadores.

Libro 3. "Transición al Servicio": En este libro se presentan recomendaciones y actividades de proceso para la transición de los servicios en el entorno empresarial. Considera la gestión del cambio así como los riesgos, beneficios, mecanismos de entrega y el apoyo de los servicios operacionales continuos.

Libro 4. "Operaciones de Servicio": El libro presenta con detalle cómo llevar a cabo el control de las actividades necesarias para lograr la excelencia en las operaciones del día a día.

Libro 5. "Mejora continua del servicio": Este libro se presenta como una guía para introducir elementos de mejora en la gestión de los servicios TI, incluyendo las cuestiones relacionadas con la retirada de los servicios.

Todos los libros mantienen la misma estructura diferenciando Objetivos, Conceptos clave, Procedimientos, Modelos y Salidas y Documentación.

Cada uno de estos libros representa una de las fases del ciclo de vida del servicio de TI, que son un reflejo de un ciclo Deming (PDCA). Por tanto, no son independientes y aislados del resto sino que se establecen múltiples interrelaciones entre ellos que afectan al ciclo de vida del servicio.

Figura 4.11. Ciclo Deming – Ciclo de vida de servicio según ITIL

CAPÍTULO V: Metodologías y/o estándares para el análisis y la gestión de riesgos

1. Introducción

Existen en la actualidad un número importante de metodologías y estándares o normas que tratan el análisis y la gestión de riesgos, tanto en el ámbito local como Internacional. Dichas metodologías y estándares, se ofrecen a las diferentes organizaciones como guías para llevar a cabo un adecuado análisis y gestión de riesgos bajo un proceso estandarizado y normalizado, lo cual ayuda a mejorar el desarrollo del proceso y por ende los resultados esperados.

Encontramos estándares y/o metodologías orientadas a la gestión de riesgos de carácter general, es decir que son aplicables a cualquier área o sector como es el caso del estándar AS/NZS ISO 31000:2009 y otras que son aplicables a sectores específicos, siendo nuestro objetivo aquellas que tienen que ver en concreto con las tecnologías de la información (sistemas de información, sistemas informáticos).

La selección de las normas y metodologías a estudiar se ha realizado con base en la relevancia, ámbito de aplicación y ámbito geográfico de la norma, prestando interés particular en las normas de ámbito local dado el objetivo de aplicación del presente trabajo.

Al final del capítulo se presenta un listado que recopila diversos estándares y metodologías para información del lector.

Para iniciar nuestro estudio de dichos estándares y metodologías hemos seleccionado el estándar de carácter general AS/NZS ISO 31000:2009, que es un estándar internacional de referencia y que aporta elementos generales importantes para la gestión de riesgos. Continuaremos con estándares y metodologías propias del ámbito del presente trabajo.

La descripción de cada metodología y/o estándar se ha tomado de los documentos oficiales de cada una de ellas, y de sus respectivas webs donde ofrecen información de carácter general.

2. La norma AS/NZS ISO 31000:2009

La norma AS/NZS ISO 31000:2009, **[AS/NZS 09]** surge como remplazo a la norma AS/NZS 4360:2004, estándar australiano para la gestión de riesgos

ampliamente conocido y utilizado a nivel mundial. Ha sido elaborada con participación conjunta entre la Organización Internacional para la Estandarización - ISO y el Comité de Normas de Australia / Nueva Zelanda.

Este estándar, suministra orientaciones genéricas para la gestión de riesgos, pudiéndose aplicar a una gran variedad de actividades, decisiones u operaciones de cualquier entidad pública o privada.

Dentro de las novedades en esta versión se ha incorporado conceptos adicionales al estándar Australiano Neozelandés AS/NZS 4360:2004 y entre sus principios más importantes se encuentran los siguientes, **[AS/NZS 09]**:

- Define el riesgo como un efecto de incertidumbre en el logro de los objetivos
- Los principios que recomienda seguir por las organizaciones son más explícitos que su antecesor AS/NZS 4360:2004.
- Aconseja integrar en forma explícita el mejoramiento continuo de la estructura de administración de riesgo.

Incorpora un anexo informativo donde describe los atributos que deberían considerar las organizaciones para apuntar al nivel más alto de desempeño en la gestión de riesgos, en relación con la criticidad de las decisiones a tomar, e indica algunos indicadores tangibles para cada atributo.

La norma está formada por 5 cláusulas y un anexo. A continuación citamos los aspectos principales de cada cláusula, que han sido tomados directamente de la norma, [AS/NZS 09]:

Cláusula 1: Alcance

El estándar tiene como objetivo ayudar a las organizaciones de todo tipo y tamaño a gestionar sus riesgos con efectividad. Proporciona los principios, el marco y un proceso destinado a gestionar cualquier tipo de riesgo en una manera transparente, sistemática y creíble dentro de cualquier alcance o contexto.

Cláusula 2: Términos y definiciones

Esta cláusula presenta una serie de términos y definiciones que se usan a lo largo del desarrollo del documento del estándar y del proceso de gestión de riesgos.

Cláusula 3: Principios

Para el estándar la gestión de riesgos se basa en los siguientes principios

- Crea valor en la organización y lo preserva.
- Está integrada en los procesos de la organización.
- Forma parte de la toma de decisiones.
- Trata explícitamente la incertidumbre.
- Es sistemática, estructurada y oportuna.
- Está basada en la mejor información disponible.
- Está hecha a medida.
- Tiene en cuenta factores humanos y culturales.
- Es transparente e inclusiva.
- Es dinámica, iterativa y sensible al cambio.
- Facilita la mejora continua de la organización.

Cláusula 4: Estructura

En esta cláusula se describe un marco o estructura general para la gestión de los riesgos en forma de ciclo PDCA (Plan–Do–Check–Act) de mejora continua que no pretende ser en sí mismo un sistema de gestión certificable, sino más bien ayudar a la organización a integrar la gestión. Es importante aclarar que esta no es una norma certificable, como otras de la familia ISO.

En la siguiente figura se resume de forma gráfica, el contenido de esta cláusula.

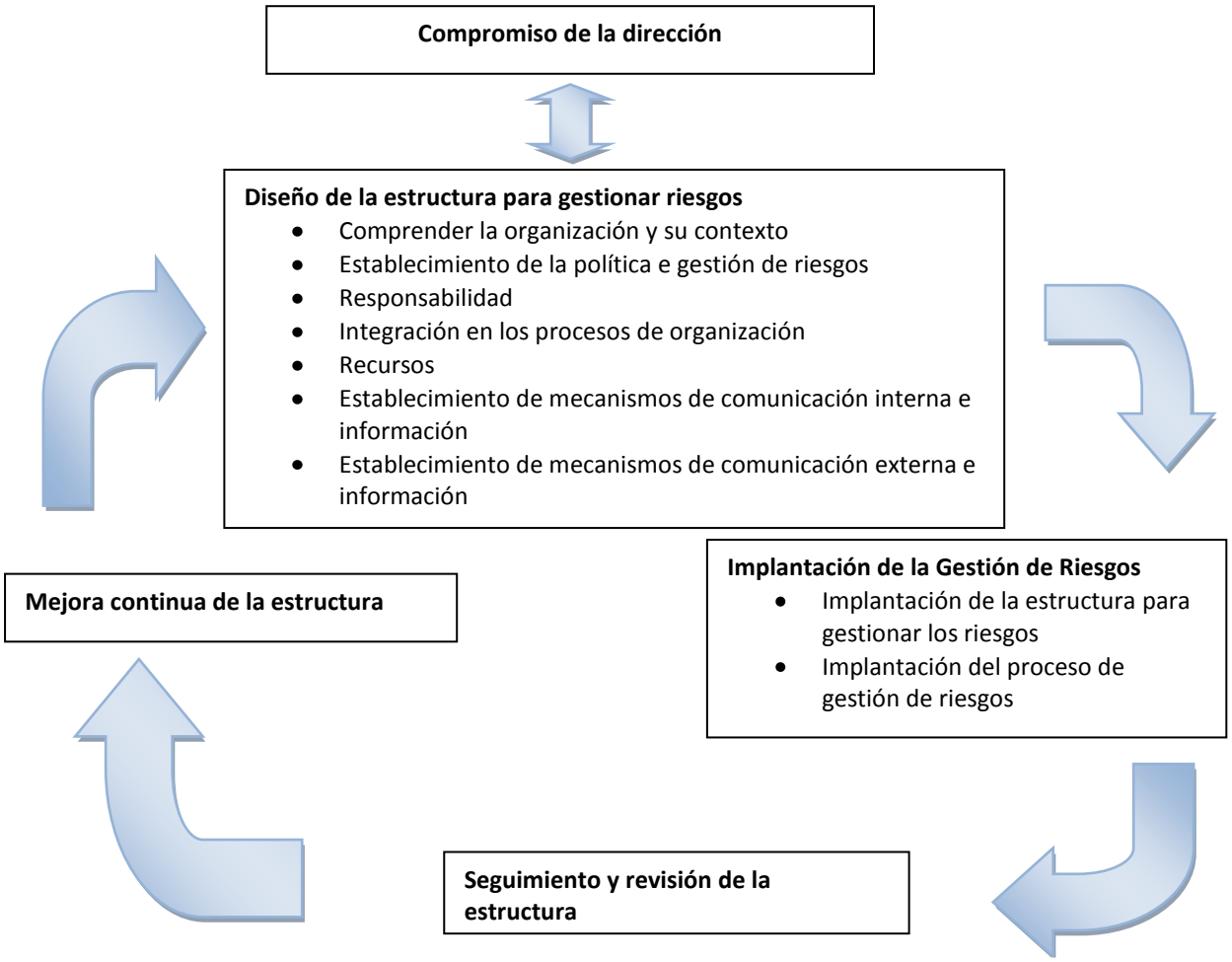


Figura 5.1. Marco general para la gestión de riesgos. [AS/NZS 09]

Cláusula 5: Procesos

A través de esta cláusula se define un proceso para la gestión de los riesgos que debería formar parte de la gestión, integrarse en su cultura y prácticas, y adaptarse a los distintos procesos operativos de la organización. Estos procesos se han conservado con respecto a la norma AS/NZS 4360:2004. El estándar establece cinco actividades básicas que se interrelacionan para llevar a cabo el proceso de gestión de riesgos y que se ilustran en las figuras 5.2 y 5.3.

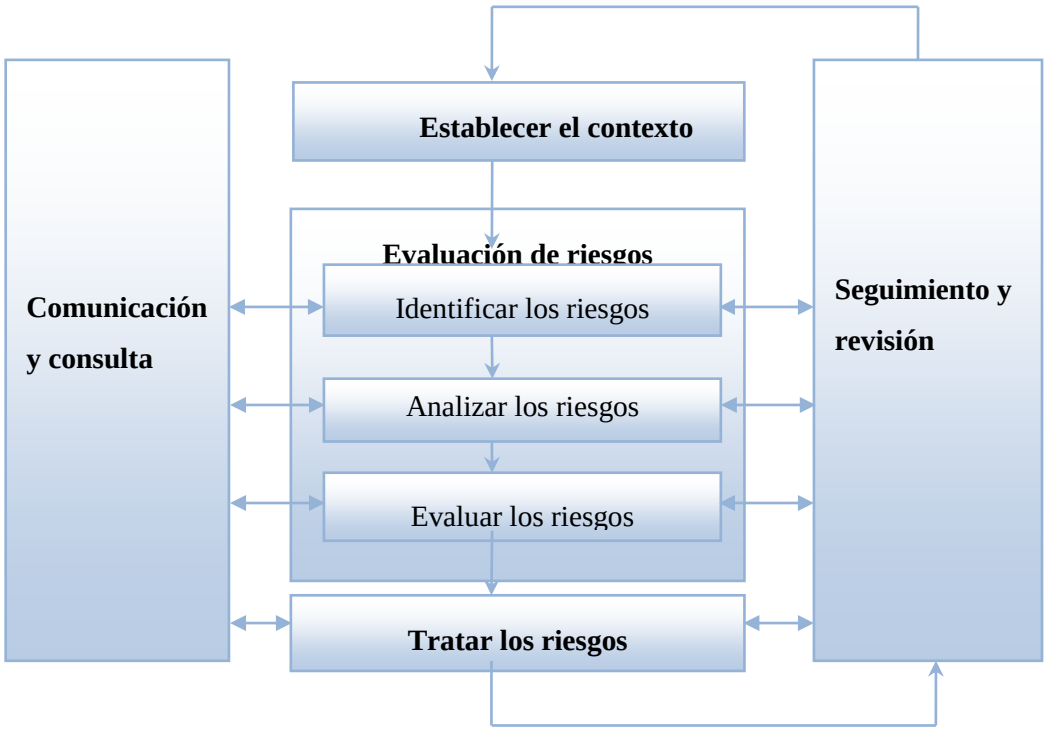


Figura 5.2. Proceso para la gestión de riesgos. [AS/NZS 09]

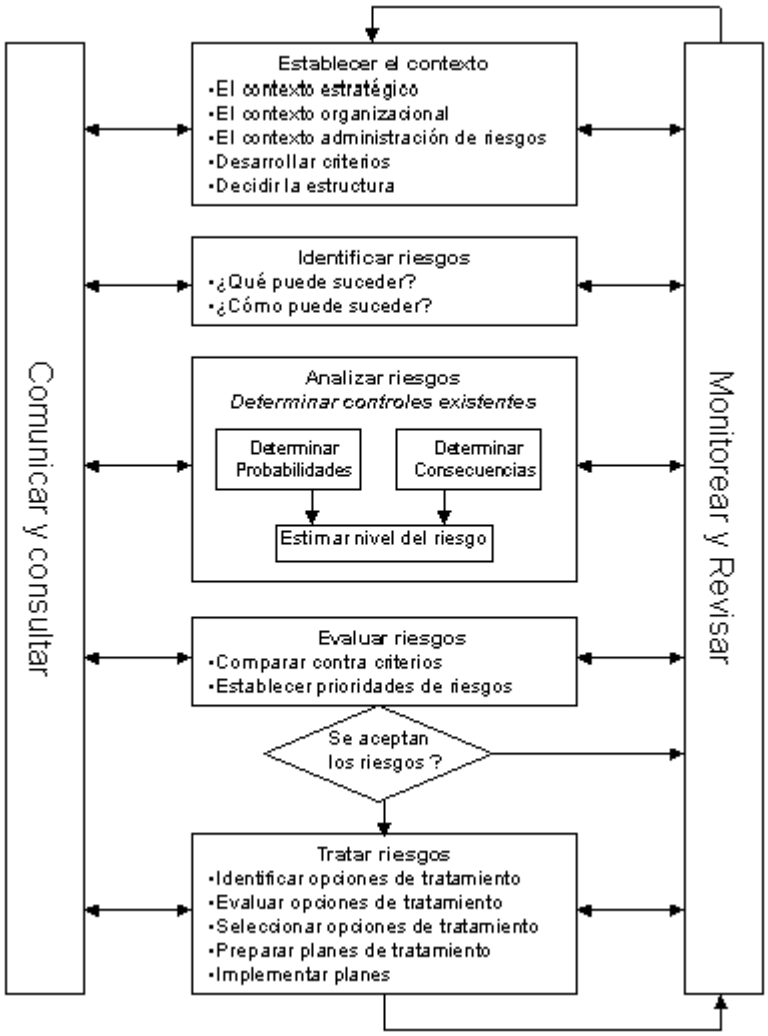


Figura 5.3. Proceso detallado para la gestión de riesgos. [AS/NZS 09]

Finalmente en la figura 5.4 podemos ver la interrelación de las cláusulas 3 a 5, que son a través de las que se fundamenta y desarrolla el proceso de gestión de riesgos:

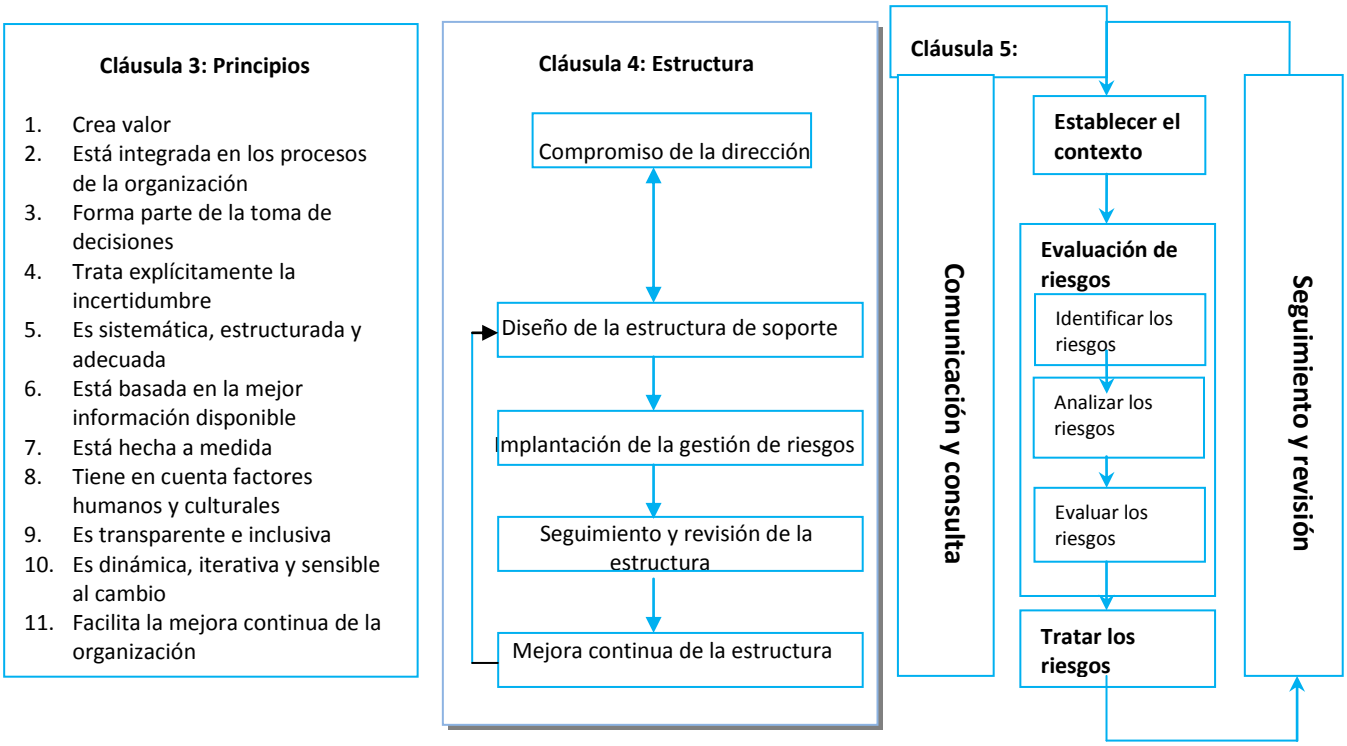


Figura 5.4. Interrelación cláusulas 3 a 5. [AS/NZS 09]

Anexo A: Atributos para mejorar la gestión de riesgos

Donde se describen los atributos que deberían considerar las organizaciones para apuntar al nivel más alto de desempeño en la gestión de riesgos, en relación con la criticidad de las decisiones a tomar, e indica algunos indicadores tangibles para cada atributo.

3. Norma UNE 71504:2008.- Metodología de análisis y gestión de riesgos para los sistemas de información

Esta norma ha sido desarrollada por el comité técnico AEN/CTN 71 Tecnología de la información, de AENOR - Asociación Española de Normalización y Certificación, **[AENO 08]**. Tal y como se indica en la norma su campo de aplicación está dirigido a los sistemas de tratamiento de la información, a los procesos de negocio que soportan, como son: toda la información que fluye en el proceso, el

marco legislativo, el equipo humano, las aplicaciones informáticas, el equipamiento informático, las redes de comunicaciones, las instalaciones y otro equipo auxiliar.

La norma establece los requisitos que debe cumplir el método para:

- Analizar los riesgos a que están expuestos los sistemas de información.
- Analizar las salvaguardas desplegadas para su protección
- Estimar el riesgo residual y
- Gestionar dichos riesgos

Conforme a lo expuesto en esta norma, para una adecuada gestión de los riesgos es necesario:

- Un método de análisis cualitativo o cuantitativo que permita identificar y calibrar los riesgos a los que está expuesta la organización.
- Un procedimiento de evaluación de los riesgos: que permita traducir los riesgos técnicos en términos de negocio o servicio.
- Un procedimiento de tratamiento: que permita interpretar las decisiones de negocio en términos técnicos y materializarlas de forma que el sistema de información se alinee efectivamente con las decisiones de la dirección.

Para desarrollar lo expuesto anteriormente la metodología UNE 71504:2008 para el análisis y la gestión de riesgos, propone una serie de actividades agrupadas en Método de Análisis, Evaluación de Riesgos, Tratamiento de los Riesgos y Administración de la Gestión de Riesgos.

- El método de análisis de riesgos a los que está expuesto un sistema se lleva a cabo mediante la ejecución de una serie de actividades que pretende establecer el contexto o marco en el que se gestiona el riesgo, la caracterización de los activos del sistema de información, de las amenazas, la determinación del riesgo potencial y la caracterización de las salvaguardas.

- La evaluación de los riesgos
- El tratamiento que se dará a los riesgos, para aquellos riesgos cuya evaluación determine que no son aceptables por la organización se aplicará un tratamiento adecuado, para aquellos riesgos que se acepten, se dispondrá de un sistema de monitorización que garantice que permanecen en el nivel estimado

  Para aplicar el tratamiento elegido se elaborara un plan de acción o plan de seguridad, el cual deberá ser aprobado por la dirección
- La administración de la gestión de riesgos. El análisis y tratamiento de los riesgos debe ser una actividad recurrente, para lo cual el proceso de gestión debe estar definido, ser válido, estar cuantificado, estar previsto su plan de revisión y actualización regular y además deberá ser auditado y estar coordinado con el proceso de gestión de cambios.

Esta norma cuenta con una serie de anexos que apoyan el proceso de análisis y gestión de riesgos, que se citan a continuación:

Anexo A: Términos en inglés

Anexo B: Evaluación de riesgos

Anexo C: Organización interna

Anexo D: Requisitos necesarios para el éxito

Anexo E: Malas prácticas

Anexo F: Modelo de Madurez

4. MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

La metodología MAGERIT **[MAGE 06]**, ha sido desarrollada por el Consejo Superior de Administración Electrónica, y publicada por el entonces Ministerio de Administraciones Públicas de España, hoy en día Ministerio de Hacienda y Administraciones Públicas

La primera versión se publicó en 1997. En 2006 se publica la versión 2.0 (que ha sido la utilizada para el desarrollo de este trabajo, ya que era la que

estaba vigente en el momento de iniciar el proyecto y en el transcurso del desarrollo del mismo). Recientemente, octubre 2012, se ha publicado la versión 3.0, que según se comenta en **[CALI 12]**, introduce los siguientes cambios respecto a la versión anterior:

- Mejor alineamiento con la normativa ISO, buscando una integración de las tareas de análisis de riesgos dentro de un marco organizacional de gestión de riesgos dirigido desde los órganos de gobierno.
- Aligerar el texto.
- Eliminar partes poco importantes o poco usadas.
- Normalizar las siguientes actividades:
  - MAR - Método de Análisis de Riesgos.
  - PAR – Proyecto de Análisis de Riesgos.
  - PS – Plan de seguridad.

Se trata de una metodología abierta, de uso muy extendido en el ámbito español, y de uso generalizado en 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.

4.1. Finalidad de MAGERIT

Según lo expuesto por el equipo de desarrollo de MAGERIT en **[MAGE 06]**, el análisis y gestión de los riesgos es un aspecto clave del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica que tiene la finalidad de poder dar satisfacción al principio de proporcionalidad en el cumplimiento de los principios básicos y requisitos mínimos para la protección adecuada de la información.

MAGERIT es un instrumento para facilitar la implantación y aplicación del Esquema Nacional de Seguridad proporcionando los principios básicos y requisitos mínimos para la protección adecuada de la información.

4.2. Objetivos de MAGERIT

Como se indica en **[MAGE 06]**, MAGERIT persigue los siguientes objetivos:

- Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

MAGERIT **[MAGE 06]**, permite:

- Estudiar los riesgos que soporta un sistema de información y el entorno asociado a él. MAGERIT propone la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la organización. Señala los riesgos existentes, identificando las amenazas que acechan al sistema de información y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados.
- Los resultados del análisis de riesgos permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

4.3. Organización de las guías de MAGERIT

De acuerdo a lo que se indica en la web oficial de MAGERIT **[MAGE 06]**, el desarrollo de la metodología se ha estructurado en tres guías: Método, Catálogo de Elementos y Guía de Técnicas.

- El Método**,** describe los pasos y las tareas básicas para realizar un proyecto de análisis y gestión de riesgos, y proporciona una serie de

aspectos prácticos. Es la guía principal donde se explica detallada la metodología

- El Catálogo de Elementos, ofrece unas pautas y elementos estándar en cuanto a: tipos de activos, dimensiones de valoración de los activos, criterios de valoración de los activos, amenazas típicas sobre los sistemas de información y salvaguardas a considerar para proteger sistemas de información.
- La Guía de Técnicas, es una guía de consulta que proporciona algunas técnicas que se emplean habitualmente para llevar a cabo proyectos de análisis y gestión de riesgos: técnicas específicas para el análisis de riesgos, análisis mediante tablas, análisis algorítmicos, árboles de ataque, técnicas generales, análisis coste-beneficio, diagramas de flujo de datos, diagramas de procesos, técnicas gráficas, planificación de proyectos, sesiones de trabajo (entrevistas, reuniones y presentaciones) y valoración Delphi.

Magerit además propone un conjunto de informes en los cuales se recogen los principales hallazgos y conclusiones en un proyecto de análisis y gestión de riesgos, los cuales se describen a continuación.

- Modelo de valor: Caracterización del valor que representan los activos para la Organización así como de las dependencias entre los diferentes activos.
- Mapa de riesgos: Relación de las amenazas a que están expuestos los activos.
- Evaluación de salvaguardas: Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan.
- Estado de riesgo: Caracterización de los activos por su riesgo residual; es decir, por lo que puede pasar tomando en consideración las salvaguardas desplegadas.
- Informe de insuficiencias: Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir los riesgos sobre el sistema.

- Plan de seguridad: Conjunto de programas de seguridad que permiten materializar las decisiones de gestión de riesgos

4.4. Productos y servicios complementarios

PILAR **[MAGE 06]**, es una herramienta que implementa la metodología MAGERIT de análisis y gestión de riesgos, desarrollada por el Centro Criptológico Nacional (CCN) y de amplia utilización en la administración pública española.

4.5. El análisis y la gestión de riesgos en MAGERIT

De acuerdo con lo propuesto en la metodología **[MAGE 06]**, las dos grandes tareas a realizar son: el análisis de riesgos y la gestión de riesgos. Vamos a hacer una breve descripción sobre la forma en que lo trata la metodología MAGERIT.

El análisis de riesgos permite determinar qué tiene la Organización y hacer una estimación sobre lo que puede pasar, dicho de otra manera, es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados.

Los elementos con los que trabaja el análisis de riesgo son:

- **Activos,** que son los elementos del sistema de información (o estrechamente relacionados con este) que aportan valor a la Organización.
- **Amenazas,** que son aquellas actuaciones o eventos que les pueden pasar a los activos causando un perjuicio a la Organización.
- **Salvaguardas (o contramedidas),** que no son sino elementos de defensa desplegados para que aquellas amenazas causen el menor daño posible.

Con estos elementos se puede estimar el impacto, es decir, lo que podría pasar y el riesgo, lo que probablemente pase.

La gestión de riesgos, permite organizar la defensa de manera concienzuda y prudente, posibilitando defensas para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones. Como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la Dirección asume.

Informalmente, se puede decir que la gestión de la seguridad de un sistema de información es la gestión de sus riesgos y que el análisis permite racionalizar dicha gestión.

A manera de resumen y antes de entrar a detallar la metodología, presentamos los elementos principales del proceso de análisis y gestión de riesgos, propuestos por la metodología, a través del siguiente gráfico.

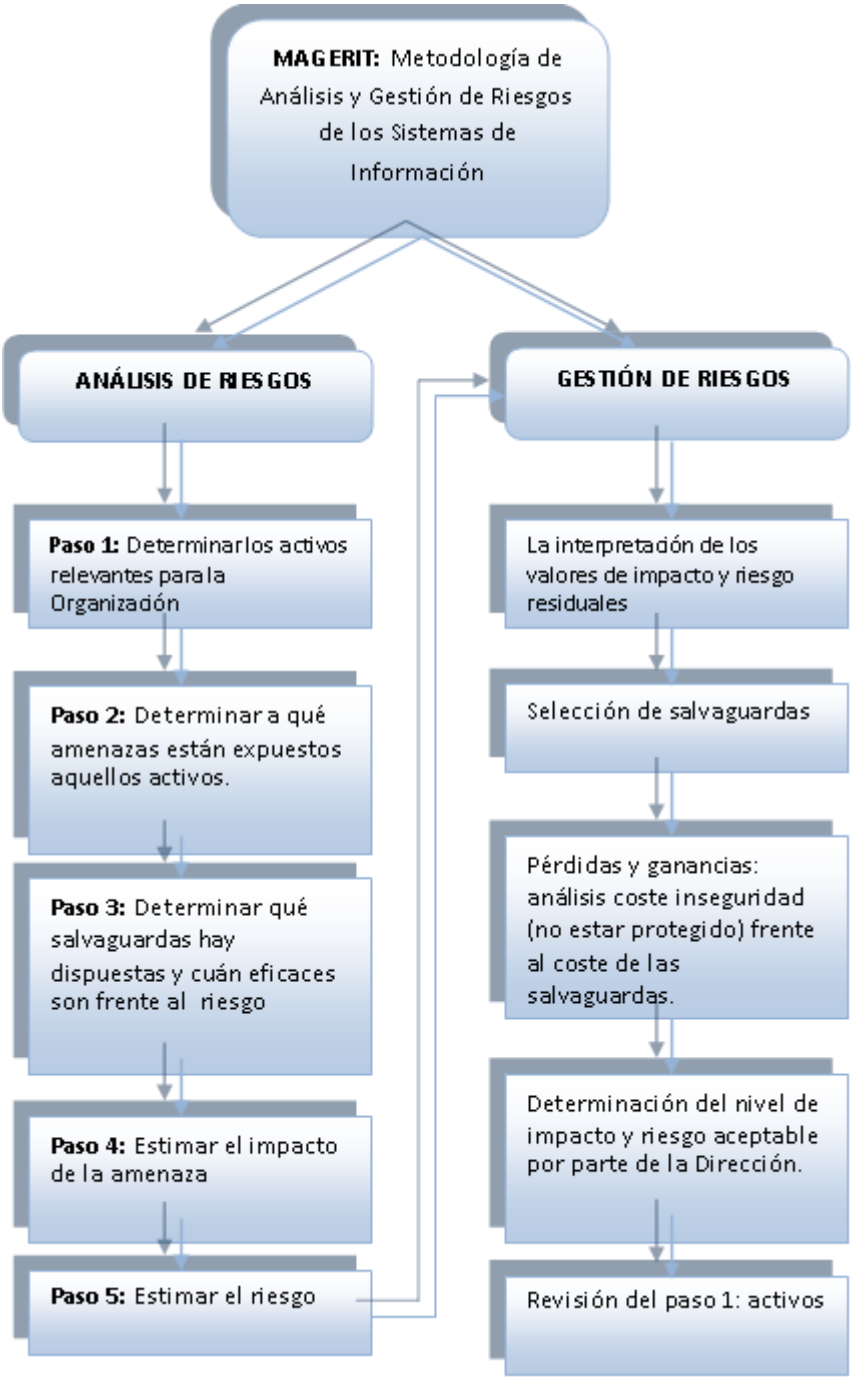


Figura 5.5. Resumen elementos del proceso de análisis y gestión de riesgos en Magerit

4.5.1. El Análisis de Riesgos según Magerit

Tal y como hemos definido en el apartado anterior, el análisis de riesgos para Magerit **[MAGE 06]**, es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados que permiten:

- Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
- Determinar a qué amenazas están expuestos aquellos activos
- Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo
- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza

Magerit **[MAGE 06]**, presenta el proceso seguido para el análisis de riesgos, tratando primero los pasos 1, 2, 4 y 5, y finalmente el paso 3. La razón expuesta para saltar el paso 3 es que esto permite, tal y como lo indican en el libro, que las estimaciones de impacto y riesgo sean "potenciales", es decir, caso de que no hubiera salvaguarda alguna desplegada. Una vez obtenido este escenario teórico, se incorporan las salvaguardas del paso 3, derivando estimaciones realistas de impacto y riesgo.

A continuación se detallan cada uno de estos pasos siguiendo la presentación sugerida por la metodología.

Paso 1: Activos

En Magerit **[MAGE 06]**, se denominan activos a los recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección.

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

- Los servicios
- Las aplicaciones informáticas (software)
- Los equipos informáticos (hardware)
- Los soportes de información
- El equipamiento auxiliar
- Las redes de comunicaciones
- Las instalaciones
- Las personas

En este punto de la metodología se tienen en cuenta diversos aspectos para la categorización de los activos y las relaciones existentes entre ellos.

Para Magerit, no todos los activos son de la misma especie. Dependiendo del tipo de activo, las amenazas y las salvaguardas son diferentes. El "Catálogo de Elementos" presenta una relación de tipos de activos.

Dentro de la metodología encontramos un concepto muy importante para realizar el análisis de riesgos y es el de dependencia entre activos. Este concepto indica la medida en que un activo superior se vería afectado por un incidente de seguridad en un activo inferior.

Se dice que un “activo superior” depende de otro “activo inferior” cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior.

MAGERIT **[MAGE 06]**, ha desarrollado una forma de clasificación de dependencias entre activos que generalmente se dan en casi todas las organizaciones y que describimos a continuación.

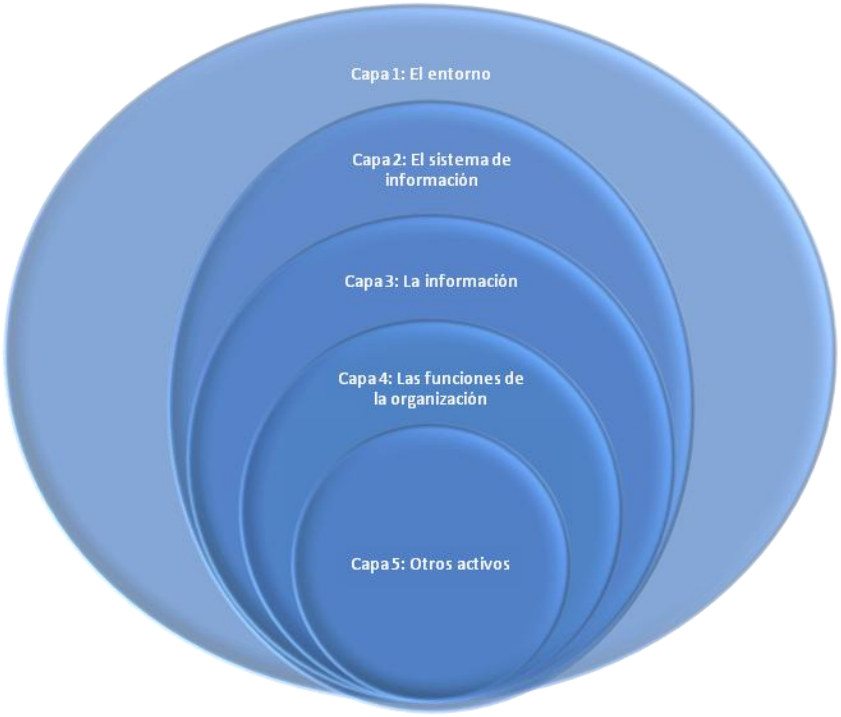


Figura 5.6. Sistema de capas para el proceso de análisis de riesgos en Magerit

En la capa 1- el entorno-, quedan encuadrados los activos que se precisan para garantizar las siguientes capas: equipamiento y suministros (energía, climatización, comunicaciones), personal (de dirección, de operación, de desarrollo, etc.) y otros como pueden ser edificios, mobiliario, etc.

En la capa 2, se encuentra el sistema de información propiamente dicho y que incluye equipos informáticos (hardware), aplicaciones (software), comunicaciones y soportes de información.

En la capa 3, encontramos la información (datos y metadatos).

En la capa 4, se sitúan las funciones de la Organización, que justifican la existencia del sistema de información y le dan finalidad así como los objetivos y la misión y los bienes y/o servicios producidos.

Por último en la capa 5, podemos encontrar otros activos como pueden ser la credibilidad o buena imagen, el conocimiento acumulado, la independencia de criterio.

Otra característica fundamental para los activos es su valor. El valor puede ser propio, o puede ser acumulado. Se dice que los activos inferiores en un esquema de dependencias, acumulan el valor de los activos que se apoyan en ellos. El valor nuclear suele estar en la información (o datos) que el sistema maneja, quedando los demás activos subordinados a las necesidades de explotación y protección de la información. La valoración de un activo puede ser cuantitativa o cualitativa.

Por último, y dentro del concepto activo, cabe hablar de sus dimensiones que se pueden calibrar desde diferentes ángulos: la autenticidad, la confidencialidad, la integridad, la disponibilidad y la trazabilidad.

Figura 5.7. Dimensiones de un activo según Magerit

Paso 2: Amenazas

El siguiente paso sugerido por la metodología **[MAGE 06]**, en el análisis de riesgos consiste en determinar las amenazas que pueden afectar a cada activo.

Las amenazas son “cosas que ocurren”. Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a nuestros activos y causar un daño.

El capítulo 5 del "Catálogo de Elementos" presenta una relación de amenazas típicas.

No todas las amenazas afectan a todos los activos, sino que hay una cierta relación entre el tipo de activo y lo que le podría ocurrir. Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía.

Una vez determinado que una amenaza puede perjudicar a un activo, hay que estimar cuán vulnerable es el activo, en dos sentidos: la degradación y la frecuencia.

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera, es decir, cómo de perjudicado resultaría el activo. La degradación se suele caracterizar como una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto “totalmente degradado”, o “degradado en una pequeña fracción”. Cuando las amenazas no son intencionales, probablemente baste conocer la fracción físicamente perjudicada de un activo para calcular la pérdida proporcional de valor que se pierde. Pero cuando la amenaza es intencional, no se puede pensar en proporcionalidad alguna pues el atacante puede causar muchísimo daño de forma selectiva.

La frecuencia pone en perspectiva aquella degradación, pues una amenaza puede ser de terribles consecuencias pero de muy improbable materialización; mientras que otra amenaza puede ser de muy bajas consecuencias, pero tan frecuente como para acabar acumulando un daño considerable.

Paso 4: Determinación del impacto

En Magerit **[MAGE 06]**, se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema. La única consideración que queda hacer es relativa a las dependencias entre activos. Es

frecuente que el valor del sistema de información se centre en los servicios que presta y los datos que maneja, al tiempo que las amenazas suelen materializarse en los medios.

Magerit diferencia dos tipos de impactos sobre un activo: el impacto acumulado y el impacto repercutido.

El impacto acumulado se calcula sobre un activo teniendo en cuenta su valor acumulado (el propio más el acumulado de los activos que dependen de él) y las amenazas a que está expuesto.

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

El impacto es tanto mayor cuanto mayor es el valor propio o acumulado sobre un activo.

El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado.

El impacto acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc.

El impacto repercutido se calcula sobre un activo teniendo en cuenta su valor propio y las amenazas a que están expuestos los activos de los que depende.

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

El impacto es tanto mayor cuanto mayor es el valor propio de un activo.

El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado.

El impacto es tanto mayor cuanto mayor sea la dependencia del activo atacado.

El impacto repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda

a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

Paso 5: Determinación del riesgo

Para Magerit **[MAGE 06]**, el riesgo es la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la frecuencia de ocurrencia. El riesgo crece con el impacto y con la frecuencia.

Sobre cada activo podemos tener riesgo acumulado, riesgo repercutido y agregación de riesgos.

Cuando hablamos de riesgo acumulado, es el que se calcula para un activo teniendo en cuenta el impacto acumulado sobre un activo debido a una amenaza y la frecuencia de la amenaza.

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

El riesgo acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc.

El riesgo repercutido es el calculado sobre un activo teniendo en cuenta el impacto repercutido sobre un activo debido a una amenaza y la frecuencia de la amenaza.

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

El riesgo repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

En los párrafos anteriores hemos reflejado los riesgos que sobre un activo tendría una amenaza en una determinada dimensión. No obstante, estos riesgos singulares pueden agregarse bajo ciertas condiciones:

- puede agregarse el riesgo repercutido sobre diferentes activos,
- puede agregarse el riesgo acumulado sobre activos que no sean dependientes entre sí, ni dependan de ningún activo superior común,
- no debe agregarse el riesgo acumulado sobre activos que no sean independientes, pues ello supondría sobreponderar el riesgo al incluir varias veces el valor acumulado de activos superiores,
- puede agregarse el riesgo de diferentes amenazas sobre un mismo activo, aunque conviene considerar en qué medida las diferentes amenazas son independientes y pueden ser concurrentes,
- puede agregarse el riesgo de una amenaza en diferentes dimensiones.

Paso 3: Salvaguardas

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

Se definen las salvaguardas o contramedidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjuran simplemente organizándose adecuadamente, otras requieren elementos técnicos (programas o equipos), otra seguridad física y, por último, está la política de personal.

El capítulo 6 del "Catálogo de Elementos" presenta una relación de salvaguardas adecuadas para cada tipo de activos.

Las salvaguardas intervienen en el cálculo del riesgo de dos formas, o bien, reduciendo la frecuencia de las amenazas o bien, limitando el daño causado. Las primeras son las que llamamos salvaguardas preventivas, que en un caso ideal, impiden completamente que la amenaza se materialice.

En el segundo caso, hay salvaguardas que limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance. Incluso algunas salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye. En cualquiera de las versiones, la amenaza se materializa; pero las consecuencias se limitan.

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

- Es teóricamente idónea
- Está perfectamente desplegada, configurada y mantenida
- Se emplea siempre
- Existen procedimientos claros de uso normal y en caso de incidencias
- Los usuarios están formados y concienciados
- Existen controles que avisan de posibles fallos

Entre una eficacia del 0% para aquellas que están de adorno y el 100% para aquellas que son perfectas, se estimará un grado de eficacia real en cada caso concreto.

Revisión del paso 4: impacto residual

Si se han hecho todos los deberes a la perfección, el impacto residual debe ser despreciable.

Si hay deberes a medio hacer (normas imprecisas, procedimientos incompletos, salvaguardas inadecuadas o insuficientes, o controles que no controlan) entonces se dice que el sistema permanece sometido a un impacto residual.

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

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

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

Revisión del paso 5: riesgo residual

Si se han hecho todos los deberes a la perfección, el riesgo residual debe ser despreciable.

Si hay deberes a medio hacer (normas imprecisas, procedimientos incompletos, salvaguardas inadecuadas o insuficientes, o controles que no controlan) entonces se dice que el sistema permanece sometido a un riesgo residual.

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

La magnitud de la degradación se toma en consideración en el cálculo del impacto residual.

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

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

4.5.2. La Gestión de Riesgos según Magerit

De acuerdo a lo sugerido en Magerit **[MAGE 06]**, el análisis de riesgos determina impactos y riesgos. Los impactos recogen daños absolutos, independientemente de que sea más o menos probable que se dé la circunstancia. En cambio el riesgo pondera la probabilidad de que ocurra. El impacto refleja el daño posible, mientras que el riesgo refleja el daño probable.

Si el impacto y el riesgo residuales son despreciables, se ha terminado. Si no, hay que hacer algo.

4.5.2.1. La interpretación de los valores de impacto y riesgo residuales

Impacto y riesgo residual son una medida del estado presente, entre la inseguridad potencial (sin salvaguarda alguna) y las medidas adecuadas que reducen impacto y riesgo a valores despreciables, se puede decir que son una métrica de carencias.

Si el valor residual es igual al valor potencial, las salvaguardas existentes no valen para nada, típicamente no porque no haya nada hecho, sino porque hay elementos fundamentales sin hacer.

Si el valor residual es despreciable, ya está. Esto no quiere decir que podamos bajar la guardia, pero sí podemos afrontar el día a día con cierta confianza. Si, por último, el valor residual es algo más que despreciable (aunque sea poco), hay una cierta exposición.

Es importante entender que un valor residual es sólo un número. Para poderlo interpretar correctamente se debe acompañar de la relación de lo que se debería hacer y no se ha hecho. Los responsables de la toma de decisiones deberán prestar cuidadosa atención a esta relación de tareas pendientes, que se denomina Informe de Insuficiencias.

4.5.2.2. Salvaguardas: selección y tipo

Las amenazas hay que intentar neutralizarlas, por principio y mientras no se justifique lo contrario.

Hay que planificar el conjunto de salvaguardas pertinentes para atajar tanto el impacto como el riesgo, bien sea reduciendo la degradación del activo (minimizando el daño) o bien reduciendo la frecuencia de la amenaza (minimizando sus oportunidades).

Toda amenaza debe ser conjurada profesionalmente, lo que quiere decir que hay que:

1. establecer una política de la Organización al respecto, o sea, unas directrices generales de quién es responsable de cada cosa

2. establecer una norma, o sea, unos objetivos a satisfacer para poder decir con propiedad que la amenaza ha sido conjurada

3. establecer unos procedimientos, o sea, instrucciones paso a paso de qué hay que hacer

4. desplegar salvaguardas técnicas que efectivamente se enfrenten a las amenazas con capacidad para conjurarlas

5. desplegar controles que permitan saber que todo lo anterior está funcionando según lo previsto.

A este conjunto de elementos se le encasilla habitualmente bajo el nombre de Sistema de Gestión de la Seguridad de la Información (SGSI), aunque se está gestionando tanto como actuando.

De lo expuesto anteriormente puede interpretarse que hay que llevar a cabo todos y cada uno de los puntos para cada amenaza. No es así. En la práctica lo dicho se traduce en desarrollar una política, unas normas y unos procedimientos junto con el despliegue de una serie de salvaguardas y controles y, ahora sí, verificar que todas y cada una de las amenazas tienen una respuesta adecuada.

De los puntos anteriores, el más "abierto", el que puede dar lugar a diversas interpretaciones es el que se refiere a la determinación de las salvaguardas apropiadas.

Es realmente un arte que requiere personal especializado aunque en la práctica las situaciones más habituales están perfectamente documentadas en la documentación existente y basta elegir de entre un catálogo en función de la magnitud del riesgo.

En los párrafos siguientes vamos a analizar los tipos de salvaguardas existentes y como seleccionarlas.

Un sistema debe considerar prioritariamente las salvaguardas de tipo preventivo que buscan que la amenaza no ocurra o su daño sea despreciable, es decir, aquellas que impidan incidentes o ataques.

En la práctica, no todo es previsible, ni todo lo previsible es económicamente razonable atajarlo en sus orígenes. Tanto para enfrentar

lo desconocido como para protegerse de aquello a lo que se permanece expuesto, es necesario disponer de elementos que detecten el inicio de un incidente y permitan reaccionar con presteza impidiendo que se convierta en un desastre.

Tanto las medidas preventivas como las de emergencia admiten una cierta degradación de los activos por lo que habrá que disponer por último de medidas de recuperación que devuelvan el valor perdido por los activos.

Es de sentido común intentar actuar de forma preventiva para que las cosas no ocurran o no puedan causar mucho daño; pero no siempre es posible y hay que estar preparados para que ocurran. Lo que no debe ser de ninguna manera es que un ataque pase inadvertido: hay que detectarlo, registrarlo y reaccionar primero con un plan de emergencia (que pare y limite el incidente) y después con un plan de continuidad y recuperación para regresar a donde se debe estar.

Completando lo expuesto anteriormente hay que recordar que conviene llegar a un cierto equilibrio entre:

- Salvaguardas técnicas: en aplicaciones, equipos y comunicaciones
- Salvaguardas físicas: protegiendo el entorno de trabajo de las personas y los equipos
- Medidas de organización: de prevención y gestión de las incidencias
- Política de personal: que, a fin de cuentas, es el eslabón imprescindible y más delicado (política de contratación, formación permanente, informe de incidencias, plan de reacción y medidas disciplinarias)

4.5.2.3. Pérdidas y ganancias

En primer lugar y aunque es de sentido común, debemos señalar que no se puede invertir en salvaguardas más allá del valor de los propios

activos a proteger. Por lo tanto, se hace necesario analizar el coste de la inseguridad (lo que costaría no estar protegidos) y el coste de las salvaguardas.

Siguiendo las directrices que marca la metodología que estamos estudiando, en la práctica cuando hay que protegerse de un riesgo que se considera significativo, aparecen varios escenarios hipotéticos (En):

E0: si no se hace nada

E1: si se aplica un cierto conjunto de salvaguardas

E2: si se aplica otro conjunto de salvaguardas

Y así en "n" escenarios con diferentes combinaciones de salvaguardas.

El análisis económico tendrá como misión decidir entre estas opciones, siendo E0 (no hacer nada) una opción posible, que pudiera estar justificada económicamente.

En cada escenario hay que estimar el coste que va a suponer. Para poder agregar costes, se contabilizan como valores negativos las pérdidas de dinero y como valores positivos las entradas de dinero:

− (recurrente) riesgo residual

− (una vez) coste de las salvaguardas

− (recurrente) coste anual de mantenimiento de las salvaguardas

+ (recurrente) mejora en la productividad

+ (recurrente) mejoras en la capacidad de la Organización para prestar nuevos servicios, conseguir mejores condiciones de los proveedores, entrar en asociación con otras organizaciones, etc.

4.5.2.4. La actitud de la Dirección

La dirección de la Organización sometida al análisis de riesgos debe determinar el nivel de impacto y riesgo aceptable. Más propiamente dicho, debe aceptar la responsabilidad de las insuficiencias.

Esta decisión no es técnica. Puede ser una decisión política o gerencial o puede venir determinada por ley o por compromisos

contractuales con proveedores o usuarios. Estos niveles de aceptación se pueden establecer por activo o por agregación de activos (en un determinado departamento, en un determinado servicio, en una determinada dimensión.)

Cualquier nivel de impacto y/o riesgo es aceptable si lo conoce y acepta formalmente la Dirección.

Si el impacto y/o el riesgo están por encima de lo aceptable, se puede o bien eliminar el activo que, aunque suena muy fuerte a veces hay activos que, simplemente, no vale la pena mantener; o bien, introducir nuevas salvaguardas o mejorar la eficacia de las presentes

Para Magerit un proyecto de Análisis y Gestión de Riesgos (AGR) conlleva tres procesos básicos:

Proceso P1: Planificación

- Se establecen las consideraciones necesarias para arrancar el proyecto AGR.
- Se investiga la oportunidad de realizarlo.
- Se definen los objetivos que ha de cumplir y el dominio (ámbito) que abarcará.
- Se planifican los medios materiales y humanos para su realización.
- Se procede al lanzamiento del proyecto.

Proceso P2: Análisis de riesgos

- Se identifican los activos a tratar, las relaciones entre ellos y la valoración que merecen.
- Se identifican las amenazas significativas sobre aquellos activos y se valoran en términos de frecuencia de ocurrencia y degradación que causan sobre el valor del activo afectado.
- Se identifican las salvaguardas existentes y se valora la eficacia de su implantación.

- Se estima el impacto y el riesgo al que están expuestos los activos del sistema.
- Se interpreta el significado del impacto y el riesgo.

Proceso P3: Gestión de riesgos

- Se elige una estrategia para mitigar impacto y riesgo.
- Se determinan las salvaguardas oportunas para el objetivo anterior.
- Se determina la calidad necesaria para dichas salvaguardas.
- Se diseña un plan de seguridad (plan de acción o plan director) para llevar el impacto y el riesgo a niveles aceptables.
- Se lleva a cabo el plan de seguridad.

4.6. Herramienta de apoyo para el análisis de riesgos: PILAR

PILAR, acrónimo de "Procedimiento Informático-Lógico para el Análisis de Riesgos" es una herramienta desarrollada bajo especificación del Centro Nacional de Inteligencia para soportar el análisis de riesgos de sistemas de información siguiendo la metodología Magerit, **[MAGE 06]**.

La herramienta soporta todas las fases del método Magerit: caracterización de los activos -identificación, clasificación, dependencias y valoración-, caracterización de las amenazas y evaluación de las salvaguardas.

La herramienta, también incorpora los catálogos del "Catálogo de Elementos" permitiendo una homogeneidad en los resultados del análisis con relación a tipos de activos, dimensiones de valoración, criterios de valoración y catálogo de amenazas.

Para incorporar este catálogo, PILAR diferencia entre el motor de cálculo de riesgos y la biblioteca de elementos, que puede ser reemplazada para seguir el paso de la evolución en el tiempo de los catálogos de elementos.

La herramienta evalúa el impacto y el riesgo, acumulado y repercutido, potencial y residual, presentándolo de forma que permita el análisis de por qué se da cierto impacto o cierto riesgo.

Las salvaguardas se califican por fases, permitiendo la incorporación a un mismo modelo de diferentes situaciones temporales. Típicamente se puede incorporar el resultado de los diferentes programas de seguridad a lo largo de la ejecución del plan de seguridad, monitorizando la mejora del sistema.

Los resultados se presentan en varios formatos: informes RTF, gráficas y tablas para incorporar a hojas de cálculo. De esta forma es posible elaborar diferentes tipos de informes y presentaciones de los resultados.

Por último, la herramienta calcula calificaciones de seguridad siguiendo los epígrafes de normas *de iure* o *de facto* de uso habitual. Cabe citarse:

- Criterios de Seguridad, normalización y conservación
- UNE-ISO/IEC 17799:2002: sistemas de gestión de la seguridad
- Real Decreto 1720/2007: reglamento de desarrollo de la LOPD.

Por último hay que destacar que PILAR incorpora tanto los modelos cualitativos como cuantitativos, pudiendo alternarse entre uno y otro para extraer el máximo beneficio de las posibilidades teóricas de cada uno de ellos.

5. OCTAVE

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), **[OCTA 08]**, es un método de análisis de riesgos orientado a activos, desarrollado por el CERT (Coordination Center, del Software Engineering Institute de la Universidad Carnegie Mellon de Pensilvania, Estados Unidos).

En OCTAVE, los activos incluyen personas, hardware y software, información y sistemas. Los activos se ordenan según la importancia que tienen para los objetivos de la organización, y las posibles amenazas y vulnerabilidades asociadas a dichos activos, así como el impacto que causaría un problema en cada activo.

El objetivo de OCTAVE es desarrollar una perspectiva de seguridad dentro de una organización, teniendo en cuenta perspectivas de todos los niveles para asegurarse que las soluciones puedan implementarse con facilidad.

Aunque OCTAVE fue desarrollada pensando en empresas, está diseñada para ser flexible y poder adaptarse a cualquier entorno. Esta flexibilidad tiene la ventaja de no atarse a ningún código concreto de buenas prácticas, poniendo el énfasis en dirigir la seguridad de la información con independencia de la tecnología actual.

OCTAVE tiene dos objetivos específicos que son:

1. Desmitificar la falsa creencia de que la Seguridad Informática es un asunto meramente técnico.
2. Presentar los principios básicos y la estructura de las mejores prácticas internacionales que guían los asuntos no técnicos.

Con relación a los activos, OCTAVE los clasifica en dos grandes grupos:

1. Sistemas: Hardware. Software y Datos.
2. Personas.

Cuando se aplica esta metodología se hace un trabajo conjunto con las diferentes áreas de la organización centrándose en las necesidades de seguridad y equilibrando los siguientes tres aspectos: riesgos operativos, prácticas de seguridad y tecnología.

El objetivo de OCTAVE va direccionado a dos aspectos diferentes: riesgos operativos y prácticas de seguridad. En este caso la tecnología es examinada en proporción a las prácticas de seguridad, esto permite a las compañías realizar la toma de decisiones de protección de información basados en los riesgos de confidencialidad, integridad y disponibilidad de los bienes afines a la información crítica.

De acuerdo a lo expuesto en la metodología, **[OCTA 08]**, OCTAVE tiene tres fases de desarrollo, que hemos esquematizado en la figura anterior y que vamos a detallar un poco más (en cuanto a sus procesos).

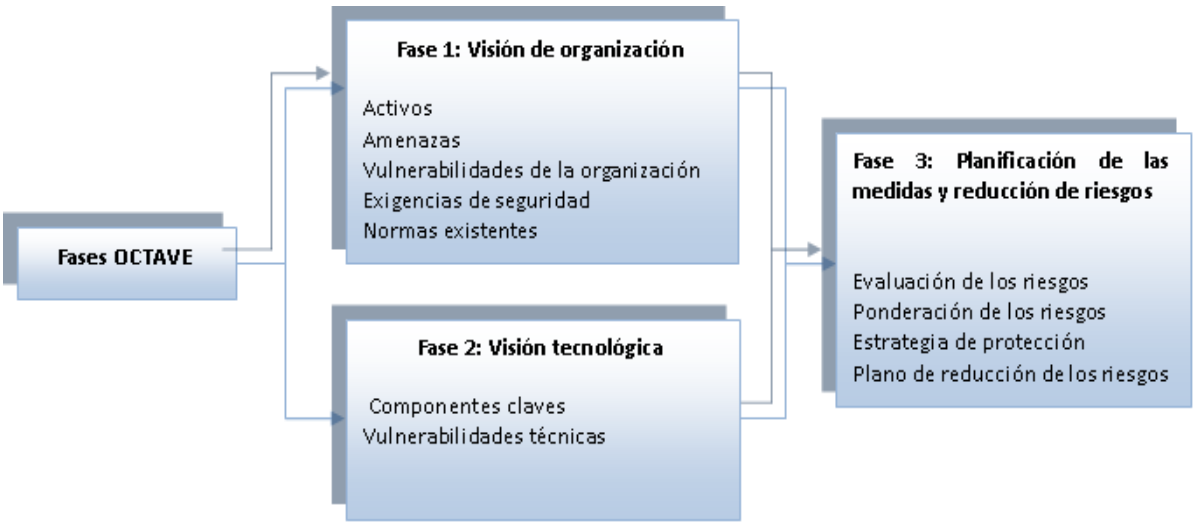


Figura 5.8. Fases de desarrollo de Octave. [OCTA 08]

Fase 1: Visión de la organización

Para realizar esta fase OCTAVE ha desarrollado una serie de procesos (1-4) que desarrollamos a continuación:

Proceso 1: Identificar el conocimiento de los altos directivos

En este proceso se recopila información de los principales activos de la organización, los niveles de seguridad y los motivos de preocupación por esos activos, así como también las estrategias actuales de protección y las vulnerabilidades de la organización. Los participantes de este nivel son los altos directivos de la organización.

Proceso 2: Identificar el conocimiento de los directivos de áreas operativas

Este proceso tiene como objetivo recopilar información a nivel operativo, es decir, de los encargados operacionales de los activos importantes de la organización, de igual forma que en el anterior proceso se identificará los requisitos de seguridad y los motivos de preocupación por esos activos. Los participantes de este nivel son los encargados de las aéreas operativas.

Proceso 3: Identificar el conocimiento del personal

En este nivel se recopila información de miembros del personal sobre activos importantes de la organización, requisitos de seguridad y motivos de preocupación por esos activos, estrategias actuales de la protección y vulnerabilidades de la organización.

En este nivel hay dos tipos de participantes: el personal de planta y el personal del departamento de Tecnología de Información.

Proceso 4: Crear perfiles de amenaza

En este proceso el equipo de análisis analiza la información obtenida durante los procesos 1 al 3, en donde se seleccionan 5 activos críticos sobre los cuales se definen los requisitos y las amenazas de seguridad para esos activos.

Fase 2: Visión Tecnológica

De igual forma en esta fase hay que continuar con los procesos para desarrollar de una manera correcta el análisis y gestión de riesgos dentro de una organización:

Proceso 5: Identificar componentes claves, los cuales son sistemas importantes para activos críticos.

En este nivel para cada activo crítico encontrado hay que identificar los componentes claves que se deben evaluar para las vulnerabilidades de la tecnología. El equipo de análisis realiza esta actividad, con ayuda del personal de TI, según la necesidad

Proceso 6: Evaluación de componentes seleccionados, donde debemos identificar las principales vulnerabilidades de los componentes críticos.

En este nivel el equipo del análisis y los miembros de equipo suplementarios evalúan cada uno de los componentes de la infraestructura de tecnología, identificando las vulnerabilidades de los mismos. Aquí se necesita la ayuda de herramientas de evaluación de vulnerabilidades.

Fase 3: Planificación de las medidas y reducción de riesgos

En esta última fase se deben seguir los siguientes procesos:

Proceso 7: Realizar un análisis de riesgos

Donde debemos identificar los riesgos que se podrían dar sobre los activos críticos de una organización.

Para realizar este proceso se utiliza la información recopilada. Este proceso utiliza la información de los procesos 1 al 6 para crear los perfiles de riesgo para los activos críticos, en donde se define cada una de las descripciones de los impactos encontrados, se crean los criterios de evaluación, y al final se evalúan los resultados de cada amenaza contra los criterios. Este proceso es realizado por el equipo del análisis, en colaboración con personal suplementario (encargado operacional del área) según lo necesitado.

Proceso 8: Desarrollo de estrategias de protección

Donde se debe definir una serie de acciones, estrategias y planes para proteger los activos críticos, los cuales deberán ser estudiados y aprobados para su ejecución.

En la figura siguiente se resumen los procesos que se ejecutan cuando se lleva a cabo un análisis de riesgos utilizando la metodología OCTAVE.

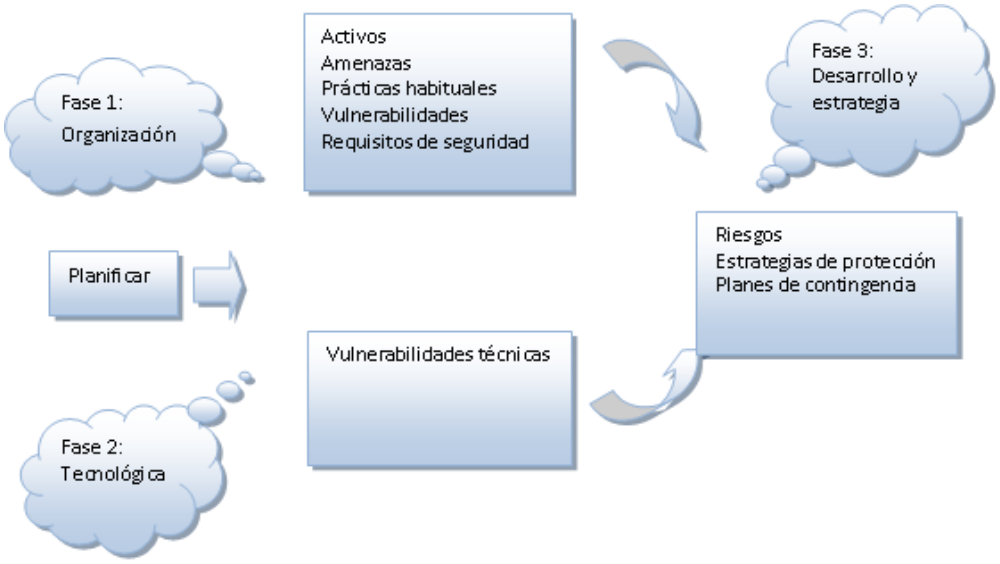


Figura 5.9. Proceso para la gestión de riesgos en Octave. [OCTA 08]

6. ISO/IEC 27005:2011: Tecnologías de la información –Técnicas de seguridad- Gestión del riesgo de seguridad de la información

La norma ISO/IEC 27005:2011, **[ISO/IEC 11]**, forma parte de la familia de ISO 27000 enfocada a la seguridad de la información, siendo un complemento a las normas ISO/IEC 27001 e ISO 27002, las cuales definen las necesidades de elaborar un análisis de riesgos pero no especifican directrices para ello.

La norma proporciona un marco para la implementación de un enfoque de gestión de riesgos, ayudando a gestionar los riesgos en un sistema de gestión de seguridad de la información (SGSI). En la norma se describe el proceso de gestión de riesgos y apoya los conceptos generales especificados en la norma ISO/IEC 27001:2005, Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad – Requisitos.

La norma como tal no proporciona ninguna metodología específica para la gestión de riesgos de seguridad, sino que aporta un enfoque genérico para la gestión de riesgos que debe apoyarse en metodologías específicas de análisis y gestión de riesgos; es aplicable a cualquier tipo de organización que quiera mejorar la gestión de sus riesgos en seguridad de la información.

En esta segunda edición, el marco descrito en la norma ISO/IEC 27005 ha sido revisado y actualizado para reflejar el contenido de los documentos de gestión de riesgos:

- ISO 31000:2009, Gestión de riesgos - Principios y directrices,
- ISO / IEC 31010:2009, Gestión de riesgos - las técnicas de evaluación de riesgos, e
- ISO Guide73: 2009, La gestión del riesgo - Vocabulario

La norma tiene el propósito de alinearse con ISO 31000:2009 con el fin de ayudar a las organizaciones que deseen gestionar sus riesgos de seguridad de la información de una manera similar a la forma de gestionar "otros" riesgos.

ISO/IEC 27005:2011 ayudará a los usuarios en la implementación de ISO/IEC 27001, la norma de sistemas de gestión de seguridad de la información, que se basa en un enfoque de gestión de riesgos. El conocimiento de los conceptos,

modelos, procesos y terminologías descritos en la norma ISO/IEC 27001 e ISO/IEC 27002: 2005, Tecnología de la información - Técnicas de seguridad - Código de buenas prácticas para la gestión de seguridad de la información, es importante para una comprensión completa de esta Norma Internacional.

La norma está estructurada en 12 cláusulas y 6 anexos que apoyan el desarrollo de cada una de las cláusulas. Las cláusulas que la conforman son las siguientes:

1. Objeto y campo de aplicación
2. Referencias y Normativas
3. Términos y definiciones
4. Estructura
5. Información general
6. Visión general
7. Establecimiento del contexto
8. Valoración del riesgo
9. Tratamiento del riesgo
10. Aceptación del riesgo
11. Comunicación del riesgo de SI
12. Monitoreo y Revisión

El proceso de gestión de riesgos propiamente dicho se describe a partir de la cláusula 7 y que mencionaremos de forma general a continuación.

Cláusula 7. Establecimiento del contexto, se definen los objetivos, el alcance y la organización para todo el proceso (políticas, enfoque)

Cláusula 8. Valoración del riesgo, se obtiene toda la información necesaria para conocer, valorar y priorizar los riesgos. Se divide en tres apartados:

- Identificación de riesgos
- Estimación de riesgos
- Evaluación de riesgos

Cláusula 9. Tratamiento del riesgo, define la estrategia para tratar cada uno de los riesgos valorados: reducción, aceptación, evitación o transferencia.

Cláusula 10. Aceptación del riesgo, se determinan los riesgos que se decide aceptar, y la justificación correspondiente a cada riesgo aceptado. Se debe tratar el riesgo residual.

Cláusula 11. Comunicación del riesgo, todos los grupos de interés intercambian información sobre riesgos, esta comunicación debe hacerse durante todo el proceso.

Cláusula 12. Monitoreo y Revisión del riesgo, el análisis de riesgos se actualiza con todos los cambios internos o externos que afectan a la valoración de los riesgos. Se realiza un monitoreo y evaluación continua.

Como mencionamos anteriormente la norma ofrece, además, una serie de anexos que apoyan todo el proceso de gestión de riesgos y que citamos a continuación:

Anexo A: Alcance y Limitaciones

Anexo B: Identificación, evaluación de activos y valoración de impactos

Anexo C: Ejemplos de amenazas críticas

Anexo D: Vulnerabilidades y métodos para valorarlas

Anexo E: Enfoques para la valoración de riesgos

Anexo F: Obligaciones para reducción de riesgos

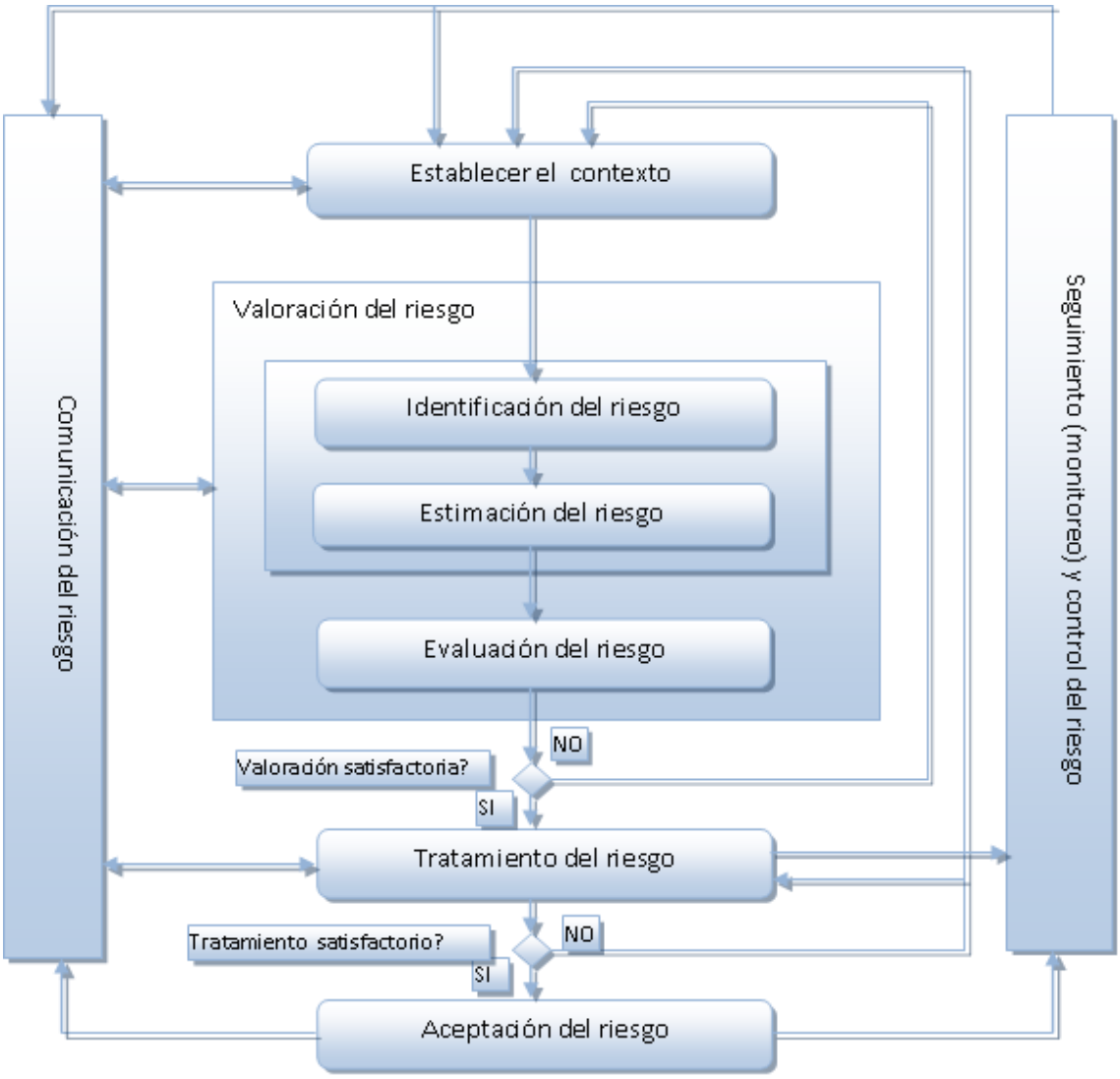


Figura 5.10. Proceso para la gestión de riesgos en ISO 27005. [ISO/IEC 11]

7. MEHARI: Método Armonizado de Análisis de Riesgos

MEHARI, **[MEHA 10]**, es una metodología desarrollada por la comisión de métodos de Clusif (Club Francés de la Seguridad de la Información) en 1996 y es de acceso público.

Mehari es un conjunto de herramientas y funcionalidades metodológicas para la gestión de la seguridad y de las medidas asociadas, basado en un análisis de riesgo preciso. Los aspectos fundamentales de MEHARI son:

- Su modelo de riesgo (cualitativo y cuantitativo),
- El examen de la eficacia de las medidas de seguridad en vigor previstas
- La capacidad para evaluar y simular los niveles de riesgo derivado de medidas adicionales

Conforme a lo expuesto en los documentos oficiales de la metodología, **[MEHA 10]**, Mehari proporciona un marco metodológico, componentes modulares y bases de datos de conocimiento, con el fin de:

- Analizar los principales problemas
- Analizar las vulnerabilidades
- Disminuir y controlar los riesgos
- Supervisar la seguridad de la información

El principal objetivo de Mehari es proporcionar un método para la evaluación y gestión de riesgos, concretamente en el dominio de la seguridad de la información, conforme a los requerimientos ISO/IEC 27005:2008, proporcionando el conjunto de herramientas y elementos necesarios para su implementación.

Otros objetivos adicionales son:

- Permitir un análisis directo e individual de situaciones de riesgos descritas en los escenarios,
- Proporcionar un completo conjunto de herramientas específicamente diseñadas para la gestión de la seguridad a corto, medio y largo plazo,

adaptables a diferentes niveles de madurez y tipos de acciones consideradas.

Mehari proporciona una metodología consistente, con unas bases de datos de conocimiento adecuadas, para ayudar a los responsables de seguridad u otras personas implicadas en la reducción de riesgos, en sus diferentes tareas y actividades.

Las diferentes herramientas y módulos de la metodología MEHARI, diseñados para acompañar un análisis de riesgos directo e individual, se pueden utilizar de forma separada unas de otras en cualquier etapa del desarrollo de la seguridad, utilizando diferentes enfoques de gestión y garantizando la consistencia de las decisiones resultantes.

Los módulos que componen Mehari se pueden seleccionar, basados en las políticas corporativas o las estrategias seleccionadas, para decidir y construir planes de acción de seguridad para la seguridad de la información. Los módulos propuestos por la metodología son los siguientes:

- Análisis o evaluación de riesgos
- Evaluación de seguridad (Evaluación de vulnerabilidades)
- Análisis de amenazas

Mehari cuenta con una serie de documentos donde se describe con mayor detalle la metodología y son los siguientes:

- Mehari: Conceptos y especificaciones funcionales
- Guías Mehari para Análisis y clasificación de amenazas
- Guía Mehari para Evaluación de servicios de seguridad
- Guías Mehari para Análisis de Riesgos
- Mehari Manual de referencia de servicios de seguridad
- Mehari base de datos de conocimiento

Según la metodología, una situación de riesgo se puede caracterizar por diferentes factores:

- Factores de reducción del riesgo, que son una función directa de las medidas de seguridad implementadas.
- Factores estructurales (u organizacionales), los cuales no dependen de medidas de seguridad, sino de la actividad principal de la organización, su entorno y su contexto.

Con el fin de evaluar los riesgos, se proponen dos opciones:

- Utilizar una serie de funciones de la base de datos de conocimiento que permita integrar los resultados de los módulos de MEHARI. Desde estas funciones es posible evaluar el nivel actual de riesgo y proponer medidas adicionales para la reducción del mismo.
- Emplear una aplicación software que proporciona una interfaz más completa que permite simulaciones, visualizaciones y más optimizaciones.

El módulo de evaluación de la seguridad permite la confección de planes de seguridad, como resultado directo de la evaluación del estado de los servicios de seguridad.

Mehari integra cuestionarios de controles de seguridad, lo que permite evaluar el nivel de calidad de los mecanismos y soluciones encaminadas a la reducción del riesgo.

La metodología proporciona un modelo de riesgos estructurado que considera los "factores de reducción del riesgo" en forma de servicios de seguridad.

Para realizar la evaluación de seguridad se puede utilizar directamente la base de datos de conocimiento Mehari para crear un marco de referencia de seguridad (o políticas de seguridad) que contendrá, y describirá, el conjunto de reglas e instrucciones de seguridad que debe seguir la empresa u organización

Mehari proporciona un módulo de análisis de amenazas que proporciona dos tipos de resultados:

- Una escala de valores de malfuncionamiento
- Una clasificación de la información y de los activos de TI

8. CRAMM-CCTA: Risk Analysis and Management Methodology-Metodología para el análisis y la gestión de riesgos

CRAMM-CCTA, **[CRAM 06]**, es una metodología de análisis y gestión de riesgos desarrollada en Reino Unido por la Agencia Central de Cómputo y Telecomunicaciones (CCTA) en 1987, y actualmente se encuentra en la versión 5.2. Esta metodología es usada de forma preferente en organismos de la administración pública británica y se ha ido extendiendo al sector privado. Actualmente es utilizada por la OTAN, el Ejército de Holanda, y numerosas empresas de todo el mundo.

Podemos decir que CRAMM es en esencia:

- Una metodología para el análisis y la gestión de riesgos.
- Una metodología que aplica sus conceptos de una manera formal, estructurada y disciplinada.
- Una metodología orientada a proteger la confidencialidad, integridad y disponibilidad de un sistema de información y de sus activos.
- Una metodología que, aunque se la encuadre, a veces, como cuantitativa, utiliza evaluaciones cuantitativas y cualitativas; por lo cual se dice que tiene un carácter mixto.

Los objetivos fundamentales que se persiguen al realizar un análisis de riesgos CRAMM son:

- Identificar las amenazas a conjuntos de activos, haciendo además una evaluación de los grados o importancia de estas vulnerabilidades
- Evaluar los niveles de riesgo, calculados a partir de las valoraciones de los activos, y de los niveles de amenazas y vulnerabilidades evaluados.

Por su parte, los objetivos que se persiguen al llevar a cabo la gestión de riesgos CRAMM, son:

- Orientar a que los responsables de la seguridad estén en condiciones, bien de evitar o aceptar riesgos individuales o bien de reducir los riesgos a un nivel aceptable.

- Reducir los riesgos a un nivel aceptable adoptando las contramedidas (en la metodología se utiliza la palabra contramedida que es similar a salvaguarda) apropiadas.

Uno de los aspectos principales de CRAMM es el soporte que proporciona la herramienta informática que posee, 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

Esta metodología, tal y como se indica en su web oficial, **[CRAM 06]**, sigue tres etapas para realizar el proceso de análisis y gestión de riesgos, las cuales se describen a continuación:

8.1. Primera etapa CRAMM: Identificación y valoración de activos

CRAMM permite identificar y valorar los activos físicos (el hardware, instalaciones), los activos de software (sistemas y aplicaciones), los datos (la información contenida en un sistema informático). Los activos físicos se valoran en términos del coste de reemplazo. Los activos de datos y de software se valoran en términos del impacto que se produciría si la información no estuviera disponible, fuera destruida, divulgada o modificada.

8.2. Segunda etapa CRAMM: Evaluación de amenazas y vulnerabilidad

Una vez comprendida la magnitud de los problemas potenciales, el siguiente paso es identificar cómo de probable es que estos problemas ocurran. CRAMM cubre toda la gama de amenazas deliberadas o accidentales que puedan afectar a los sistemas de información, incluyendo hacking, virus, fallos de equipos o software, daños intencionales o el terrorismo y errores humanos.

Esta etapa concluye con el cálculo del nivel del riesgo subyacente o real.

8.3. Tercera etapa CRAMM: selección y recomendación de contramedidas

CRAMM contiene una gran biblioteca que consta de más de 3000 contramedidas detalladas organizadas en más de 70 agrupaciones lógicas. El software CRAMM utiliza las medidas de los riesgos determinados en la etapa anterior y los compara con el nivel de seguridad (un nivel de umbral asociado a cada contramedida), con el fin de determinar si los riesgos son lo suficientemente grandes para justificar la implementación de una determinada contramedida. CRAMM ofrece una serie de utilidades, que incluyen la posibilidad de hacer un análisis hacia atrás, que permita responder interrogantes como: ¿Qué pasa si?, funciones de asignación de prioridades y herramientas de reportes, que ayudan en la implementación de las contramedidas y la activa gestión de los riesgos identificados.

En la figura 5.11, se puede observar el modelo que sigue CRAMM para el análisis y la gestión de riesgos.

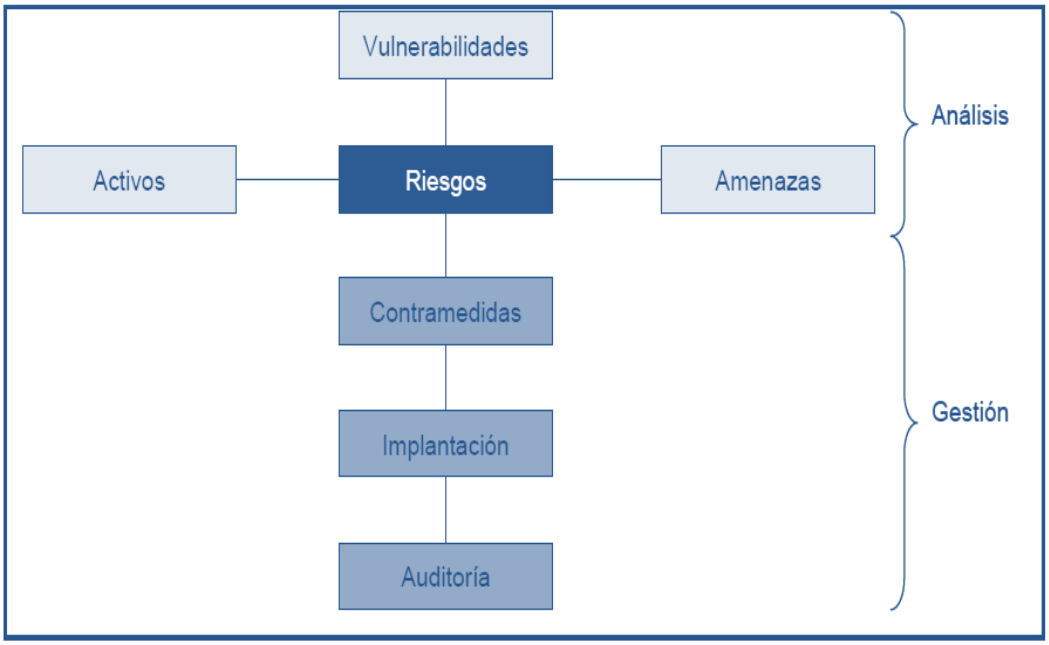


Figura 5.11 Modelo de análisis y gestión de riesgos de CRAMM. [CRAM 06]

9. Listado de algunas metodologías, estándares y herramientas para el análisis y la gestión de riesgos [ISSA 11]

- MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), promovida por el Ministerio de Administraciones Públicas de España.
- EAR/Pilar (Entorno de análisis de riesgos). Herramienta en español, basada en Magerit.
- ISO/IEC 27005 es el estándar ISO de la serie 27000 dedicado a la gestión de riesgos de seguridad de la información.
- MEHARI (Méthode Harmonisée d'Analyse de Risques). Método de análisis y gestión de riesgos, desarrollado por el Clusif (Club de la Sécurité des Systèmes d'Information Français).
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation). Metodología de evaluación de riesgos desarrollada por el Software Engineering Institute (SEI) de la Carnegie Mellon University. OCTAVE-S es la versión para pequeñas empresas (menos de 100 empleados).
- CRAMM (CCTA Risk Analysis and Management Method). Metodología y herramienta de análisis y gestión de riesgos desarrollada por la "Central Computer and Telecommunications Agency" del Reino Unido y gestionada por "Insight Consulting Limited" (Grupo Siemens). Existe en versión Expert y Express, incluye software y no es gratuita.
- Inventario de metodologías y herramientas de análisis y gestión de riesgos de ENISA (European Network and Information Security Agency). Incluye sistema de comparativas.
- "Risk management guide for information technology systems". Publicada por NIST (National Institute of Standards and Technology) de EEUU.
- AS/NZS ISO 31000:2009 es el estándar australiano de gestión de riesgos de la seguridad de la información.
- EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité). Metodología de gestión de los riesgos de seguridad de sistemas de

información desarrollada por la ”Direction Centrale de la Sécurité des Systèmes d’Information” francesa. Disponible en español. Está acompañada por un software multilingüe -francés, inglés, alemán, español- gratuito para varias plataformas -Windows, Linux, Solaris-.

- Estándar de análisis de riesgos del “Bundesamt für Sicherheit in der Informationstechnik” de Alemania.
- IRAM (Information Risk Analysis Methodologies) es una metodología de análisis de riesgos del Information Security Forum sólo disponible para sus miembros.
- FIRM (Fundamental Information Risk Management) es una metodología de gestión de riesgos del Information Security Forum.
- Citicus ONE es un software comercial (disponible en varios idiomas, pero no en español) de gestión de riesgos de seguridad de la información, basado en la metodología FIRM.
- Guía en inglés de evaluación de riesgos de la Policía de Canadá.
- Introducción a la metodología FAIR (Factor Analysis of Information Risk).
- Security Risk Management Guide de Microsoft.
- COBRA (Consultative, Objective and Bi-functional Risk Analysis). Software -no gratuito- de evaluación del riesgo de “C&A Systems Security Ltd.”.
- RA2 – Art of Risk. Software de análisis de riesgos y soporte de SGSI. No es gratuito.
- Whitepaper de SANS sobre gestión del riesgo.
- Guía de evaluación de riesgos de seguridad de ASIS.
- CERO es una aplicación web que permite tener una visión global de los riesgos a los que se expone una compañía, Operativos y de LA/FT.

CAPÍTULO VI: El análisis de riesgos dentro de una auditoría informática

1. Introducción

El objetivo de este capítulo es realizar un análisis del papel del "análisis de riesgos dentro de una auditoría informática" como tema central de este PFC, de tal manera que podamos encajarlo dentro de una propuesta metodológica de una auditoría informática basada en riesgos.

Para realizar este análisis vamos a estudiar cada área de forma independiente y luego analizaremos cómo encaja el análisis de riesgos dentro de una auditoría, vamos a partir de los aportes realizados por entidades y metodologías oficiales e iremos realizando un análisis personal de dichos aportes, evaluando de qué forma el análisis de riesgos puede servir a una auditoría informática.

2. El papel del análisis de riesgos dentro de una auditoría informática

En la actualidad las organizaciones están experimentando un aumento en el uso de tecnologías para el procesamiento de información vital para el desarrollo de sus objetivos de negocio. La gestión efectiva de dicha información así como de las tecnologías que soportan su procesamiento y explotación es un aspecto fundamental para el éxito de dichas organizaciones, máxime cuando esta información traspasa las fronteras organizacionales y viaja a través de redes, lo cual conlleva un incremento de las vulnerabilidades y por ende de las amenazas.

Por otro lado, las organizaciones tienden a tener una mayor dependencia de las tecnologías de la información y los sistemas informáticos, lo cual hace que se hagan inversiones importantes en infraestructura tecnológica para soportar sus procesos de negocio, que a su vez también requiere de una adecuada gestión.

Así pues, en este contexto, se deben generar estrategias y planes que proporcionen directrices efectivas de control y que permitan la realización de un proceso de evaluación, revisión y verificación de la información, de los procesos y tecnologías que los soportan.

La auditoría informática y el análisis de riesgos han sido los métodos usados comúnmente de forma independiente para evaluar los sistemas de información, cada una con un enfoque diferente. De un lado la auditoría informática es un proceso de revisión y verificación y el análisis de riesgos un proceso de diagnóstico y revisión.

La auditoría informática sólo identifica el nivel de "exposición" por la falta de controles, mientras que el análisis de riesgos facilita la "evaluación" de los riesgos y recomienda acciones en base al coste/beneficio de las mismas, tal y cómo se indica en, **[SOBR 99].**

Debido a los cambios en los modelos de operación de los negocios, impulsados por los avances en las tecnologías de información -que hemos indicado anteriormente-, el surgimiento de normativas nacionales e internacionales en el ámbito de las tecnologías de información relacionadas con el procesamiento, explotación y entrega de información y servicios basados en dichas tecnologías, y los nuevos modelos de control interno impulsados por ejemplo, por marcos de trabajo ampliamente conocidos y aceptados como COBIT, la auditoría informática se ha enfrentado a la necesidad de evolucionar de un enfoque de verificación efectuado a posteriori, a un enfoque preventivo y proactivo basado en la valoración de los riesgos y la evaluación de la eficacia y eficiencia de los procedimientos y los controles establecidos en las organizaciones, orientados a mejorar las características de seguridad, calidad, eficiencia y eficacia de los sistemas de información y las tecnologías asociadas.

Ahora bien, cabe preguntarnos cómo encajar el análisis de riesgos y la auditoría informática. Para responder a este interrogante vamos a remitirnos a algunas metodologías y/o estándares que consideran el análisis de riesgos como parte de una auditoría informática.

En primer lugar encontramos en **[MAGE 06]** la siguiente referencia al tema:

"El análisis de riesgos es una piedra angular de los procesos de evaluación, certificación, auditoría y acreditación que formalizan la confianza que merece un sistema de información. Dado que no hay dos sistemas de información iguales, la evaluación de cada sistema concreto requiere amoldarse a los componentes que

lo constituyen. El análisis de riesgos proporciona una visión singular de cómo es cada sistema, qué valor posee, a qué amenazas está expuesto y de qué salvaguardas se ha dotado".

"Una auditoría puede servirse de un análisis de riesgos que le permita (1) saber qué hay en juego, (2) saber a qué está expuesto el sistema y (3) valorar la eficacia y eficiencia de las salvaguardas."

De acuerdo a lo expuesto podemos observar que el papel que puede desempeñar un análisis de riesgos dentro de una auditoría informática, está enfocado a utilizar la información proveniente de dicho análisis relativa al valor que posee el o los sistemas o procesos a auditar, las amenazas y sus salvaguardas, lo cual le permitirá al auditor focalizar su trabajo y a priorizar las áreas o procesos a auditar.

Encontramos en **[ISAC 07]**, en su serie de estándares, guías y procedimientos al respecto del tema que nos ocupa, el estándar **S11: Uso de la evaluación de riesgos en la planeación de auditoría,** que nos proporciona las siguientes líneas básicas:

"El auditor de SI debe utilizar una técnica o enfoque apropiado de evaluación de riesgos al desarrollar el plan general de auditoría de SI y al determinar prioridades para la asignación eficaz de los recursos de auditoría de SI.

Al planear revisiones individuales, el auditor de SI debe identificar y evaluar los riesgos relevantes al área bajo revisión."

Para la aplicación de este estándar, **[ISAC 10]** recomienda el uso de la guía **G13: Uso de la evaluación de riesgos en la planeación de auditoría,** que da las claves para la aplicación del estándar y el procedimiento de auditoría de SI **P1: Medición de la evaluación de riesgos de SI** que proporciona ejemplos de procedimientos a seguir.

A través de este estándar podemos observar claramente un enfoque de auditoría que hace uso del análisis de riesgos. El papel principal del análisis de riesgos es servir de base para la selección de las áreas a revisar que tengan una mayor exposición a riesgos, e incluirlas en un plan general de auditoría o en una auditoría puntual.

Con la aplicación de este enfoque es posible identificar los riesgos y vulnerabilidades que le permitirán al auditor determinar que controles son necesarios para mitigar esos riesgos. En este sentido es importante establecer una clara relación entre riesgo y control, y conocer los tipos de riesgos y los controles que se utilizan para mitigarlos, es quizás este un punto clave para el uso de este enfoque de auditoría ya que permitirá al auditor centrarse en aquellas áreas con mayor exposición a riesgos.

Como resultado de la auditoría se obtendrá un informe que mostrará las inconsistencias entre las necesidades identificadas en el análisis de riesgos y la realidad detectada durante la inspección del sistema, área o proceso.

En la actualidad muchas organizaciones utilizan un enfoque de auditoría basada en el análisis de riesgos, como un enfoque de auditoría moderno, que les permite desarrollar y mejorar su proceso de auditoría continua. Es importante puntualizar que en un proceso de auditoría que haga uso de este enfoque, los auditores pueden partir de un análisis de riesgos ya elaborado o realizar ellos mismos este análisis.

El desarrollo de una auditoría bajo este enfoque basado en riesgos puede alinearse con metodologías, estándares y marcos de trabajo, nacionales e internacionales de control interno, auditoría, gestión de riesgos y seguridad informática tales como Magerit, ISO 27005, ISO 27002, COBIT, Esquema Nacional de Seguridad, entre otros, los cuales han sido tratados en capítulos anteriores.

De la anterior exposición podemos concluir que, el principal uso que puede hacerse del análisis de riesgos dentro de una auditoría informática es por un lado la planificación de la auditoría y definir su alcance y por otro, la verificación de los controles implementados frente a los riesgos identificados.

3. Desarrollo de una auditoría con un enfoque en el análisis de riesgos

El desarrollo de una auditoría bajo este enfoque lo podemos englobar en cuatro fases como se muestra en la siguiente figura:

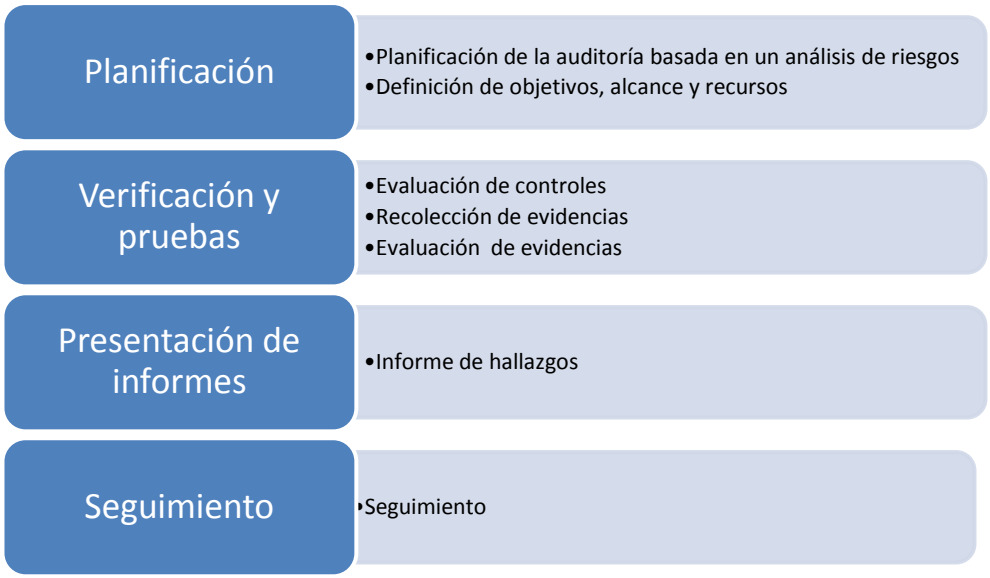


Figura 6.1. Fases de una auditoría

CAPÍTULO VII: Análisis comparativo de estándares, marcos de trabajo y guías y normas de auditoría informática

1. Introducción

En este capítulo realizaremos un análisis comparativo de los diferentes estándares, guía y marcos de trabajo relacionados con la auditoría informática y el control aplicado a los sistemas informáticos, y que han sido expuestos en el capítulo IV.

Debido al carácter complementario de cada uno de estos estándares, guías y marcos de trabajo, abordaremos este análisis desde la perspectiva del aporte que cada uno puede brindar a una auditoría informática y al control de los sistemas informáticos (SI) y no desde el punto de vista de sus diferencias y similitudes, como es el caso de los análisis comparativos de las metodologías y estándares de análisis de riesgos que trataremos en el siguiente capítulo.

Dado que cada uno tiene una naturaleza, objetivo y enfoque diferente, este análisis se realizará agrupándolos según su naturaleza, para lo cual se han dividido en 3 grupos así: **estándares, marcos de trabajo y guías y normas**.

En el primer grupo analizaremos los **estándares.** En este grupo encontramos los estándares emitidos por la ISO - Organización Internacional de Normalización, que han sido seleccionados debido a la relevancia que sus normas tienen a nivel internacional y que recogen el consenso de gran variedad de expertos en la materia, lo que permite a la hora de ser adoptados, contar con normas y recomendaciones de facto.

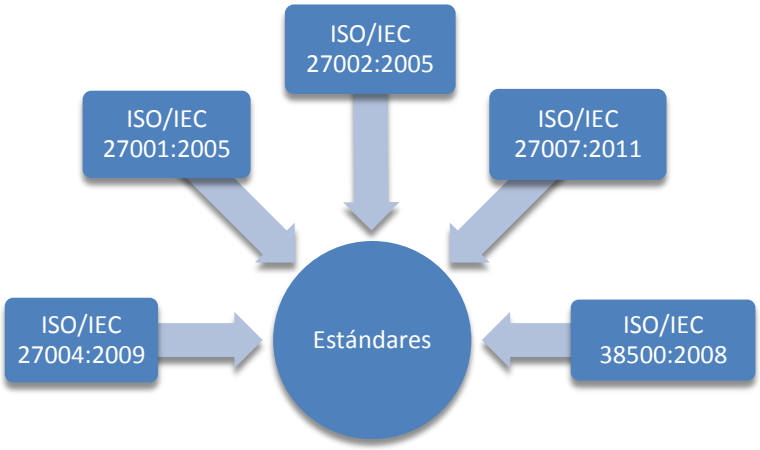


Figura 7.1. Estándares relacionados con la auditoría y el control informático

2. Estándares

En este apartado vamos a tomar como referencia los estándares de la familia ISO 2700 y el estándar ISO/IEC 38500:2008.

En primer lugar, abordaremos algunos estándares de la familia ISO 27000 relacionados directamente con temas de seguridad de la información y que recogen las mejores prácticas recomendadas, además de dar pautas para desarrollar, implementar y mantener un Sistema de Gestión de la Seguridad de la Información (SGSI) y especificar los requerimientos para la implementación de controles de seguridad diseñados de acuerdo a las necesidades específicas de una empresa o una parte de esta.

Dentro de esta familia 27000 podemos destacar los siguientes elementos fundamentales y su estándar asociado, que recogemos en la siguiente figura:

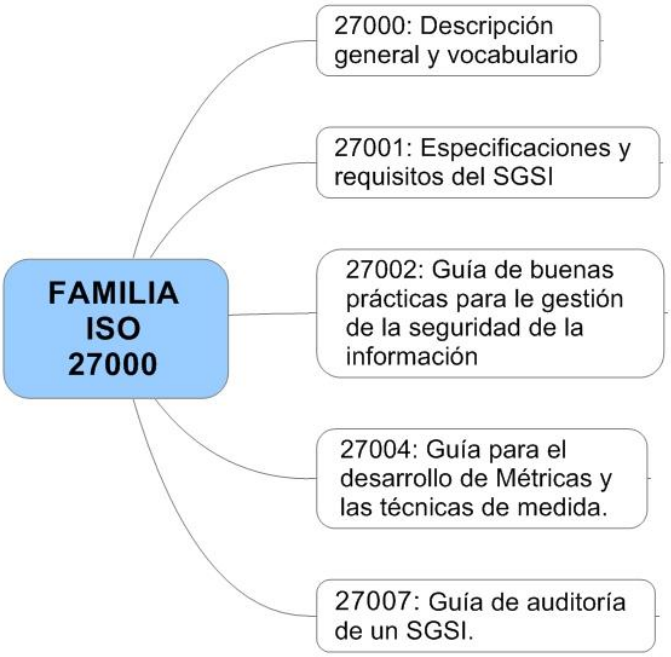


Figura 7.2. Familia ISO 27000

Como se puede apreciar cada estándar tiene un objetivo particular y por tanto una aplicabilidad diferente. En conjunto son complementarios y permiten el desarrollo de un Sistema de Gestión de Seguridad de la Información -SGSI- .

En el caso particular de la auditoría informática, el estándar que tiene mayor relación y del que se podría hacer uso para el desarrollo de la misma es el 27002, ya que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información, que deben ser implementados y que posteriormente servirán de base para realizar una auditoría.

A continuación abordamos dentro de este grupo, el estándar ISO/IEC 38500:2008. Éste está enfocado al gobierno corporativo de Tecnologías de la Información y la Comunicación (TIC) y ofrece un conjunto de buenas prácticas para que la dirección de las organizaciones lo utilice al evaluar, dirigir y monitorizar el uso de las TIC. Así mismo, ayuda a la buena gestión de los procesos y decisiones empresariales relacionadas con los servicios de información y comunicación que son utilizados habitualmente en una organización y, suelen estar gestionados tanto por especialistas en TIC internos o ubicados en otras unidades de negocio de la organización, como por proveedores de servicios externos.

La aplicación de esta norma en una organización permite:

- Llevar un control adecuado de los procesos relacionados con el gobierno de TI,
- Llevar un control de los recursos de TI,
- Proveer las bases para la realización de evaluaciones objetivas de la gestión y uso de la TI y,
- Ofrecer la garantía de cumplir con los requerimientos legales y normativos

3. Marcos de trabajo

En el segundo grupo encontramos los **marcos de trabajo.** Éstos son conjuntos de mejores prácticas recomendadas por consenso de expertos para ser aplicadas en un área en particular. No son estándares ni metodologías.

En este grupo hemos estudiado COBIT e ITIL. El primero como marco de trabajo de control interno para TI, que ofrece una serie de mejores prácticas, las cuales están orientadas al control de la información y tecnología relacionada.

COBIT además se ha convertido en un marco de referencia general para el gobierno de TI en las organizaciones y el segundo conjunto de mejores prácticas y recomendaciones efectivas para la administración de servicios de TI, con un enfoque de procesos.

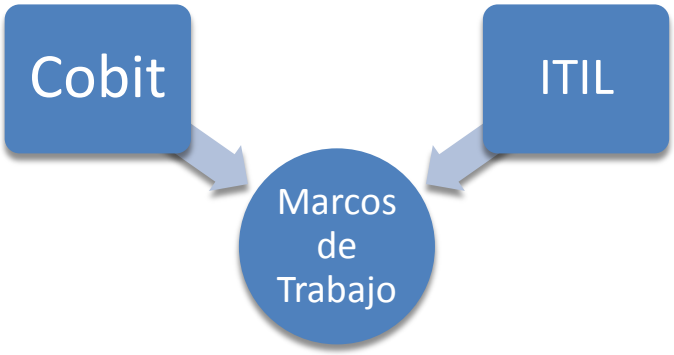


Figura 7.3. Marcos de trabajo relacionados con la auditoría y el control informático

Tanto COBIT como ITIL pueden ser usados como prácticas complementarias dentro de una empresa y alinearse dentro de su gestión de TI. A nivel de auditoría pueden servir como soporte en el proceso de revisión y verificación, siendo COBIT el más orientado hacia la auditoría y el control.

COBIT proporciona un enfoque a los auditores que permite identificar problemas de control de TI dentro de la infraestructura de TI de la empresa. Podemos decir, por tanto, que con COBIT las auditorías serán más eficientes y exitosas.

COBIT es un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores TI, usuarios y por supuesto, los auditores involucrados en el proceso.

La estructura del modelo COBIT propone un marco de actuación donde:

- Se evalúan los criterios de información, como por ejemplo la seguridad y calidad,

- se auditan los recursos que comprenden la tecnología de información, como por ejemplo los recursos humanos, instalaciones, sistemas, y,
- se realiza una evaluación sobre los procesos involucrados en la organización.

COBIT es un modelo de evaluación y monitoreo que se focaliza en el control del negocio y la seguridad TI y que abarca controles específicos de TI desde una perspectiva de negocios.

La adecuada implementación de un modelo COBIT en una organización, proporciona a la misma una herramienta, para evaluar de manera ágil y consistente el cumplimiento de los objetivos de control y controles detallados, que a su vez aseguran que los procesos y recursos de información y tecnología contribuyan al logro de los objetivos del negocio en un mercado cada vez más exigente, complejo y diversificado.

A continuación mencionamos los aportes que hace cada marco de trabajo y como se pueden aplicar y alinear dentro de una empresa, apoyados en lo expuesto en **[ITGI 08]**:

- COBIT está basado en marcos de referencia establecidos, tales como CMM del SEI (Software Engineering Institute), ISO 9000, ITIL e ISO/IEC 27002, sin embargo COBIT no incluye tareas y pasos de procesos porque, aunque está orientado a procesos de TI, es un marco de referencia para gestión y control antes que un marco de referencia para procesos.
- COBIT se focaliza en lo que una empresa necesita hacer, no cómo lo tiene que hacer. La audiencia objetivo es la alta gerencia, los gerentes funcionales, los gerentes de TI y los auditores.
- ITIL proporciona un marco de trabajo de mejores prácticas integral, consistente y coherente para la gestión de servicios de TI y los procesos relacionados, la promoción de un enfoque de alta calidad para el logro de la eficacia y eficiencia del negocio en la gestión de servicios de TI.
- El papel del marco de trabajo de ITIL es describir los enfoques, las funciones, los roles y procesos en los que las organizaciones pueden basar sus propias prácticas.

- COBIT puede ser utilizado en el más alto nivel, ofreciendo un marco general de control basado en un modelo de procesos de TI que debería adaptarse a cada organización.
- Los estándares y las prácticas específicas, tales como ITIL e ISO/IEC 27002 abarcan áreas discretas y pueden ser mapeadas en el marco COBIT, estructurando una jerarquía de materiales de orientación.

Debido a su alto nivel, a la amplia cobertura y porque está basado en muchas prácticas existentes, frecuentemente se hace referencia a COBIT como un 'integrador', que permite ubicar diferentes prácticas bajo un mismo contexto, y ayudando a enlazar estas varias prácticas de TI con los requerimientos del negocio.

En la figura siguiente podemos observar la relación existente entre los diferentes marcos de trabajo y estándares analizados.

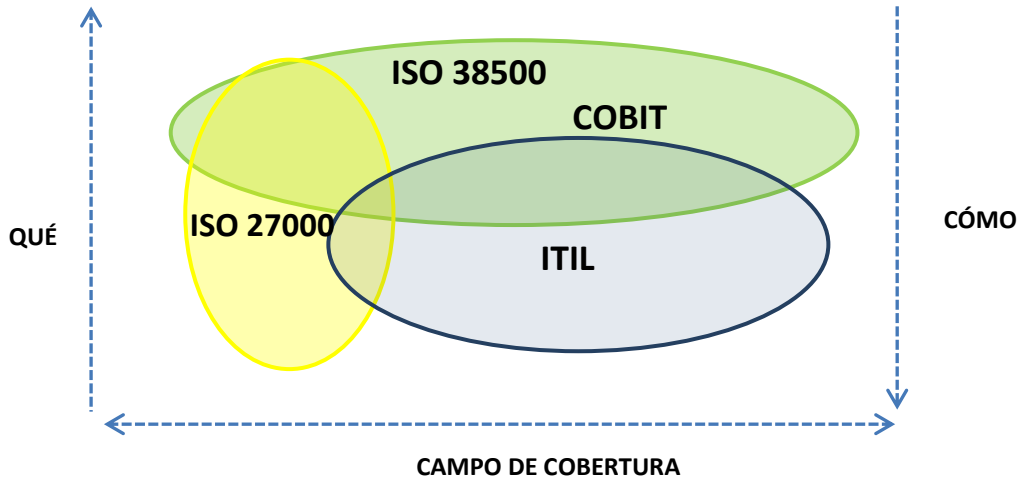


Figura 7.4.Relación entre ITIL, COBIT, ISO 27000, ISO 38500

COBIT, ISO 38500 e ISO/IEC 27002 pueden utilizarse para ayudar a definir **qué** debería hacerse e ITIL muestra el **cómo** para los aspectos de la gestión de servicios.

A continuación presentamos un resumen de las aplicaciones típicas que pueden hacerse con este tipo de estándares y prácticas son las siguientes y que han sido recopiladas con el apoyo del texto contenido en **[ITGI 08]**

- **Apoyar la gobernabilidad a través de:**
  - Proporcionar una política de gestión y un marco de control.
  - Facilitar el proceso de asignación de propietarios, responsabilidades claras y rendición de cuentas para las actividades de TI.
  - Alinear los objetivos de TI con los objetivos del negocio, definiendo prioridades y la asignación de recursos.
  - Asegurar el retorno de la inversión y optimizar los costos.
  - Asegurar la identificación de los riesgos significativos y que sean transparentes para la administración; asignar la responsabilidad en la gestión del riesgo y que se integre en la organización, y asegurar a la dirección que se han implementado controles eficaces.
  - Asegurar que los recursos se han organizado de manera eficiente y que existe suficiente capacidad (infraestructura técnica, procesos y habilidades) para ejecutar la estrategia de TI.
  - Asegurar que las actividades críticas de TI pueden ser monitoreadas y medidas, de modo que los problemas puedan ser identificados y que las medidas correctivas puedan ser adoptadas.
- **Definir los requisitos del servicio y las definiciones del proyecto, tanto internamente como con los proveedores de servicios, por ejemplo:**
  - Estableciendo objetivos claros de TI relacionados con el negocio así como métricas.
  - Definiendo los servicios y proyectos en términos de usuario final.
  - Elaborando acuerdos de niveles de servicio y contratos que pueden ser monitoreados por los clientes.
  - Asegurando que los requisitos del cliente han sido plasmados apropiadamente en requisitos operativos y técnicos de TI.

  - Considerando los portafolios de servicios y de proyectos en conjunto, a fin de establecer las prioridades relativas, de modo que los recursos se asignen de manera equitativa y viable.
- **Verificar la capacidad profesional o demostrar competencia en el mercado a través de:**
  - Las evaluaciones y las auditorías independientes de terceros.
  - Compromisos contractuales.
  - Constancias y certificaciones.
- **Facilitar la mejora continua por:**
  - Evaluaciones de madurez.
  - Análisis de brechas.
  - Benchmarking.
  - Planificación de la mejora.
  - Evitar la reinvención de buenos enfoques ya probados.
- **Como marco para la auditoría, evaluación y una visión externa a través de:**
  - Criterios objetivos y mutuamente entendidos.
  - Benchmarking para justificar las debilidades y brechas en los controles.
  - Incrementando la profundidad y el valor de las recomendaciones mediante enfoques generalmente aceptados.

4. Guías y normas de auditoría

En el tercer grupo, encontramos las **normas y guías de auditoría**, de un lado las publicadas por ISACA y de otro las publicadas por el Instituto de Auditores Internos.

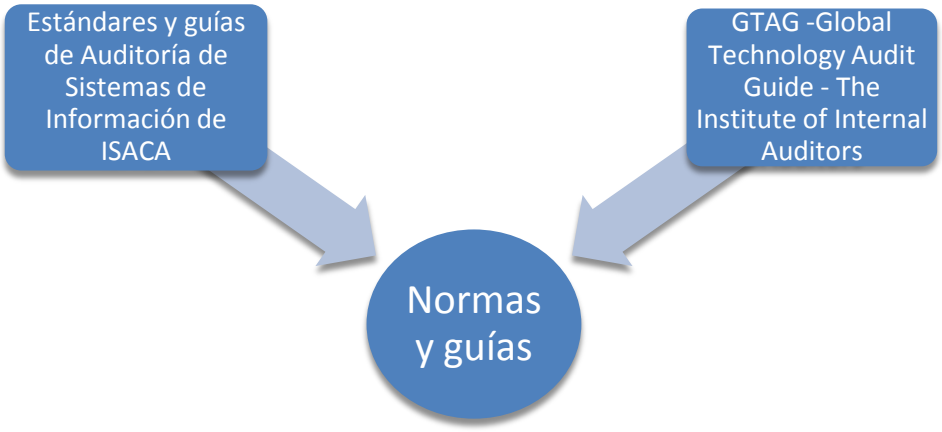


Figura 7.5. Normas y guías de auditoría informática

Ambas tienen como objetivo común servir de guía a los auditores a la hora de abordar una auditoría, ofreciendo información estandarizada y específica para las diferentes áreas relacionadas en una auditoría.

Las normas y guías de ISACA tienen un campo de aplicación amplio y cubren aspectos de orden procedimental (planeación, reporte, actividades de seguimiento, documentación) y aspectos técnicos concretos (por ejemplo, controles de acceso, controles biométricos). Esto lo consiguen a través de tres niveles de "asesoramiento" diferentes: los estándares que definen requisitos obligatorios para la auditoría de SI; las guías o directrices, que proporcionan asesoramiento en la aplicación de los estándares; y los procedimientos que proporcionan ejemplos de procedimientos que podría seguir un auditor de SI.

Las normas y guías de ISACA son reconocidas a nivel mundial y tienen una amplia aceptación en el colectivo de los auditores, por lo cual son de uso recomendado al llevarse a cabo un proceso de auditoría informática en cualquier tipo de organización. Son de acceso público lo cual facilita su uso.

En el caso de las guías GTAG, su principal objetivo es proveer un lenguaje común para la auditoría informática, que no contenga demasiados aspectos técnicos y que pueda ser fácilmente entendido por personal no técnico, cada guía sirve como fuente de recursos para auditores e informáticos en distintos aspectos

relacionados con los riesgos de las tecnologías de la información y las mejores prácticas aplicables, cubren múltiples aspectos del proceso de auditoría desde su planeación y gestión hasta aspectos puntuales como por ejemplo la gestión de la identidad.

Si bien son reconocidas en el mundo de la auditoría, no cuentan con tanta popularidad como las guías de ISACA, el acceso a las guías es solo para miembros lo cual puede dificultar su uso. A continuación se presenta una tabla comparativa donde se pueden observar los aspectos generales de cada estándar, marco o guía.

	COBIT	ITIL	ISO/IEC 27000	ISO/IEC 38500	Normas y guías de Auditoría de Sistemas de Información de ISACA	GTAG -Global Technology Audit Guide - The Institute of Internal Auditors
Objetivo	Marco de trabajo de control interno para TI, que ofrece una serie de mejores prácticas, las cuales están orientadas al control de la información y tecnología relacionada	Guía de las mejores prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información	Marco de referencia de seguridad de la información	Gobierno TI: Proporcionar un marco de principios para que la dirección de las organizaciones lo utilice al evaluar, dirigir y monitorizar el uso de las TIC.	Definir los requisitos obligatorios para la auditoría, proporcionar asesoramiento en la aplicación de los estándares de Auditoría de SI, proporcionar información sobre cómo cumplir con los estándares al realizar trabajos de auditoría de SI	Proporcionar información de alto nivel sobre aspectos tecnológicos que puedan ayudar a los auditores internos y externos a comprender mejor los diferentes riesgos, los controles y los temas del buen gobierno relacionados con aspectos tecnológicos

	COBIT	ITIL	ISO/IEC 27000	ISO/IEC 38500	Normas y guías de Auditoría de Sistemas de Información de ISACA	GTAG -Global Technology Audit Guide - The Institute of Internal Auditors
Áreas	4 dominios y 34 procesos	5 dominios		Define 3 tareas principales: evaluar, dirigir, monitorizar	14 Estándares, 42 guías, 11 procedimientos.	13 guías
Creador	ISACA	OGC - Oficina de comercio gubernamental	ISO	ISO	ISACA	Institute of Internal Auditors- IIA
Para qué se implementa	COBIT brinda las mejores prácticas y herramientas para el monitoreo y la gestión de las actividades de TI. Ayuda a las organizaciones a gestionar los riesgos	ITIL permite la adecuada gestión de servicios de TI, los procesos relacionados, a través de la promoción de un enfoque de alta calidad para el logro de la eficacia y eficiencia del	Desarrollar, implementar y mantener un Sistema de Gestión de la Seguridad de la Información (SGSI) y especificar los	Para llevar un control adecuado de los procesos relacionados con el gobierno de TI, un control de los recursos de TI y da las bases para la realización de	Permiten llevar procesos de auditoría estandarizados, guiados por estándares, guías y procedimientos que aplica específicamente a la auditoría de SI y de aplicabilidad internacional.	Como guía para los auditores internos y externos en distintos aspectos relacionados con la auditoría , el control y los riesgos de las tecnologías de la información y las

	relacionados con TI y a asegurar el cumplimiento, la continuidad, seguridad y privacidad.	negocio en la gestión de servicios de TI. Proporcionar una adecuada gestión de la calidad. Aumentar la eficiencia. Alinear los procesos de negocio y la infraestructura TI. Reducir los riesgos asociados a los Servicios TI. Generar negocio.	requerimientos para la implementación de controles de seguridad	evaluaciones objetivas de la gestión y uso de la TI.		mejores prácticas aplicables

Tabla 7.1. Tabla comparativa estándares, marcos de trabajo y guías de auditoría informática.

CAPÍTULO VIII: Análisis comparativo de estándares y metodologías de análisis de riesgos

1. Introducción

En este apartado realizaremos un análisis comparativo de los diferentes estándares y metodologías de análisis de riesgos que son de uso frecuente y que han sido expuestos en el capítulo V, con el objetivo de tener una visión general de los aportes que hace cada uno de ellos y tener un elemento de decisión para seleccionar una metodología y/o estándar al momento de realizar un análisis de riesgos.

Es importante destacar que hay una diferencia importante a tener en cuenta entre los estándares y las metodologías en general. En el primer caso, los estándares, dan las pautas generales de qué hacer para llevar a cabo un análisis de riesgos y la metodología proporciona los pasos exactos que se deben llevar a cabo para un análisis de riesgos. Es por este motivo, por el que pueden verse como complementarios, es decir, es posible seguir un estándar como guía o marco dentro de un análisis de riesgos y utilizar una metodología en particular para llevar a cabo dicho análisis.

Para realizar este análisis vamos a segmentarlo por grupos de características de tal forma que podamos ver aspectos relevantes de cada estándar o metodología, como sigue a continuación.

2. Análisis de características generales

Metodología/Estándar	Creador	Fecha última versión	País	Ámbito	Acceso
AS/NZS ISO 31000:2009	Organización Internacional para la Estandarización - ISO y el Comité de Normas de Australia /Nueva Zelanda	2009	Australia/Nueva Zelanda	Estándar de carácter genérico para el análisis y la gestión de riesgos.	Restringido / de pago
UNE 71504:2008	Comité técnico AEN/CTN 71 Tecnología de la información, de AENOR - Asociación Española de Normalización y Certificación	2008	España	Metodología de análisis y gestión de riesgos para los sistemas de información	Restringido / de pago
MAGERIT Versión 2.0	Consejo Superior de Administración Electrónica, y publicada por el Ministerio de Hacienda y Administraciones Públicas de España	2006	España	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.	Público

Metodología/Estándar	Creador	Fecha última versión	País	Ámbito	Acceso
OCTAVE Operationally Critical Threat, Asset, and Vulnerability Evaluation	CERT - Coordination Center del Software Engineering Institute de la Universidad Carnegie Mellon	2005	Estados Unidos	Método de análisis de riesgos orientado a activos.	Público
ISO/IEC 27005:2011	Organización Internacional para la Estandarización - ISO	2011		Estándar para la gestión del riesgo de seguridad de la información.	Restringido / de pago
MEHARI - Método Armonizado de Análisis de Riesgos	Comisión de métodos de Clusif (Club de la seguridad de los sistemas de información franceses)	2010	Francia	Método de análisis de riesgo	Público
CRAMM-CTA -Risk Analysis and Management Methodology-	Agencia Central de Cómputo y Telecomunicaciones (CCTA)	2010	Reino Unido	Metodología para el análisis y la gestión de riesgos	Restringido / de pago

Tabla 8.1. Características generales de los estándares y/ metodologías de análisis de riesgos

En este primer cuadro comparativo podemos observar las características generales de cada metodología o estándar. Como se puede apreciar todas las metodologías y estándares analizados cubren el proceso de análisis y gestión de riesgos. Encontramos diferencias en el tipo de acceso que se tiene a la documentación de las metodologías y estándares, lo cual puede ser un factor importante a tener en cuenta al momento de seleccionar una u otra, algunas son de acceso público y otras restringido para miembros de las entidades promotoras o de pago directo.

En general se cuenta con versiones recientes de cada metodología y estándar, los creadores o promotores de estas metodologías y estándares son entidades de reconocimiento en el ámbito local que la desarrolla y a nivel mundial, lo que da un respaldo importante a cada una de ellas.

A continuación presentamos una segunda tabla en la que se comparan los ámbitos de aplicación y procesos metodológicos.

3. Análisis del ámbito de aplicación y procesos metodológicos

Metodología / Estándar	Ámbito de aplicación	Etapas / Fases que se llevan a cabo
AS/NZS ISO 31000:2009	Cualquier organización pública o privada. Estándar de carácter genérico orientado a una amplia gama de actividades, operaciones, procesos, funciones, proyectos, productos, servicios, activos.	1. Establecer el contexto 2. Identificar riesgos 3. Analizar riesgos 4. Evaluar riesgos 5. Tratar riesgos 6. Monitorear y revisar 7. Comunicar y consultar
UNE 71504:2008	Cualquier organización pública o privada, orientación hacia los sistemas informáticos	1. Determinar el contexto 2. Identificar riesgos 3. Analizar riesgos 4. Evaluar riesgos 5. Tratamiento de los riesgos 6. Administración de la gestión del riesgo 7. Comunicación y consulta
MAGERIT Versión 2.0	Uso preferente en la administración pública española, pero puede aplicarse en cualquier tipo de organización. Orientada a los sistemas informáticos	1. Análisis de riesgos 2. Caracterización de los activos a. Caracterización de las amenazas b. Caracterización de las salvaguardas c. Estimación del estado de riesgo 3. Gestionar los riesgos

Metodología / Estándar	Ámbito de aplicación	Etapas / Fases que se llevan a cabo
OCTAVE **Operationally Critical Threat, Asset, and Vulnerability Evaluation**	Cualquier organización pública o privada. Orientada a los sistemas informáticos	**Fase 1- Construir perfiles de amenazas basados en los activos** Proceso 1: Identificar el conocimiento de los altos directivos Proceso 2: Identificar el conocimiento de los directivos de áreas operativas Proceso 3: Identificar el conocimiento del personal operativo Proceso 4: Crear perfiles de amenaza **Fase 2- Identificar vulnerabilidades en la infraestructura** Proceso 5: Identificar componentes claves Proceso 6: Evaluación de componentes seleccionados **Fase 3- Desarrollar estrategias y planes de seguridad** Proceso 7: Realizar un análisis de riesgos Proceso 8: Desarrollar estrategias de protección
ISO/IEC 27005:2011	Cualquier organización pública o privada. Orientada a los sistemas informáticos.	1. Establecimiento del contexto 2. Valoración del riesgo 3. Tratamiento del riesgo 4. Aceptación del riesgo 5. Comunicación del riesgo 6. Monitoreo y Revisión

Metodología / Estándar	Ámbito de aplicación	Etapas / Fases que se llevan a cabo
MEHARI - Método Armonizado de Análisis de Riesgos	Cualquier organización pública o privada Orientada a los sistemas informáticos.	**Fase1: Valoración de riesgos** Identificación de riesgos Estimación de riesgos Evaluación de riesgos **Fase2: Tratamiento del riesgo.** Decidir entre las siguientes alternativas: Retener el riesgo Reducir el riesgo Transferir el riesgo Evitar el riesgo **Fase3: Gestión del riesgo** Desarrollo de planes de acción Implementación de planes de acción Monitoreo
CRAMM-CTA -Risk Analysis and Management Methodology - Metodología para el análisis y la gestión de riesgos	Uso preferente en la administración pública británica, pero puede ser adaptada a cualquier entidad pública o privada. Orientada a los sistemas informáticos.	1. Definir marco de gestión del riesgo 2. Identificar riesgos 3. Identificar propietarios de los riesgos 4. Evaluar riesgos 5. Definir niveles aceptables de riesgo 6. Identificar respuestas adecuadas al riesgo 7. Implantar respuestas 8. Obtener garantías de la efectividad 9. Monitorizar y revisar

Tabla 8.2. Ámbito de aplicación y procesos metodológicos

En este segundo cuadro comparativo se puede observar que cada metodología y/o estándar puede ser aplicado en general en cualquier tipo de organización, ya sea esta pública o privada, en el caso de Magerit y CRAMM han sido concebidas con una orientación primaria hacia las administraciones públicas pero de igual forma pueden adaptarse a otro tipo de organizaciones.

A excepción del estándar **AS/NZS ISO 31000:2009**, las demás están orientadas específicamente a los sistemas informáticos, pese a ello dicha norma al ser de carácter general podría aplicarse en este ámbito particular.

Otra cuestión a tener en cuenta en este punto es que **ISO 27005** y **AS/NZS ISO 31000**, son estándares y no proveen una metodología concreta de análisis de riesgos, dichos estándares describen a través de sus diferentes cláusulas, el proceso recomendado para llevar a cabo un análisis de riesgos y proporcionan un marco general para la gestión de riesgos, pero deben apoyarse en metodologías particulares de análisis y gestión de riesgos.

En cuanto a las etapas o fases generales seguidas por cada una de las metodologías y estándares se observa una similitud generalizada en cuanto al proceso seguido, se aprecia un enfoque estructurado donde se separan claramente las actividades de análisis de riesgos frente a la gestión de riesgos, las diferencias entre una y otra metodología y estándar están marcadas en el desarrollo particular de cada etapa o fase.

4. Análisis de los aspectos propios del proceso de análisis de riesgos

Metodología / Estándar	Tipos de análisis	Caracterización y Valoración de activos	Caracterización y Valoración de amenazas	Caracterización y Valoración de vulnerabilidades	Caracterización y Valoración de Salvaguardas	Estimación de riesgos	Tratamiento de riesgos
AS/NZS ISO 31000:2009	Cualitativo Semi-cuantitativo Cuantitativo	No se define explícitamente un método de identificación y valoración de activos	No se define explícitamente un método de identificación y valoración de amenazas	No se define explícitamente un método de identificación y valoración de vulnerabilidades	No se define explícitamente un método identificación y valoración de salvaguardas	Se sugieren métodos cualitativos y cuantitativos que pueden ser aplicados. No detalla alguna técnica en particular	Estrategias: - Evitar el riesgo - Reducir la probabilidad de la ocurrencia - Reducir las consecuencias - Transferir los riesgos - Retener los riesgos
UNE 71504:2008	Admite métodos de valoración cuantitativa y cualitativa	Sugiere procedimiento de caracterización y valoración de activos, no muy detallado.	Sugiere procedimiento de caracterización de amenazas, no indica un método en particular, no muy detallado	Se describe como una actividad dentro del proceso, no se detalla.	Describe las actividades necesarias para la caracterización y valoración de salvaguardas	Sugiere criterios a tener en cuenta, no se menciona un método particular	Estrategias: - Riesgos no aceptables: se aplicará tratamiento adecuado - Riesgos aceptables: sistema de monitorización que garantice ese nivel

Metodología / Estándar	Tipos de análisis	Caracterización y Valoración de activos	Caracterización y Valoración de amenazas	Caracterización y Valoración de vulnerabilidades	Caracterización y Valoración de Salvaguardas	Estimación de riesgos	Tratamiento de riesgos
MAGERIT Versión 2.0	Análisis cuantitativos y cualitativos	Detalla la forma de caracterizar activos y hacer su valoración, provee ejemplos y sugiere técnicas	Detalla la forma de caracterizar amenazas y hacer su valoración, provee ejemplos y sugiera técnicas	No se considera explícitamente	Detalla la forma de caracterizar salvaguardas y hacer su valoración, provee ejemplos y sugiere técnicas	Detalla la forma de estimar el impacto del riesgo, estimar el riesgo e interpretar los resultados, provee ejemplos y sugiere técnicas	Provee un proceso detallado para la gestión de riesgos
OCTAVE	Análisis cuantitativos y cualitativos.	Detalla la forma de caracterizar activos, provee guías y ejemplos	Detalla la forma de caracterizar amenazas, provee guías y ejemplos	Detalla la forma de caracterizar vulnerabilidades, provee guías y ejemplos	No se considera explícitamente	Se identifican los riesgos y se evalúa el impacto en términos de una escala predefinida (alto, medio, bajo)	Se basa en el desarrollo de: -Estrategias de protección - Planes de mitigación y lista de acciones.

Metodología/ Estándar	Tipos de análisis	Caracterización y Valoración de activos	Caracterización y Valoración de amenazas	Caracterización y Valoración de vulnerabilidades	Caracterización y Valoración de Salvaguardas	Estimación de riesgos	Tratamiento de riesgos
ISO/IEC 27005:2011	Análisis cuantitativos y cualitativos preferentemente	Detalla la forma de identificar activos y hacer su valoración, provee ejemplos.	Presenta ejemplos de amenazas típicas, no detalla la forma de valorarlos.	Presenta ejemplos de vulnerabilidades y describe formas de valoración	No se considera explícitamente	Describe procedimiento para realizar estimación del riesgo.	Sugiere alguna de estas estrategias: -Retención del riesgo -Evitación del riesgo -Transferencia del riesgo
MEHARI	Análisis cualitativos y cuantitativos	Describe procedimientos para la Identificación de activos	Describe procedimientos para la Identificación de amenazas	Describe procedimientos para la Identificación de activos	No se considera explícitamente	Describe procedimientos para la estimación del riesgo	-Retención del riesgo -Reducción del riesgo -Evitación del riesgo -Transferencia del riesgo
CRAMM-CTA	Análisis cuantitativos o cualitativos	Describe procedimientos para la Identificación y valoración de activos	Describe procedimientos para la evaluación de amenazas	Describe procedimientos para la evaluación de vulnerabilidades	No se considera explícitamente	Describe el procedimiento para la estimación del riesgo	No se considera explícitamente

Tabla 8.3. Aspectos propios del proceso de análisis de riesgos

En este tercer cuadro comparativo se analizan aspectos puntuales de cada metodología y/o estándar que son fundamentales a la hora de realizar un análisis de riesgos, y que hacen parte del modelo o proceso de análisis de riesgos utilizado por cada una de ellas.

La principal particularidad que podemos encontrar en este punto, es como cada estándar y/o metodología aborda el desarrollo de cada uno de los aspectos tratados, algunas con mayor o menor detalle. En general se observa que estándares como **ISO/IEC 27005:2011** y **AS/NZS ISO 31000:2009** no detallan o sugieren técnicas particulares para el desarrollo de cada una de las tareas, sino que indican la forma en que se debería llevar a cabo el proceso de análisis de riesgos y que aspectos deben considerarse. Estos estándares podrían apoyarse en metodologías concretas que provean métodos detallados de análisis de riesgos.

En el caso de las metodologías analizadas se puede observar que metodologías como **MAGERIT** y **OCTAVE** son bastante detalladas en sus fases de desarrollo y proveen herramientas adicionales para apoyar el trabajo del análisis de riesgos, como son guías, ejemplos, métodos de caracterización y valoración, catálogos de elementos y herramientas software.

OCTAVE desarrolla el análisis de riesgos partiendo de la perspectiva de los integrantes de la organización quienes están involucrados permanentemente en dicho proceso y aportan una visión desde el punto de vista organizacional y tecnológico, lo que permite forjar una visión en todos los niveles de la organización de los riesgos de seguridad de la información, siendo este enfoque una de las principales diferencias frente a otras metodologías.

Tras desarrollar el análisis de riesgos la metodología permite desarrollar estrategias de protección frente al riesgo y planes de seguridad.

OCTAVE cuenta con versiones diferentes que pueden ser adaptadas a las organizaciones dependiendo de su tamaño. Otra ventaja importante de esta metodología es que es de acceso público lo que facilita la disponibilidad de los documentos y herramientas de apoyo. Es una metodología de reconocimiento internacional y se encuentra incluida en el “Inventory of Risk Management / Risk

Assessment Methods“ de ENISA (*European Network and Information Security Agency*), solo se encuentra disponible en inglés.

Por su parte **MAGERIT** se presenta como una muy buena opción a la hora de seleccionar una metodología de análisis de riesgos, que además de que cubre el proceso de gestión de riesgos, provee fases muy detalladas para el proceso de análisis de riesgos, indicando métodos particulares para la caracterización y valoración de activos, amenazas y salvaguardas, así como para la estimación de los riesgos tanto potenciales como residuales.

Lo anterior es posible ya que adicionalmente al documento base donde se detalla la metodología se cuenta con dos documentos adicionales que proveen de un lado una guía de consulta que sugiere algunas técnicas que se emplean habitualmente para llevar a cabo proyectos de análisis y gestión de riesgos - 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, diagramas de procesos, técnicas gráficas, planificación de proyectos, sesiones de trabajo (entrevistas, reuniones y presentaciones) y valoración Delphi, tal como se indica en **[MAGE 06] -** y de otro lado se cuenta con un catálogo de elementos que ofrece unas pautas y elementos estándar en cuanto a: tipos de activos, dimensiones de valoración de los activos, criterios de valoración de los activos, amenazas típicas sobre los sistemas de información y salvaguardas a considerar para proteger sistemas de información, tal como se indica en **[MAGE 06].**

MAGERIT está alineada con la normativa vigente de carácter nacional relacionada con las Tecnologías de la Información y Comunicación, como son entre otras La Ley de Protección de Datos de Carácter Personal, Firma Electrónica y procedimientos administrativos específicos, entre otros. De igual forma se constituye en un instrumento que ayuda a la implantación y aplicación del Esquema Nacional de Seguridad.

MAGERIT cuenta con el reconocimiento de ENISA (European Network and Information Security Agency) que la ha incluido desde el año 2009 en su “Inventory of Risk Management/Risk Assessment Methods“, lo que le aporta

reconocimiento internacional y cumple con estándares internacionales como ISO/IEC 27001, ISO/IEC 15408, ISO/IEC 27002, e ISO/IEC 27005.

MAGERIT cuenta con una herramienta software de apoyo llamada EAR/PILAR, los documentos de la metodología están disponibles en inglés y español y son de libre acceso, sin embargo la herramienta software no es de uso público.

En el ámbito nacional encontramos otra metodología que puede ser considerada incluso como un estándar y es la **UNE 71504:2008** que ofrece las directrices para llevar a cabo un análisis de riesgos. Esta metodología, si bien no es tan detallada como **OCTAVE o MAGERIT** ni ofrece métodos particulares de caracterización y valoración de los diferentes elementos de su modelo, ofrece pautas para la caracterización y valoración de activos, amenazas, vulnerabilidades y salvaguardas, y establece pautas para la estimación del riesgo potencial y residual.

Esta metodología separa dentro de su proceso general el análisis, la evaluación y el tratamiento de los riesgos, hace uso del modelo **ALARP** para la evaluación de riesgos que agrupa los riesgos para su evaluación en tres zonas: zona de riesgos inaceptables, zona de riesgos intermedia y zona de riesgos tolerables.

Está disponible en español y no es de acceso público, está alineada con **MAGERIT** y no se encuentra aún incluida en el "Inventory of Risk Management / Risk Assessment Methods" de ENISA.

En cuanto a **MEHARI** su principal característica es que está totalmente enfocada a responder a las pautas dadas por la ISO/IEC 27005 para el análisis y la gestión de riesgos. Cuenta con documentos de apoyo que guían el desarrollo de dichos procesos y aunque sin proponer métodos concretos ofrecen una buena guía metodológica.

Un aspecto importante a destacar de **MEHARI** es que cuenta con una base de datos de conocimiento en formato de hoja de cálculo, que puede ser descargada y que facilita el desarrollo de las diferentes fases de la metodología.

Los documentos de la metodología y la base de datos son de libre acceso, está disponibles por completo en francés e inglés y algunos documentos introductorios en español, italiano, alemán, portugués y chino, entre otros.

Se encuentra incluida en el "Inventory of Risk Management/Risk Assessment Methods" de ENISA.

En lo que respecta a **CRAMM**, en esencia es la base de una herramienta software que guía todo el proceso de análisis y gestión de riesgos, que goza de gran prestigio en el Reino Unido, cumple con el estándar ISO 27002 y no es de acceso público por lo cual no se cuenta con muchos detalles de la misma. Se encuentra incluida en el "Inventory of Risk Management/Risk Assessment Methods" de ENISA, está disponible en inglés, alemán, holandés y checo.

Capítulo IX: Propuesta de una guía para llevar a cabo una auditoría informática

1. Introducción

En este apartado se presenta la propuesta de una guía de auditoría informática que hace uso del análisis de riesgos como parte de la planificación de dicha auditoría, de tal forma que permita definir el alcance de la misma y ayude a priorizar el o las áreas a auditar.

El objetivo de la guía es servir como referencia y ayuda al desarrollo de una auditoría informática en empresas pequeñas y medianas en el ámbito nacional que, con independencia de su sector de actividad hagan uso de tecnologías informáticas.

La guía estará apoyada en estándares, guías y metodologías de reconocimiento en el sector y que han sido seleccionadas por su pertinencia, de acuerdo al análisis realizado en apartados anteriores.

Para el caso del análisis de riesgos se usará Magerit y para la evaluación de controles se usará COBIT, también se seguirán las recomendaciones de las normas y guías de auditoría de sistemas de información de ISACA.

En primera instancia se presenta el contenido o estructura de la guía y posteriormente se irá desarrollando cada punto de manera detallada.

Como complemento al documento que se presenta a continuación, se ha elaborado una web con todo el contenido de la guía para que pueda ser consultada de una manera ágil y que se incluye como anexo a la memoria del proyecto.

2. Contenido de la guía

La guía se estructura según el esquema que se indica a continuación:

1. Introducción
2. Alcance y ámbito de aplicación
3. Objetivos
4. Términos y definiciones
5. Estándares y metodologías relacionados
6. Proceso de realización de la auditoría

7. Fase de planificación
   7.1. Etapa 1: Conocimiento preliminar de la empresa y/ o área a auditar
   7.2. Etapa 2: Desarrollo del análisis de riesgos, siguiendo la metodología Magerit V2.0
   7.3. Informe final del análisis de riesgos
   7.4. Informe de planificación de la auditoría
   7.5. Fase de evaluación de controles
      7.5.1. Etapa 1: Identificación y selección de controles a evaluar
      7.5.2. Etapa 2: Recolección y evaluación de evidencias
   7.6. Fase de elaboración y presentación de informes
      7.6.1. Informe de hallazgos y recomendaciones
      7.6.2. Documentación final de la auditoría
   7.7. Fase de seguimiento
      7.7.1. Establecimiento de pautas para el seguimiento de la auditoría
   7.8. Anexos de la guía

2.1. Introducción

Dado el creciente uso de las Tecnologías de la Información y la Comunicación en todas las empresas, con independencia de su tamaño y sector, se hace necesario contar con estrategias encaminadas a asegurar sus recursos informáticos, entendidos estos como recursos lógicos: -software- y recursos físicos: equipos, soportes de almacenamiento de información, medios de comunicación, hardware en general e instalaciones y recursos humanos que hacen uso de dichos recursos, los operan y administran.

Dichos recursos soportan la operación cotidiana de las empresas y en su conjunto constituyen los sistemas informáticos a través de los cuales se procesa, almacena y transmite información. Es importante indicar que puede existir información que no esté automatizada, que sea necesario asegurar y para la cual se pueden considerar algunos procedimientos de control.

De acuerdo con lo anterior es necesario contar con procedimientos que permitan revisar y evaluar el funcionamiento de dichos sistemas informáticos y establecer controles, de tal forma que se garantice su operación de forma segura y eficiente y que además, permita cumplir con la normativa vigente.

Con el fin de ayudar a cumplir con lo anterior se presenta esta guía de auditoría, que pretende servir de orientación en el desarrollo de una auditoría informática con un enfoque de riesgos.

2.2. Alcance y ámbito de aplicación

Esta guía de auditoría está orientada a las PYMES de cualquier sector, que hagan uso de las Tecnologías de la Información y Comunicación y, que apoyen o soporten su operación y procesos en sistemas informáticos. La guía se apoya en estándares y normativas tanto de ámbito local como internacional, por lo que puede ser aplicada en cualquier contexto que reúna los requerimientos particulares.

2.3. Objetivos

- Proporcionar una guía de auditoría que facilite el desarrollo de un proceso de verificación y evaluación de los sistemas informáticos dentro de una empresa.
- Proporcionar un enfoque de auditoría basado en análisis de riesgos que haga de la auditoría y el control un proceso dinámico y constante dentro de una empresa.
- Apoyar el cumplimiento de la normativa vigente relacionada con las Tecnologías de la Información y Comunicación, el tratamiento de la información y demás normativa relacionada.

2.4. Términos y definiciones

Activo: Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberadamente con consecuencias para la Organización. Incluye datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y personal. (UNE 71504-008).

Amenaza: Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos. (Magerit).

Análisis de riesgos: Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización. (Magerit).

Auditoría Informática: La auditoría de los sistemas de información se define como cualquier auditoría que abarca la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes.(ISACA).

Conjunto de procedimientos y técnicas para evaluar y controlar un sistema informático o de información, con el fin de constatar si sus actividades son las adecuadas en relación con las normativas generales de aplicación y los objetivos prefijados por la organización. [CARI 06].

Auditoría de seguridad: Estudio y examen independiente del historial y actividades de un sistema de información, con la finalidad de comprobar la idoneidad de los controles del sistema, asegurar su conformidad con la estructura de seguridad y procedimientos operativos establecidos, a fin de detectar brechas en la seguridad y recomendar cambios en los procedimientos, controles y estructuras de seguridad. (Magerit).

Alcance de la Auditoría: Marco o límite de una auditoría en el que se determina el tiempo que se va a emplear, las materias o áreas que se van a cubrir, la profundidad de las pruebas a realizar, los objetivos y la metodología aplicable. [CONT 10].

Control: Las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para proporcionar una garantía razonable de que los objetivos del negocio se alcanzarán y los eventos no deseados serán prevenidos o detectados. (COBIT).

Evidencia: Prueba determinante en un proceso. (RAE).

Prueba obtenida por cualquiera de los diversos procedimientos empleados por el auditor en el curso de una auditoría. La evidencia es competente, cuando es válida y confiable; es relevante cuando guarda una relación lógica y patente con el hecho a demostrar o refutar; y es suficiente cuando es objetiva y convincente y sirve para sustentar los hallazgos, conclusiones y recomendaciones del auditor. **[CONT 10]**.

Gestión de riesgos: Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.

Selección e implantación de las medidas o 'salvaguardas' de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

La gestión de riesgos se basa en los resultados obtenidos en el análisis de los riesgos. (Magerit).

Hallazgo: Toda situación irregular encontrada durante el proceso de una auditoría. En su descripción se debe incluir información necesaria para que el lector pueda entender y juzgar el hallazgo sin explicación adicional.

Hechos o situaciones irregulares que impactan significativamente el desempeño de la organización,**[CONT 10]**.

Identificación de riesgos: Proceso de determinación de qué le puede ocurrir a cada activo y cuáles serían las consecuencias. (UNE 71504-008).

Impacto: Consecuencia que sobre un activo tiene la materialización de una amenaza. (Magerit).

Mapa de riesgos Informe: Relación de las amenazas a que están expuestos los activos. (Magerit).

Objetivo de control: Una declaración del resultado o propósito que se desea alcanzar al implementar procedimientos de control en un proceso en particular. (COBIT).

Programa de Auditoría: Es un plan detallado de la auditoría donde se define el cómo, dónde y el porqué, dividiéndose cada uno de ellos en procedimientos. Esquema detallado del trabajo por realizar y los procedimientos a emplear durante la Fase de Ejecución, determinando la extensión y la oportunidad con que serán aplicados, así como los papeles de trabajo que han de ser elaborados. **[CONT 10].**

Procedimientos de Auditoría: Comprobaciones, instrucciones y detalles incluidos en el programa de auditoría, que se deben llevar a cabo en forma sistemática y razonable.

Pasos específicos que desarrollará el auditor para examinar la gestión, detectar hallazgos y recopilar la evidencia necesaria**. [CONT 10].**

Riesgo: El potencial de que una amenaza específica explote las debilidades de un activo o grupo de activos para ocasionar pérdida y/o daño a los activos. Por lo general se mide por medio de una combinación del impacto y la probabilidad de ocurrencia. (COBIT).

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización. (Magerit).

Salvaguarda: Procedimiento o mecanismo tecnológico que reduce el riesgo. (Magerit).

Sistema de Información / Informático: Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar (tratar), mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

Vulnerabilidad: Estimación de la exposición efectiva de un activo a una amenaza. Se determina por dos medidas: frecuencia de ocurrencia y degradación causada.

Debilidad en la seguridad de un sistema de información. (Magerit).

2.5. Estándares y metodologías relacionados

A continuación se incluye un catálogo de los estándares y metodologías relacionados con el desarrollo de esta guía.

ISO 27001. Es la norma principal de la serie 27000 y contiene los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI). Tiene su origen en la BS 7799-2:2002 y es la norma con la cual se certifican, por auditores externos, los SGSI de las organizaciones.

ISO 27002. Es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

Magerit V2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, desarrollada por el Consejo Superior de Administración Electrónica, y publicada por el Ministerio de Hacienda y Administraciones Públicas de España.

COBIT. Objetivos de Control para la Información y la Tecnología relacionada, es un marco de trabajo de control interno para TI (Tecnologías de la Información), que ofrece una serie de mejores prácticas, las cuales están orientadas al control de la información y tecnología relacionada y que se ha convertido en un marco de referencia general para el gobierno de TI en las organizaciones.

Guías de Auditoría de ISACA: Conjunto de normas de auditoría que guían y apoyan el trabajo del auditor, publicadas por ISACA, cuyos objetivos son los de informar a los auditores del nivel mínimo de rendimiento aceptable para satisfacer las responsabilidades profesionales establecidas en el Código de Ética Profesional y de informar a la gerencia y a otras partes interesadas de las expectativas de la profesión con respecto al trabajo de aquellos que la ejercen.

2.6. Proceso de realización de la auditoría

El proceso de realización de la auditoría sigue el esquema que se muestra en la imagen a continuación:

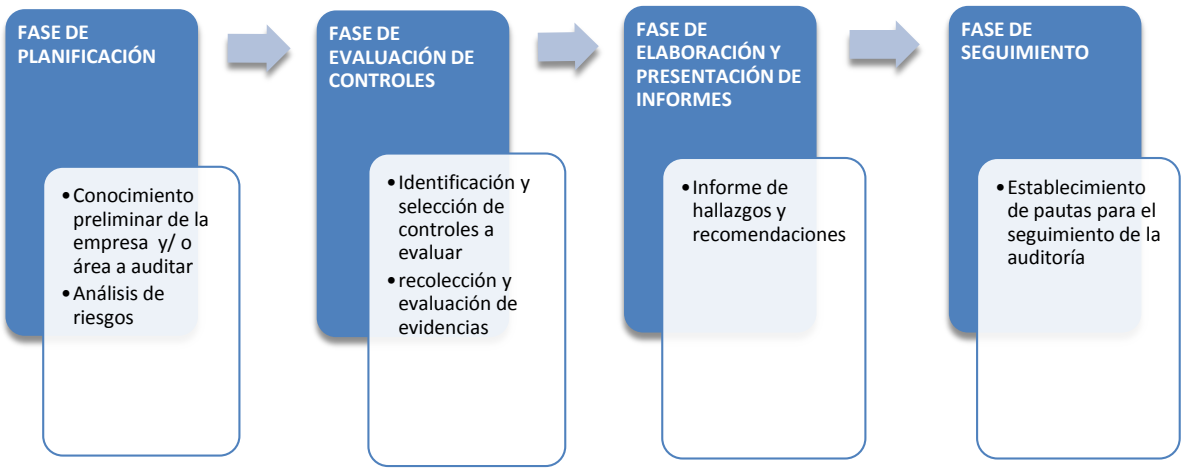


Figura 9.1: Fases de la auditoría

2.6.1. Fase de planificación

En esta fase se llevará a cabo la definición de los objetivos de la auditoría y el alcance de la misma, basada en un análisis de riesgos.

Objetivos

Los objetivos de esta fase son determinar las áreas o procesos a ser auditados, definir el universo de la auditoría, identificar las áreas prioritarias y ayudar en la asignación de recursos necesarios para la ejecución de la auditoría.

Alcance

Esta fase comprende la realización de dos etapas principales: un análisis para el conocimiento preliminar de la empresa y la realización del análisis de riesgos.

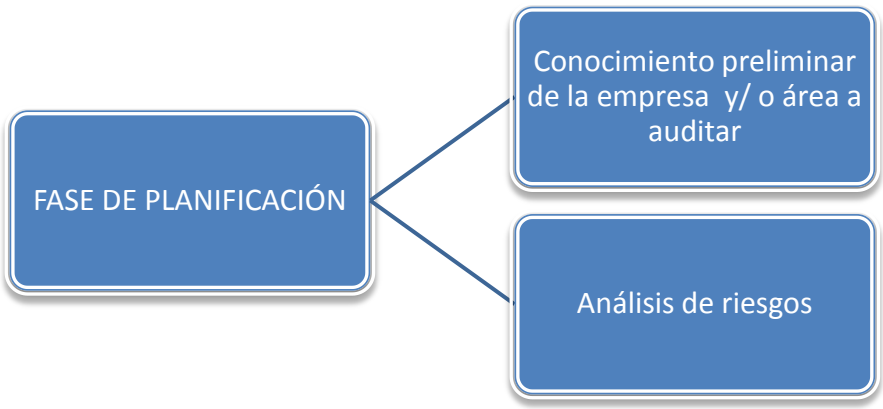


Figura 9.2: Etapas de la fase de planificación

2.6.1.1. Etapa 1: Conocimiento preliminar de la empresa y/o área a auditar

Para el desarrollo de esta actividad se debe realizar un análisis detallado de la empresa y/o área a auditar. Para ello se deben analizar diferentes fuentes de información y emplear diferentes mecanismos para la obtención de la información necesaria.

Para esta actividad se debe disponer de:

- Conocimiento del negocio y la industria en la que opera
- Conocimiento de la arquitectura tecnológica

- Normas regulatorias
- Evaluaciones de riesgos previas
- Informes de auditorías previos
- Información financiera reciente

Como mecanismos para realizar esta investigación preliminar se pueden usar los siguientes:

- Entrevistas con los actores involucrados en las áreas y procesos a auditar y los involucrados en el proyecto de auditoría.
- Revisión de documentación proporcionada por la empresa
- Inspección de las instalaciones donde se llevará a cabo la auditoría y observación de operaciones.
- Revisión de informes de auditoría anteriores si se han realizado.
- Estudio y evaluación del sistema de control interno.

Una vez finalizada esta actividad se tendrá un conocimiento global de la empresa y / o del área a auditar.

El auditor puede documentar esta actividad, realizando un registro de los aspectos más relevantes encontrados durante esta investigación preliminar, para este registro no se plantea un formato particular sino que será a criterio del auditor.

2.6.1.2. Etapa 2: Desarrollo del análisis de riesgos

El objetivo de esta actividad es realizar un análisis de riesgos basado en la metodología Magerit. Si existe un análisis de riesgos previo se hará uso de éste, de lo contrario se procederá a la realización de dicho análisis como parte de la fase de planificación de la auditoría.

Para el desarrollo de estas actividades se hará uso de los documentos oficiales de la metodología, tomando de ellos los aspectos relevantes de cada actividad. En todo momento se conservarán los planteamientos de la metodología, no obstante se ajustarán aquellos aspectos que se consideren necesarios al contexto de la guía. Los documentos a utilizar son los siguientes:

- Magerit - El Método
- Magerit - Catálogo de Elementos
- Magerit - Guía de Técnicas

Se desarrollarán tres actividades centrales cuyo resultado final será un mapa de riesgos de la empresa, que será utilizado para definir los objetivos y el alcance de la auditoría.

Las tres actividades a desempeñar son las siguientes:

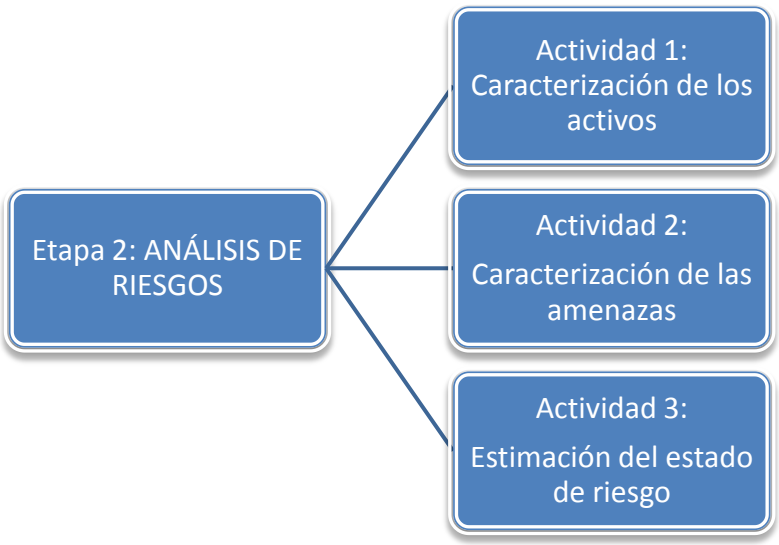


Figura 9.3: Actividades de la etapa de Análisis de Riesgos

Como apoyo al desarrollo de cada una de estas actividades es posible usar la herramienta PILAR, que ha sido desarrollada para brindar un soporte automatizado en el proceso del análisis de riesgos. Por otra parte como alternativa al uso de dicha herramienta, se propone a lo largo de la guía el uso de una serie de plantillas que facilitarán la realización de este análisis. El uso de una u otra alternativa dependerá del criterio de quienes ejecuten las diferentes actividades.

Actividad 1: Caracterización de los activos

El objetivo de esta actividad es reconocer los activos que componen los procesos y definir las dependencias entre ellos. Así y a partir de la información recopilada en la etapa anterior, esta actividad profundiza en el estudio de los activos con vistas a obtener la información necesaria para realizar las estimaciones de riesgo. Para el desarrollo de esta actividad se deben llevar a cabo las siguientes tareas:

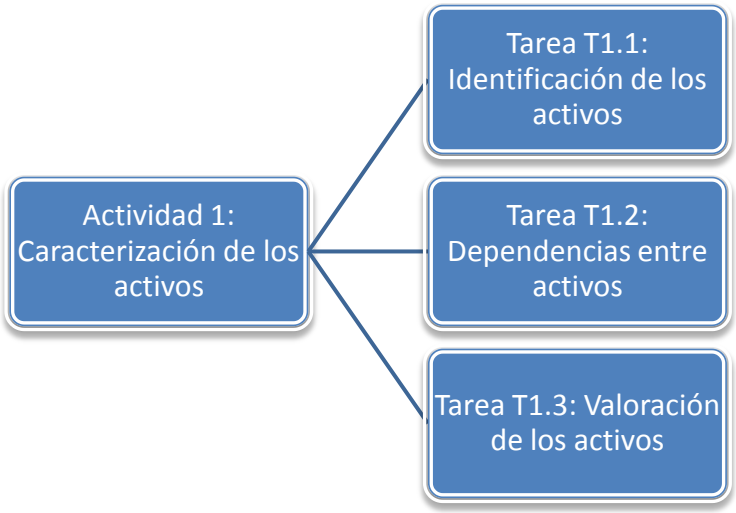


Figura 9.4: Tareas de la actividad Caracterización de los activos

Tarea T1.1: Identificación de los activos

Objetivos: El objetivo de esta tarea es identificar los activos que componen el dominio del análisis, determinando sus características, atributos y clasificación en los tipos determinados.

Productos de entrada: como información de entrada para el adecuado desarrollo de esta la tarea se puede utilizar la siguiente:

- Inventarios de datos manejados por la Organización
- Procesos de negocio
- Diagramas de uso
- Diagramas de flujo de datos

- Inventarios de equipamiento lógico
- Inventarios de equipamiento físico
- Caracterización funcional de los puestos de trabajo
- Locales y sedes de la Organización

Productos de salida: Una vez finalizada esta tarea se obtendrán los siguientes productos de salida:

- Relación de activos a considerar
- Caracterización de los activos

Técnicas, prácticas y pautas: Para la ejecución de esta actividad se recomienda una serie de técnicas y pautas que facilitaran el desarrollo de la tarea y que son sugeridas por la metodología Magerit. Dichas técnicas se encuentran en los documentos que provee la metodología:

- Diagramas de flujo de datos (ver "Guía de Técnicas" 3.2)
- Diagramas de procesos (ver "Guía de Técnicas" 3.3)
- Entrevistas (ver "Guía de Técnicas" 3.6.1)
- Reuniones (ver "Guía de Técnicas" 3.6.2)
- Ver también la sección 2.1.1 del documento “El Método”.

Para la identificación de los activos es necesario determinar una serie de características que lo definen y que se sugieren a continuación:

- Código, típicamente procedente del inventario.
- Nombre (corto).
- Descripción (larga).
- Tipo (o tipos) que caracterizan el activo.
- Unidad responsable. A veces hay más de una unidad. Por ejemplo, en el caso de aplicaciones cabe diferenciar entre la unidad que la mantiene y la que la explota.
- Persona responsable. Especialmente relevante en el caso de datos. A veces hay más de un responsable. Por ejemplo en caso de datos de

carácter personal cabe diferenciar entre el responsable del dato y el operador u operadores que lo manejan.

- Ubicación. Técnica (en activos intangibles) o geográfica (en activos materiales).
- Cantidad, si procede como puede ser en el caso de la informática personal (por ejemplo, 350 equipos de sobremesa).
- Otras características específicas del tipo de activo.

Para el registro de estas características se sugiere el uso de una plantilla que forma parte de los anexos de este documento. [Anexo 1].

Tarea T1.2: Dependencias entre activos

Objetivos: Identificar y valorar las dependencias entre activos, es decir, la medida en que un activo de orden superior se puede ver perjudicado por una amenaza materializada sobre un activo de orden inferior.

Productos de entrada: Como información de entrada para el adecuado desarrollo de esta tarea se puede utilizar la siguiente:

- Resultados de la tarea T1.1, Identificación de activos
- Procesos de negocio
- Diagramas de flujo de datos
- Diagramas de uso

Productos de salida: Una vez finalizada esta tarea se obtendrán los siguientes productos de salida:

- Diagrama de dependencias entre activos

Técnicas, prácticas y pautas: Para la ejecución de esta actividad se recomienda una serie de técnicas y pautas que facilitarán el desarrollo de la tarea y que son sugeridas por la metodología Magerit. Dichas técnicas se encuentran en los documentos que provee la metodología:

- Diagramas de flujo de datos (ver "Guía de Técnicas" 3.2)
- Diagramas de procesos (ver "Guía de Técnicas" 3.3)

- Entrevistas (ver "Guía de Técnicas" 3.6.1)
- Reuniones (ver "Guía de Técnicas" 3.6.2)
- Valoración Delphi (ver "Guía de Técnicas" 3.7)
- Ver también la sección 2.1.1 del documento “El Método”.

Para cada dependencia se sugiere registrar la siguiente información:

- Estimación del grado de dependencia: hasta un 100%
- Explicación de la valoración de la dependencia
- Entrevistas realizadas de las que se ha deducido la anterior estimación

Para la realización de esta actividad se puede usar como apoyo una matriz de dependencias donde se crucen los activos padres y sus activos hijos o dependientes. Dichas dependencias se pueden evaluar en función de la dependencia de un activo dentro de las dimensiones de valoración de los activos definidas en la metodología y que se listan a continuación:

[D] disponibilidad

[I] integridad de los datos

[C] confidencialidad de los datos

[A_S] autenticidad de los usuarios del servicio

[A_D] autenticidad del origen de los datos

[T_S] trazabilidad del servicio

[T_D] trazabilidad de los datos

Para el desarrollo de esta tarea se sugiere el uso de una plantilla que forma parte de los anexos de este documento. [Anexo 2]. De igual forma puede hacerse uso de la herramienta PILAR.

Esta información de dependencias también se puede visualizar de forma gráfica a través de la construcción de un gráfico de dependencias entre activos. Este gráfico se puede construir de forma manual basándose en la matriz de dependencias construida o de forma automática a través de la herramienta PILAR.

Tarea T1.3: Valoración de los activos

Objetivos: Los objetivos de esta tarea son los siguientes:

- Identificar en qué dimensión es valioso el activo
- Valorar el coste que para la Organización supondría la imposibilidad del uso del activo

Productos de entrada: Como información de entrada para el adecuado desarrollo de esta tarea se puede utilizar lo siguiente:

- Resultados de la tarea T 1.1, Identificación de los activos
- Resultados de la tarea T 1.2, Dependencias entre activos

Productos de salida: Una vez finalizada esta tarea se obtendrán los siguientes productos de salida:

- Modelo de valor: informe de valor de los activos

Técnicas, prácticas y pautas: Para la ejecución de esta actividad se recomienda una serie de técnicas y pautas que facilitaran el desarrollo de la tarea y que son sugeridas por la metodología Magerit. Dichas técnicas se encuentran en los documentos que provee la metodología:

- Entrevistas (ver "Guía de Técnicas" 3.6.1)
- Reuniones (ver "Guía de Técnicas" 3.6.2)
- Valoración Delphi (ver "Guía de Técnicas" 3.7)
- Ver también la sección 2.1.1, del documento “El Método”.

Para el desarrollo de esta tarea y la adquisición del conocimiento requerido, puede ser necesario entrevistar a diferentes colectivos dentro de la Organización:

- Dirección o gerencia, que conocen las consecuencias para la misión de la organización
- Responsables de los servicios, que conocen las consecuencias de la no prestación del servicio o de su prestación degradada
- Responsables de los datos, que conocen las consecuencias de la degradación de los datos
- Responsables de sistemas de información y responsables de operación, que conocen las consecuencias de un incidente

Para cada valoración de un activo conviene registrar la siguiente información:

- Dimensiones en las que el activo es relevante
- Estimación de la valoración en cada dimensión
- Explicación de la valoración
- Entrevistas realizadas de las que se han deducido las anteriores estimaciones.

Para la valoración de los activos se utilizarán las dimensiones de valoración definidas por la metodología:

[D] disponibilidad

[I] integridad de los datos

[C] confidencialidad de los datos

[A_S] autenticidad de los usuarios del servicio

[A_D] autenticidad del origen de los datos

[T_S] trazabilidad del servicio

[T_D] trazabilidad de los datos

Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión.

La valoración de activos se realizará con base a la escala propuesta por la metodología y que se presenta a continuación:

Valor		Criterio
10	muy alto	daño muy grave a la organización
7-9	Alto	daño grave a la organización
4-6	medio	daño importante a la organización
1-3	bajo	daño menor a la organización
0	despreciable	irrelevante a efectos prácticos

Para la valoración de los activos se sugiere el uso de una matriz de valoración donde se consigne para cada activo su valor en la dimensión que corresponda y que indica la medida del perjuicio para la organización si el activo a valorar se ve dañado en dicha dimensión.

Dicha matriz se encuentra en una plantilla que forma parte de los anexos de este documento. [Anexo 2]. De igual forma puede hacerse uso de la herramienta PILAR.

Actividad 2: Caracterización de las amenazas

Objetivo: El objetivo de esta actividad es identificar y valorar las amenazas posibles para cada activo, de tal forma que se obtenga un mapa de riesgos de la empresa.

Para el desarrollo de esta actividad se deben llevar a cabo las siguientes tareas:

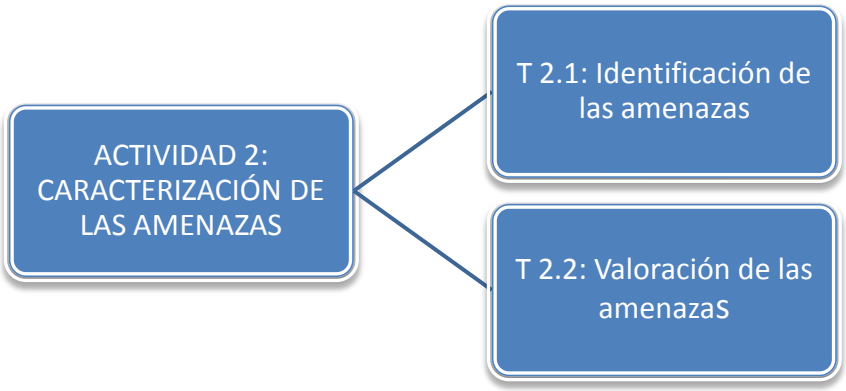


Figura 9.5: Tareas de la actividad Caracterización de las amenazas

Tarea T2.1: Identificación de las amenazas

Objetivos: Identificar las amenazas relevantes sobre cada activo

Productos de entrada: Como información de entrada para el adecuado desarrollo de esta tarea se puede utilizar la siguiente:

- Resultados de la actividad A 1, Caracterización de los activos

Productos de salida: Una vez finalizada esta tarea se obtendrán los siguientes productos de salida:

- Relación de amenazas posibles

Técnicas, prácticas y pautas: Para la ejecución de esta actividad se recomienda una serie de técnicas y facilitaran el desarrollo de la tarea y que son sugeridas por la metodología Magerit. Dichas técnicas se encuentran en los documentos que provee la metodología:

- Catálogos de amenazas (ver "Catálogo de Elementos", capítulo 5)
- Árboles de ataque (ver "Guía de Técnicas" 2.3)
- Entrevistas (ver "Guía de Técnicas" 3.6.1)
- Reuniones (ver "Guía de Técnicas" 3.6.2)
- Valoración Delphi (ver "Guía de Técnicas" 3.7)
- Ver también la sección 2.1.2, del documento “El Método”.

En esta tarea se identifican las amenazas significativas sobre los activos identificados, tomando en consideración:

- el tipo de activo
- las dimensiones en que el activo es valioso
- la experiencia de la Organización

Para cada amenaza sobre cada activo conviene registrar la siguiente información:

- explicación del efecto de la amenaza
- entrevistas realizadas de las que se ha deducido la anterior estimación
- antecedentes, si los hubiera, bien en la propia Organización, bien en otras organizaciones que se haya considerado relevantes

Para la identificación de las amenazas se usará un catálogo de amenazas posibles sobre los activos de un sistema de información, definidas por la metodología y que se han identificado como las amenazas típicas a las que puede

estar expuesto un activo. A continuación se listan las amenazas, que se encuentran de forma detallada en el documento "Catálogo de Elementos":

[N] Desastres naturales

[N.1] Fuego

[N.2] Daños por agua

[N.*] Desastres naturales

[I] De origen industrial

[I.1] Fuego

[I.2] Daños por agua

[I.*] Desastres industriales

[I.3] Contaminación mecánica

[I.4] Contaminación electromagnética

[I.5] Avería de origen físico o lógico

[I.6] Corte del suministro eléctrico

[I.7] Condiciones inadecuadas de temperatura y/o humedad

[I.8] Fallo de servicios de comunicaciones

[I.9] Interrupción de otros servicios y suministros esenciales

[I.10] Degradación de los soportes de almacenamiento de la información

[I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados

[E.1] Errores de los usuarios

[E.2] Errores del administrador

[E.3] Errores de monitorización (log)

[E.4] Errores de configuración

[E.7] Deficiencias en la organización

[E.8] Difusión de software dañino

[E.9] Errores de [re-]encaminamiento

[E.10] Errores de secuencia

[E.14] Escapes de información

[E.15] Alteración de la información

[E.16] Introducción de información incorrecta

[E.17] Degradación de la información

[E.18] Destrucción de información

[E.19] Divulgación de información

[E.20] Vulnerabilidades de los programas (software)

[E.21] Errores de mantenimiento/actualización de programas (software)

[E.23] Errores de mantenimiento/actualización de equipos (hardware)

[E.24] Caída del sistema por agotamiento de recursos

[E.28] Indisponibilidad del personal

[A] Ataques intencionados

[A.4] Manipulación de la configuración

[A.5] Suplantación de la identidad del usuario

[A.6] Abuso de privilegios de acceso

[A.7] Uso no previsto

[A.8] Difusión de software dañino

[A.9] [Re-]encaminamiento de mensajes

[A.10] Alteración de secuencia

[A.11] Acceso no autorizado

[A.12] Análisis de tráfico

[A.13] Repudio

[A.14] Interceptación de información (escucha)

[A.15] Modificación de la información

[A.16] Introducción de falsa información

[A.17] Corrupción de la información

[A.18] Destrucción la información

[A.19] Divulgación de información

[A.22] Manipulación de programas

[A.24] Denegación de servicio

[A.25] Robo

[A.26] Ataque destructivo

[A.27] Ocupación enemiga

[A.28] Indisponibilidad del personal

[A.29] Extorsión

[A.30] Ingeniería social

Para realizar el registro de las amenazas identificadas se sugiere el uso de una plantilla que forma parte de los anexos de este documento, [Anexo 3]. De igual forma puede hacerse uso de la herramienta PILAR.

Tarea T2.2: Valoración de las amenazas

Objetivos: Los objetivos de esta tarea son:

- Estimar la frecuencia de ocurrencia de cada amenaza sobre cada activo
- Estimar la degradación que causaría la amenaza en cada dimensión del activo si llegara a materializarse

Productos de entrada: Como información de entrada para el adecuado desarrollo de esta tarea se puede utilizar la siguiente:

- Resultados de la tarea T2.1, Identificación de las amenazas
- Series históricas de incidentes
- Antecedentes: incidentes en la Organización

Productos de salida: Una vez finalizada esta tarea se obtendrán los siguientes productos de salida:

- Mapa de riesgos: informe de amenazas posibles, caracterizadas por su frecuencia de ocurrencia y la degradación que causarían en los activos.

Técnicas, prácticas y pautas: Para la ejecución de esta actividad se recomienda una serie de técnicas y pautas que facilitaran el desarrollo de la tarea y que son sugeridas por la metodología Magerit. Dichas técnicas se encuentran en los documentos que provee la metodología:

- Árboles de ataque (ver "Guía de Técnicas" 2.3)
- Entrevistas (ver "Guía de Técnicas" 3.6.1)
- Reuniones (ver "Guía de Técnicas" 3.6.2)
- Valoración Delphi (ver "Guía de Técnicas" 3.7)
- Ver también la sección 2.1.2, del documento “El Método”.

En esta tarea se valoran las amenazas identificadas en la tarea anterior, tomando en consideración:

- la experiencia (historia) universal
- la experiencia (historia) del sector de actividad
- la experiencia (historia) del entorno en que se ubican los sistemas
- la experiencia (historia) de la propia Organización

Para cada amenaza sobre cada activo conviene registrar la siguiente información:

- estimación de la frecuencia de la amenaza
- estimación del daño (degradación) que causaría su materialización
- explicación de las estimaciones de frecuencia y degradación
- entrevistas realizadas de las que se han deducido las anteriores estimaciones

Para realizar el registro de las amenazas identificadas y su valoración se hará uso de una matriz que permita registrar para cada activo:

- las amenazas a las que puede estar expuesto,
- la frecuencia de ocurrencia expresada como una tasa anual (incidencias por año), la cual indica cada cuánto se materializa la amenaza y,
- la degradación estimada del activo en cada una de las dimensiones de seguridad, expresada como porcentaje de su valor e indica cuán perjudicado resultaría el activo.

La frecuencia se modela como una tasa anual de ocurrencia, siendo valores típicos los siguientes:

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

La matriz sugerida se encuentra en una plantilla que forma parte de los anexos de este documento, [Anexo2]. De igual forma puede hacerse uso de la herramienta PILAR.

Actividad 3: Estimación del estado de riesgo

El objetivo de esta actividad es realizar estimaciones del estado de riesgo dentro de la empresa objeto del análisis.

Para obtener estas estimaciones deben llevarse a cabo las siguientes tareas:

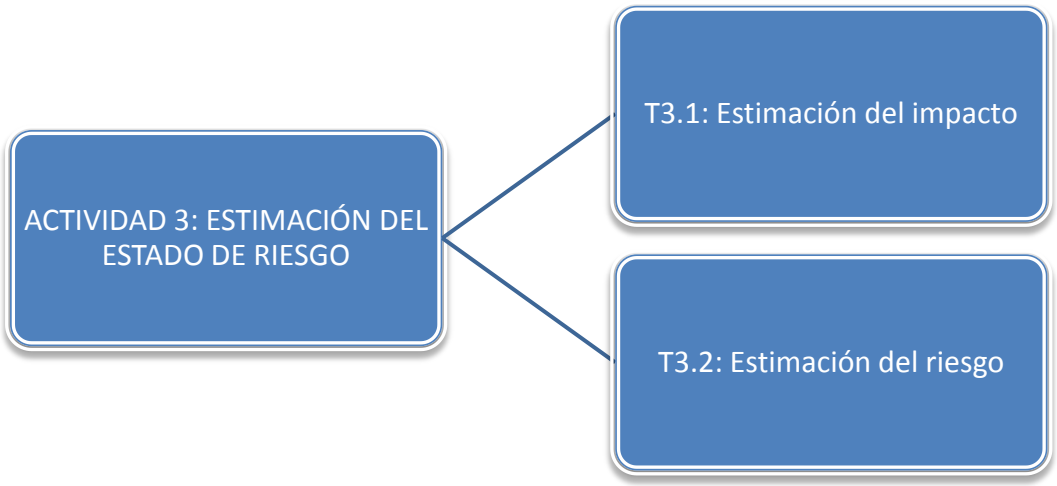


Figura 9.6: Tareas de la actividad Estimación del Estado de riesgo

T3.1: Estimación del impacto

Objetivos: Determinar el impacto potencial al que están expuestos los activos del sistema.

Productos de entrada: Como información de entrada para el adecuado desarrollo de esta tarea se puede utilizar la siguiente:

- Resultados de la actividad 1, Caracterización de los activos
- Resultados de la actividad 2, Caracterización de las amenazas

Productos de salida: Una vez finalizada esta tarea se obtendrán los siguientes productos de salida:

- Informe de impacto (potencial) por activo

Técnicas, prácticas y pautas: Para la ejecución de esta actividad se recomienda una serie de técnicas y pautas que facilitaran el desarrollo de la tarea y que son sugeridas por la metodología Magerit. Dichas técnicas se encuentran en los documentos que provee la metodología:

- Análisis mediante tablas (ver "Guía de Técnicas" 2.1)
- Análisis algorítmico (ver "Guía de Técnicas" 2.2)
- Ver también la sección 2.1.3 y 2.1.6, del documento “El Método”.

El impacto potencial es aquel al que está expuesto el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, pero no las salvaguardas actualmente desplegadas.

El cálculo de este impacto puede hacerse siguiendo alguno de los enfoques algorítmicos sugeridos por la metodología:

Modelo cualitativo: En un análisis de riesgos cualitativo se busca saber qué es lo que hay, sin cuantificarlo con precisión más allá de relativizar los elementos del modelo. Para llevarlo a término se hace uso de un modelo de cálculo que trabaja sobre una escala discreta de valores.

Modelo cuantitativo: En un análisis de riesgos cuantitativo se busca saber qué y cuánto hay, cuantificando todos los aspectos posibles. El

modelo propuesto no trabaja sobre una escala discreta de valores, sino con números reales (en el sentido matemático) positivos.

Modelo escalonado: Ciertas dimensiones de degradación de un activo se modelan más adecuadamente como escalones de valor. El caso típico es la interrupción del servicio, que responde a esquemas donde se observa una serie de escalones de interrupción que terminan con la destrucción total o permanente del activo.

Los modelos anteriores nos permiten de forma general valorar los activos, el impacto de las amenazas y el riesgo al que se está expuesto y de manera particular obtener los siguientes valores:

- El valor de los activos.
- Las dependencias entre activos.
- El valor acumulado.
- La degradación [del valor] de un activo.
- Impacto acumulado de una amenaza sobre un activo.
- Impacto repercutido de una amenaza sobre un activo.
- Frecuencia de una amenaza.
- El riesgo.

Para el cálculo del impacto se sugiere el uso de la plantilla correspondiente al [Anexo 2] de este documento, en la que para cada activo se tendrá en cuenta el valor acumulado sobre el activo en una dimensión de seguridad particular y la degradación causada por la amenaza en dicha dimensión. El cálculo del impacto se hará a través de un modelo cuantitativo y es una función del valor de activo por su degradación.

Tarea T3.2: Estimación del riesgo

Objetivos: El objetivo de esta tarea es determinar el riesgo potencial al que está sometido el sistema objeto de análisis.

Productos de entrada: Como información de entrada para el adecuado desarrollo de esta tarea se puede utilizar la siguiente:

- Resultados de la actividad 1, Caracterización de los activos
- Resultados de la actividad 2, Caracterización de las amenazas

Productos de salida: Una vez finalizada esta tarea se obtendrán los siguientes productos de salida:

- Informe de riesgo (potencial) por activo

Técnicas, prácticas y pautas: Para la ejecución de esta actividad se recomienda una serie de técnicas y pautas que facilitaran el desarrollo de la tarea y que son sugeridas por la metodología Magerit. Dichas técnicas se encuentran en los documentos que provee la metodología:

- Análisis mediante tablas (ver "Guía de Técnicas" 2.1)
- Análisis algorítmico (ver "Guía de Técnicas" 2.2)
- Ver también la sección 2.1.4 y 2.1.7 del documento “El Método”.

Para la estimación del riesgo se hará uso de la plantilla correspondiente al [Anexo 2] de este documento y se podrá hacer uso de alguno de los modelos descritos en el apartado anterior -modelo cualitativo, modelo cuantitativo y modelo escalonado-.

2.6.1.3. Informe final del análisis de riesgos

Una vez finalizado el análisis de riesgos se obtiene un mapa de riesgos de la organización o área de análisis, que servirá como base para la planificación de la auditoría.

Como parte de este proceso se obtendrán una serie de documentos finales que en su conjunto darán al auditor un panorama detallado de la situación de riesgo. Dichos documentos son los siguientes:

Modelo de valor

Informe que detalla los activos, sus dependencias, las dimensiones en las que son valiosos y la estimación de su valor en cada dimensión.

Mapa de riesgos

Informe que detalla las amenazas significativas sobre cada activo, caracterizándolas por su frecuencia de ocurrencia y por la degradación que causaría su materialización sobre el activo.

Estado de riesgo

Informe que detalla para cada activo el impacto y el riesgo frente a cada amenaza.

2.6.1.4. Informe de planificación de la auditoría

Como resultado de las fases de conocimiento de la organización y el análisis de riesgos el auditor presentará un informe donde se detalle el plan de la auditoría. Dicho plan debe contener los siguientes elementos básicos:

- Introducción
- Objetivos de la auditoría
- Alcance de la auditoría
- Planificación de los procedimientos de auditoría a ejecutar
- Recursos necesarios para la ejecución de la auditoría
- Plazo de ejecución

2.6.2. Fase de evaluación de controles

En esta fase se llevará a cabo la identificación y selección de controles a evaluar con base al mapa de riesgos obtenido en la fase anterior y a la planificación de la auditoría.

Se evaluarán los controles establecidos como medidas para mitigar el impacto de las amenazas. Estas medidas pueden prevenir o reducir la

probabilidad de que un riesgo ocurra, detectar la ocurrencia de un riesgo y minimizar el impacto o transferir el riesgo, a través de:

- La identificación de todos los controles que existen para minimizar el riesgo
- Determinando y evaluando todo control nuevo o adicional que se identifique durante el análisis del riesgos
- Priorizando todos los riesgos identificados, identificando aquellos controles que sean más eficaces y eficientes en la mitigación del riesgo.

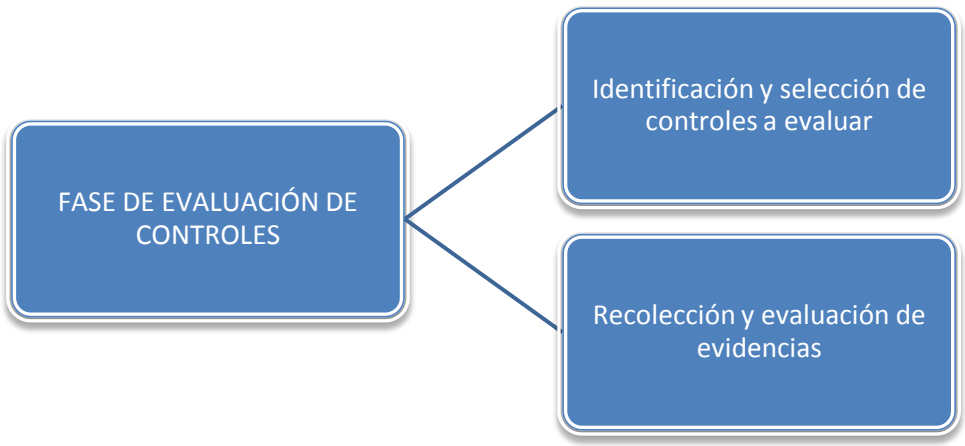


Figura 9.7: Etapas de la fase de Evaluación de Controles

Objetivos

El objetivo de esta fase es identificar los controles a evaluar, con el fin de verificar que medidas permiten realizar un adecuado tratamiento de los riesgos.

Alcance

Esta fase comprende la realización de dos etapas: la identificación y selección de controles a evaluar y la recolección y evaluación de evidencias, a través de las que se podrá hacer una adecuada evaluación de las medidas de

control desplegadas para cada amenaza y las medidas requeridas para aquellas amenazas que no están siendo tratadas.

2.6.2.1. Etapa 1: Identificación y selección de controles a evaluar

Para la identificación y selección de controles a evaluar se hará uso de los controles establecidos en el estándar ISO 27002 y en COBIT. Se recomienda para empresas pequeñas hacer uso de ISO 27002 ya que provee un grupo de áreas de control más generales. En el caso de COBIT está orientado a empresas medianas y grandes que tengan procesos de TI ampliamente desarrollados, no obstante se podrá hacer una combinación de ambos si así se requiere.

Para la identificación y selección de controles a evaluar se clasificarán las amenazas identificadas y consignadas en el mapa de riesgos, en cada área o grupo de controles ISO 27002 y/o COBIT, de tal manera que para cada amenaza se evalúe el control que debería implementarse o el control que ayudaría a minimizar el impacto de la amenaza.

Para realizar esta identificación y posterior selección de controles se sugiere el uso de la plantilla correspondiente al [Anexo 4] de este documento.

2.6.2.2. Etapa 2: Recolección y evaluación de evidencias

Una vez seleccionados los controles a evaluar se procede a la recolección y evaluación de evidencias, para lo que inicialmente se debe llevar a cabo el diseño de las pruebas de auditoría pertinentes. Este es un trabajo donde se determinan en términos generales: el objetivo de la prueba (se describen brevemente los procesos a emplear), tipo de pruebas, técnicas a utilizar y recursos requeridos en cuanto a información, hardware, software y personal.

Para el registro de esta información se sugiere el uso de una plantilla que permita dejar evidencia de las pruebas realizadas y que hará parte del informe final de auditoría.

Dicha plantilla forma parte del [Anexo 5] de este documento.

Existen dos tipos de pruebas que pueden ser utilizadas por el auditor:

Pruebas de cumplimiento: Buscan determinar si existe el control para el riesgo identificado.

Pruebas sustantivas: Buscan conocer la forma en que está implementado el control, en caso de que exista.

Además, el auditor puede hacer uso de alguna de las siguientes técnicas para el diseño y ejecución de las pruebas de auditoría:

- Observación
- Indagación: entrevistas, cuestionarios, diagramas de flujo
- Conciliación (contraste de información con personas o documentos)
- Inspección
- Investigación analítica: Evaluar tendencias
- Confirmación
- TAAC'S: Técnicas de Auditoría Asistidas por Computador

Para llevar a cabo la evaluación de los controles, se hará uso particular y a manera de ejemplo, de los controles definidos en el estándar ISO 27002 y se utilizará una matriz de verificación como parte de las pruebas de auditoría a usar por el auditor. Esta matriz está orientada a realizar pruebas de cumplimiento.

Dicha matriz de verificación se implementará a través de una plantilla que forma parte del [Anexo 4] del presente documento.

La plantilla presenta, para cada amenaza, el grupo de control en el que ha sido clasificada, la sección dentro de ese grupo de control y las preguntas de chequeo que permiten verificar la existencia o el cumplimiento de ese control.

Una vez realizado este procedimiento de verificación se obtendrá como resultado un estado general del cumplimiento de los controles frente a las amenazas y los controles que son necesarios desplegar.

El auditor según su juicio hará uso de las pruebas que considere pertinentes.

Una vez realizada esta evaluación se hará una selección de los controles que es necesario implementar y/o reforzar, para lo cual se tendrán en cuenta los siguientes aspectos:

- El coste del control comparado con el beneficio que reporta su implantación
- El nivel de riesgo que la organización está preparada para aceptar
- Los métodos de reducción de riesgos preferidos por la dirección (eliminar el riesgo, minimizar la probabilidad de ocurrencia, minimizar el impacto, transferencia del riesgo)

2.6.3. Fase de elaboración y presentación de informes

Objetivo

El objetivo de esta fase es realizar el informe final de la auditoría y la presentación de los hallazgos y recomendaciones.

Alcance

Esta fase comprende la estructuración y redacción del informe y la presentación del mismo, siguiendo algunas pautas y recomendaciones de carácter general y algunas particulares propuestas por ISACA.

2.6.3.1. Informe de hallazgos y recomendaciones

Una vez se ha finalizado la ejecución de las pruebas de auditoría, se debe proceder a la realización del informe de hallazgos y recomendaciones.

El objetivo de este informe es comunicar los resultados de la auditoría a la gerencia y/o a quien se considere pertinente.

En este informe se consignan los hallazgos, observaciones y recomendaciones. No tiene un formato en particular, pero se sugieren algunas pautas generales a tener en cuenta al momento de elaborar dicho informe:

- La elaboración del informe debe ser cuidadosa en cuanto a la información que contiene, no debe dar lugar a ambigüedades, y los hallazgos y recomendaciones deben ser claramente descritos.
- El informe debe estar documentado con las pruebas de auditoría realizadas.

- La información consignada en el informe debe ser de carácter confidencial.

ISACA provee dentro de sus estándares de auditoría, en particular el estándar S2 – Reporte, una serie de pautas para la elaboración del informe y que se sugieren dentro de esta guía, en el momento de hacer el informe de auditoría. Dichas recomendaciones se presentan a continuación:

03 El auditor de SI debe suministrar un informe, en un formato apropiado, al finalizar la auditoría. El informe debe identificar la organización, los destinatarios previstos y respetar cualquier restricción con respecto a su circulación.

04 El informe de auditoría debe indicar el alcance, los objetivos, el período de cobertura y la naturaleza, plazo y extensión de las labores de auditoría realizadas.

05 El informe debe indicar los hallazgos, conclusiones y recomendaciones, así como cualquier reserva, calificación o limitación que el auditor de SI tuviese en cuanto al alcance de la auditoría.

06 El auditor de SI debe tener evidencia de auditoría suficiente y apropiada para respaldar los resultados reportados.

07 Al emitirse, el informe del auditor de SI debe ser firmado, fechado y distribuido de acuerdo con los términos del estatuto de auditoría o carta de compromiso.

Para la realización del informe de auditoría se sugiere una plantilla, que forma parte del [Anexo 6] de este documento.

2.6.3.2. Documentación final de la auditoría

La documentación que se genera en el proceso de auditoría es el registro del trabajo de auditoría realizado y de la evidencia que soporta las conclusiones de la auditoría.

Dicha documentación debe incluir como mínimo:

- La planificación y preparación del alcance y objetivos de la auditoría
- Mapa de riesgos

- La descripción y/o recorridos en el área de auditoría vista
- El programa de auditoría
- Los pasos de auditoría realizados y la evidencia recopilada
- Los hallazgos, conclusiones y recomendaciones de auditoría

2.6.4. Fase de seguimiento

Objetivo

El objetivo de esta fase es establecer los mecanismos de seguimiento pertinentes de tal forma que pueda hacerse una evaluación constante de la eficacia de los controles desplegados y se puedan hacer los ajustes necesarios, actuando de una manera proactiva frente a los riesgos.

Alcance

Esta fase comprende el diseño de mecanismos de seguimiento por parte de la empresa y con el apoyo del auditor, de tal forma que se ajusten a la dinámica de la empresa.

2.6.4.1. Establecimiento de pautas para el seguimiento de la auditoría

Dado el enfoque basado en riesgos sobre el cual se sustenta la auditoría y que la hace dinámica, es necesario realizar evaluaciones periódicas para verificar la efectividad de los controles implementados y el impacto repercutido sobre los riesgos identificados.

El auditor, en conjunto con la empresa, debe establecer la periodicidad de las revisiones del estado del riesgo.

Para llevar a cabo esta revisión se parte del mapa de riesgos obtenido previamente y del reporte de los controles desplegados para el tratamiento de dichos riesgos.

2.6.5. Anexos de la guía

A continuación se presenta la lista de anexos de la guía de auditoría, cada anexo es un fichero independiente al documento principal.

- [Anexo 1]-Plantilla-identificacion-activos.docx

Esta plantilla permite consignar la información detallada de cada uno de los activos identificados.

- [Anexo 2]- Plantilla-valoracion-activos.xlsx[9]

Esta plantilla permite obtener el mapa de riesgos de la organización. Está diseñada como una hoja de cálculo que consta de:

Clasificación-activos: En esta hoja se hace una relación de cada uno de los activos y sus categorías, sugeridos en Magerit y servirá como base para la selección de los activos en el proceso de valoración de riesgos.

Valoración-activos: En esta hoja se lleva a cabo una valoración de los activos identificados, para lo cual se puede seleccionar la categoría del activo y el activo a particular que se quiera valorar. Cada activo se valora en la dimensión de valoración que corresponda con base en la escala de valoración sugerida por Magerit y que se encuentra especificada en esta hoja.

Dependencia entre activos: En este apartado se podrá establecer la dependencia que existe entre los diferentes activos identificados, para lo cual de un lado se seleccionarán los activos de nivel superior y de otro los activos de nivel inferior que dependen de los anteriores y se establece una relación de dependencia donde se marcan con un uno (1) aquellos activos que dependan de otro de nivel superior y con un cero (0) los que no tienen dependencia.

Clasificación-amenazas: En esta hoja se presentan las amenazas sugeridas por Magerit, clasificadas por grupos, y que servirán de base para la valoración de las amenazas. También se presenta la escala de valoración de amenazas de acuerdo con su frecuencia de ocurrencia.

[9] En este anexo se encuentran agrupadas las siguientes plantillas: valoración de activos, registro y valoración de amenazas y estimación de riesgo.

Valoración-amenazas: En esta hoja se realiza la valoración de las amenazas. Esta valoración se lleva a cabo identificando para cada activo las amenazas a las que está expuesto. Para cada amenaza se consignará la frecuencia de ocurrencia de acuerdo con la escala indicada y la degradación estimada del activo en cada una de sus dimensiones de seguridad, expresada como porcentaje del valor del activo (lo que indica en qué medida resultaría perjudicado el activo si se materializa la amenaza).

Estimación del impacto: Esta hoja contiene una fórmula que permite calcular de forma automática el impacto. Este cálculo se hace en función del valor del activo y la degradación estimada del mismo.

Estimación del riesgo: En esta hoja se realiza la estimación del riesgo como una función de la frecuencia de las amenazas y el impacto estimado.

- [Anexo 3]-Plantilla-identificacion-amenazas.docx

Esta plantilla permite realizar una descripción detallada de cada una de las amenazas identificadas.

- [Anexo4]Plantilla_identificación_evaluacion_controles_ISO_27002.xls

Esta plantilla permite realizar una verificación de los controles establecidos en la organización objeto del análisis, con base en los controles establecidos en la ISO27002. Cada amenaza identificada se clasifica dentro de alguno de los grupos de controles y se realiza una verificación de los controles asociados. La valoración del cumplimiento del control o estado del control se hace en función del nivel de cumplimiento expresado en porcentaje.

- [Anexo 5]- Plantilla_pruebas_de_auditoria.docx

Esta plantilla permite consignar de forma detallada las pruebas de auditoría realizadas y sus resultados.

- [Anexo 6]- Plantilla_informe_auditoria.docx

Esta plantilla presenta la estructura sugerida para la realización del informe de auditoría.

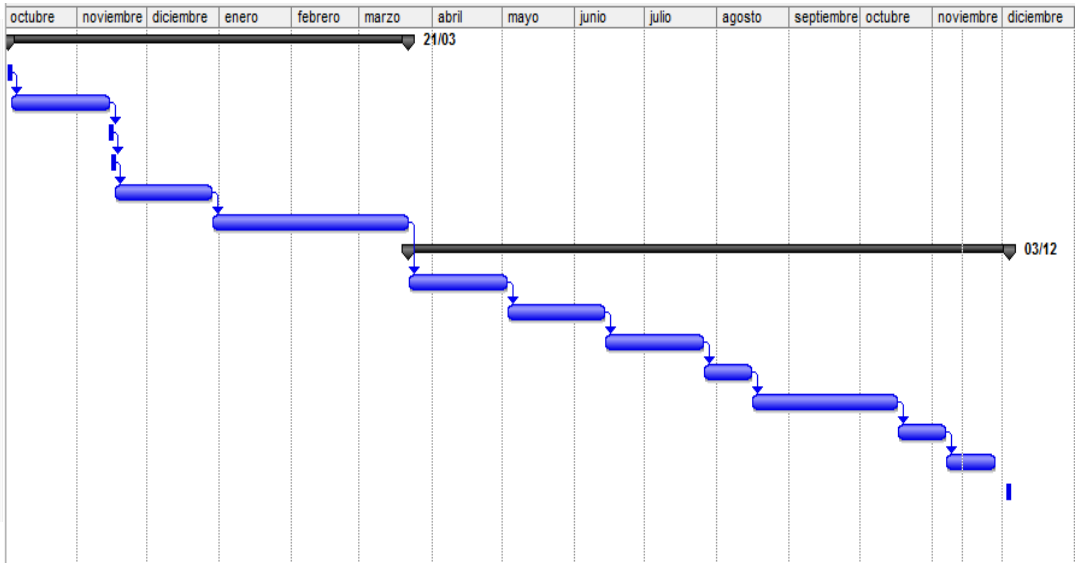
Planificación y Presupuesto

Hitos Planificación

FASE I : MARCO TEÓRICO	**123 días**	**lun 03/10/11**	**mié 21/03/12**
Definición de los objetivos del proyecto	1 día	lun 03/10/11	lun 03/10/11
Revisión bibliográfica inicial	30 días	mar 04/10/11	lun 14/11/11
Elaboración de la estructura de la memoria	1 día	mar 15/11/11	mar 15/11/11
Definición del indice del documento	1 día	mié 16/11/11	mié 16/11/11
Revisión detallada información	30 días	jue 17/11/11	mié 28/12/11
Redacción del Marco Teórico	60 días	jue 29/12/11	mié 21/03/12
FASE II : PROPUESTA GUÍA AUDITORÍA	**184 días**	jue 22/03/12	lun 03/12/12
Realización del análisis comparativo de las metodologías de auditoría	30 días	jue 22/03/12	mié 02/05/12
Realización del análisis comparativo de las metodologías de análisis de riesgos	30 días	jue 03/05/12	mié 13/06/12
Realización del análisis del papel del análisis de riesgos dentro de una auditoría informática	30 días	jue 14/06/12	mié 25/07/12
Definición estructura de la guía de auditoría	15 días	jue 26/07/12	mié 15/08/12
Elaboración guía de auditoría	45 días	jue 16/08/12	mar 16/10/12
Desarrollo de la página web para la guía de auditoría	15 días	mié 17/10/12	mar 06/11/12
Elaboración de las conclusiones y trabajos futuros	15 días	mié 07/11/12	mar 27/11/12
Entrega del documento final	1 día	lun 03/12/12	lun 03/12/12

Planificación temporal

FASE I : MARCO TEÓRICO	
Definición de los objetivos del proyecto	
Revisión bibliográfica inicial	
Elaboración de la estructura de la memoria	
Definición del indice del documento	
Revisión detallada información	
Redacción del Marco Teórico	
FASE II : PROPUESTA GUÍA AUDITORÍA	
Realización del análisis comparativo de las metodologías de auditoría	
Realización del análisis comparativo de las metodologías de análisis de riesgos	
Realización del análisis del papel del análisis de riesgos dentro de una auditoría informática	
Definición estructura de la guía de auditoría	
Elaboración guía de auditoría	
Desarrollo de la página web para la guía de auditoría	
Elaboración de las conclusiones y trabajos futuros	
Entrega del documento final	



Presupuesto por partidas

MANO DE OBRA	HORAS	COSTE
FASE I : MARCO TEÓRICO		
Definición de los objetivos del proyecto	4	120€
Revisión bibliográfica inicial	60	1.800€
Elaboración de la estructura de la memoria	4	120€
Definición del índice del documento	4	120€
Revisión detallada información	60	1.800€
Redacción del Marco Teórico	120	3.600€
FASE II : PROPUESTA GUÍA AUDITORÍA		
Realización del análisis comparativo de las metodologías de auditoría	40	1.200€
Realización del análisis comparativo de las metodologías de análisis de riesgos	40	1.200€
Realización del análisis del papel del análisis de riesgos dentro de una auditoría informática	20	600€
Definición estructura de la guía de auditoría	8	240€
Elaboración guía de auditoría	120	3.600€
Desarrollo de la página web para la guía de auditoría	32	960€
Elaboración de las conclusiones y trabajos futuros	8	240€
TOTAL MANO DE OBRA	**520**	**15.600€**

MEDIOS MATERIALES	CANTIDAD	COSTE
Microsoft Office 2010 (versión hogar y pequeña empresa)	1	379€
Ordenador portátil	1	650€
TOTAL MEDIOS MATERIALES		**1.029€**
TOTAL PRESUPUESTO		**16.629€**

El presupuesto total de este proyecto ascienda a la cantidad de **16.629 euros.**

El ingeniero consultor:

Fdo.: Mª del Carmen Crespo Rin

Conclusiones

A través del estudio realizado del estado de la cuestión de las áreas de conocimiento involucradas en este trabajo, se ha podido ver como la auditoría informática y el análisis de riesgos son áreas del conocimiento que han tenido una evolución importante tanto a nivel teórico, a través de los aportes realizados por organizaciones públicas y privadas, como a nivel práctico a través de su aplicación en el ámbito empresarial como mecanismos de evaluación y control.

Se han realizado importantes esfuerzos en el desarrollo de normativas, estándares, metodologías y marcos de trabajo enfocados hacia la auditoría informática y el análisis de riesgos, de reconocimiento internacional, que ayudan a la estandarización y normalización de estas disciplinas del conocimiento y que permiten a las empresas contar con referentes para sus procesos de auditoría y análisis de riesgos.

Tras realizar el estudio teórico se ha podido observar que si bien existen estándares y normativa relacionada con las dos áreas objeto de este trabajo, no hay una metodología concreta de auditoría informática que dé las pautas de como poder llevar a cabo una auditoría con un enfoque de análisis de riesgos, aunque sí existen recomendaciones sobre cómo usar el análisis de riesgos dentro de una auditoría como es el caso de las guías de auditoría de ISACA.

El estudio comparativo de las metodologías, estándares y marcos de trabajo nos ha mostrado las diferentes posibilidades en cuanto a técnicas y métodos que tienen las empresas a la hora de abordar un proceso de auditoría y análisis de riesgos, y como debe hacerse un análisis cuidadoso de cuál es la que mejor se adaptará a cada situación particular. Algunos factores importantes a tener en cuenta para dicho análisis son: el tipo de empresa, el tamaño, la madurez de sus procesos de TI, el alcance de la auditoría y/o análisis de riesgos, los recursos técnicos, financieros y de personal con que cuentan, en cuanto a la metodología

se debería tener en cuenta su ámbito de aplicación, el alcance, el tipo de acceso (público o privado), y los procesos, fases o etapas que desarrollan.

Para el desarrollo de la guía de auditoría se ha usado la metodología Magerit para la fase de análisis de riesgos, por ser una metodología de reconocimiento en al ámbito local e internacional y por ofrecer un proceso detallado para la ejecución del análisis de riesgos, además de poner a disposición múltiples recursos para guiar dicho proceso; otro factor importante es que se encuentra alineada con estándares y normativa nacional e internacional y que se puede aplicar en cualquier tipo de empresa y de cualquier tamaño, adaptándose fácilmente a empresas medianas y pequeñas.

Para el caso de la evaluación de controles se ha decidido optar por ISO 27002 por proporcionar un grupo de controles claramente segmentados y que cubren un amplio espectro de los tipos de controles a aplicar para sistemas de información y que pueden adaptarse a cualquier tipo de empresa, además de ser un estándar de ámbito mundial.

En trabajos futuros se podría abordar la guía de auditoría con base en otra metodología de análisis de riesgos como complemento a Magerit, de tal forma que permita contrastar otros métodos de estimación de riesgos. Por otra parte se podría revisar la recién publicada versión 3 de Magerit y ajustar la guía de acuerdo a los cambios introducidos en la misma.

Otra línea futura podría enfocarse en usar COBIT para la evaluación de controles, de tal forma que pueda ampliarse el alcance de aplicación de la guía, dado el amplio espectro que cubre COBIT.

Bibliografía

[AENO 08] Asociación Española de Normalización y Certificación – AENOR
UNE 71504:2008: Metodología de análisis y gestión de riesgos para los sistemas de Información.
http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0041430&PDF=Si
Fecha de acceso: Octubre de 2011

[AIFC 08] Blog: Auditoría, Informática, Fraudes, CAATTs
La familia ISO 27000
http://fraudit.blogspot.com/2008/07/la-familia-iso-27000.html
Fecha de acceso: Octubre de 2011

[AS/NZS 09] Comité de Normas de Australia / Nueva Zelanda - Organización Internacional para la Estandarización – ISO AS/NZS ISO 31000:2009
http://www.iso.org/iso/catalogue_detail?csnumber=43170
Fecha de acceso: Octubre de 2011

[AVEL 08] J. Cao Avellaneda
Artículo: "Publicada la ISO 27005:2008 sobre gestión del riesgo."
Blog Sistemas de Gestión Seguridad de la Información, 2008
http://sgsi-iso27001.blogspot.com/2008/06/publicada-la-iso-270052008-sobre-gestin.htmlFecha de acceso: Octubre de 2011

[BALL 10] M. Ballester
Gobierno de las TIC ISO/IEC 38500
Journal ISACA, 2010
http://www.isaca.org/Journal/Past-Issues/2010/Volume-1/Pages/Gobierno-de-las-TIC-ISO-IEC-385001.aspx
Fecha de acceso: Noviembre de 2011

[CALI 12] Blog calidad en las TIC
http://calidadtic.blogspot.com.es/2012/10/disponible-la-nueva-version-de-magerit.html
Fecha de acceso: Octubre de 2012

[CARI 06] L. Carima Moreno
Tesis: La auditoría Informática
Universidad de Colima, México, Facultad de ingeniería Mecánica y Eléctrica, 2006

[COBIT 07] Instituto de Administración de las Tecnologías de la Información – ITGI
Objetivos de control para la información y tecnologías relacionadas – CoBiT 4.1
http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx
Fecha de acceso: Octubre de 2011

[CRAM 06] Agencia Central de Cómputo y Telecomunicaciones (CCTA)
CRAMM-CCTA: Risk Analysis and Management Methodology-Metodología para el análisis y la gestión de riesgos
http://www.cramm.com/
Fecha de acceso: Noviembre de 2011

[DIAZ 10] M. Díaz Sampedro
Artículo: Publicada la norma ISO 27004:2009
Portal Navactiva, 2010
http://www.navactiva.com/es/documentacion/publicada-la-norma-iso-27004-2009_49051
Fecha de acceso: Diciembre de 2011

[ECHE 97] José Antonio Echenique García, Auditoría en informática, 1997, McGraw-HILL.

[ENS 10] Ministerio de la Presidencia. Secretaría General Técnica
Esquema Nacional de Seguridad.
https://www.ccn-cert.cni.es/index.php?option=com_content&view=article&id=2420&Itemid=211&lang=es#1
Fecha de acceso: Diciembre de 2011

[FORU 11] Forum ISO 27001 security
ISO/IEC 27007:2011
http://www.iso27001security.com/html/27007.html
Fecha de acceso: Diciembre de 2011

[GOME 03] L. Gómez, M. Farías, M. Mendoza
Ponencia: Importancia del Análisis de Riesgo de Seguridad
Grupo de Seguridad de RedCUDI, México
seguridad.cudi.edu.mx/congresos/2003/cudi2/impariesgo.pdf

[GTAG 09] Global Technology Audit Guides (GTAG®)
Institute of Internal Auditors - IIA
http://www.theiia.org/guidance/technology/
Fecha de acceso: Noviembre de 2011

[HERN 00] Enrique Hernández Hernández. Auditoría en informática: Un enfoque metodológico y práctico, 2000, Compañía Editorial Continental

[INTE 10] Instituto Nacional de las Tecnologías de la Comunicación - INTECO
Curso Sistema de Gestión de la Seguridad de la Información - SGSI,
http://cert.inteco.es/Formacion/SGSI/Conceptos_Basicos/
Fecha de acceso: Diciembre de 2011

[ISAC 07] Information Systems Audit and Control Association - ISACA
Normas Generales Para la Auditoría de Sistemas de Información
http://www.isaca.org/Knowledge-Center/Standards/Pages/Standards-for-IS-Auditing-Spanish-.aspx
Fecha de acceso: Noviembre de 2011

[ISAC 10] Information Systems Audit and Control Association - ISACA
IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals, 2010

[ISO/IEC 05] Organización Internacional para la Estandarización - ISO
ISO/IEC 27002:2005: Tecnologías de la información – Técnicas de Seguridad - Código de buenas prácticas para la Gestión de la Seguridad de la Información.
http://www.iso.org/iso/catalogue_detail?csnumber=50297
Fecha de acceso: Diciembre de 2011

[ISO/IEC 05a] Organización Internacional para la Estandarización - ISO
ISO/IEC 27001:2005: Tecnologías de la información - Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103
Fecha de acceso: Diciembre de 2011

[ISO/IEC 09] Organización Internacional para la Estandarización - ISO

ISO/IEC 27004:2009: Tecnologías de la información – Técnicas de Seguridad – Mediciones para la Gestión de la Seguridad de la Información.

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42106

Fecha de acceso: Noviembre de 2011

[ISO/IEC 11] Organización Internacional para la Estandarización - ISO

ISO/IEC 27005:2011: Tecnologías de la información –Técnicas de Seguridad - Gestión del riesgo de seguridad de la información.

http://www.iso.org/iso/catalogue_detail?csnumber=56742

Fecha de acceso: Diciembre de 2011

[ISSA 11] ISSA (Information Systems Security Association) - Perú

Inventario de metodologías y herramientas de análisis y gestión de riesgos.

http://issaperu.org/?p=88

Fecha de acceso: Octubre de 2011

[ISSA 11a] ISSA (Information Systems Security Association) – Perú

Artículo: ISO 27004

http://issaperu.org/?p=13

Fecha de acceso: Octubre de 2011

[ITGI 08] IT Governance Institute
Alineando CobiT® 4.1, ITIL® V3 y ISO/IEC 27002 en beneficio de la empresa, 2008
http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-Cobit-4.1,-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa-v2,7.pdf
Fecha de acceso: Marzo de 2012

[ITGO 11] IT Governance – Web
ISO/IEC 27007:2011
http://www.itgovernance.co.uk/products/3716
Fecha de acceso: Diciembre de 2011

[LARR 09] A. Larrondo
Proyecto Fin de Carrera: "Uso de la norma ISO/IEC 27004 para Auditoría Informática".
E-archivo Universidad Carlos III de Madrid. Ingeniería Técnica de Informática de Gestión, 2010.
http://e-archivo.uc3m.es/handle/10016/10564
Fecha de acceso: Noviembre de 2011

[MAGE 97] Ministerio de Hacienda y Administraciones Públicas
Magerit versión 1.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
Centro de Transferencia de Tecnología – CTT
http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=184
Fecha de acceso: Octubre de 2011

[MAGE 06] Ministerio de Hacienda y Administraciones Públicas
Magerit versión 2.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
Centro de Transferencia de Tecnología – CTT
http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=184
Fecha de acceso: Octubre de 2011

[MEHA 10] Clusif (Club Francés de la Seguridad de la Información)
MEHARI: Método Armonizado de Análisis de Riesgos
http://www.clusif.asso.fr/en/clusif/present/
Fecha de acceso: Noviembre de 2011

[NAVA 10] F. Nava García
Apuntes asignatura Auditoría informática
Universidad Rey Juan Carlos, 2010
http://www.gavab.escet.urjc.es/wiki/bin/ai/[10]
Fecha de acceso: Octubre de 2011

[OCTA 08] Software Engineering Institute (SEI), Carnegie Mellon
OCTAVE: Operationally Critical Threat, Asset, and Vulnerability Evaluation. Method Implementation Guide.
http://www.cert.org/octave/octavemethod.html
Fecha de acceso: Noviembre de 2011

[OOCI 03] Conceptos de auditoría Informática
Auditoría Informática Apuntes
http://www.oocities.org/mx/acadentorno/aui.htm
Fecha de acceso: Octubre de 2011

[10] A fecha de finalización de la memoria esta web no estaba disponible, pero fue usada información de dicha web cuando estuvo disponible.

[PIAT 08] M.Piattini, E. del Peso, M. Del Peso
Auditoría de Tecnologías y Sistemas de Información
Alfaomega, Ra-Ma, Madrid, España. 2008

[RUBI 09] E. Rubio, J. Patiño
"Desarrollo de Políticas de Seguridad Informática e Implementación de Cuatro Dominios en Base a la Norma 27002 para el Área de Hardware en la Empresa Uniplex Systems S.A. en Guayaquil".
Repositorio de la Escuela Politécnica del Litoral. Facultad de Ingeniería en Electricidad y Computación, 2009.

[SOBR 99] Roberto Sobrinos Sánchez. Escuela Superior de Informática de Ciudad Real Universidad de Castilla – La Mancha.
Planificación y Gestión de Sistemas de Información, 1999

[STIC 10] Centro Criptológico Nacional
Guía de Seguridad (CCN-STIC-802)
Esquema Nacional de Seguridad
Guía de Auditoría

[UCMA 09] Universidad de Castilla-La Mancha - Departamento de Informática
Metodología de la Auditoría Informática
Apuntes asignatura auditoría de sistemas de información, 2009
http://www.dsi.uclm.es/asignaturas/42366/[11]
Fecha de acceso: Noviembre de 2011

[11] A fecha de finalización de la memoria esta web no estaba disponible, pero fue usada información de dicha web cuando estuvo disponible.

[WIKI 11] Wikipedia

ISO/IEC 27007:2011

http://en.wikipedia.org/wiki/ISO/IEC_27007

Fecha de acceso: Diciembre de 2011