UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA

Escuela Técnica Superior de Ingeniería Informática

Departamento de Ingeniería de Software y Sistemas Informáticos

TESIS DOCTORAL

MISITILEON (Metodología que Integra Seguridad en ITIL Evolucionada y Orientada a la Normalización)

Elena Ruiz Larrocha
Ingeniera Superior en Informática

2010

UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA

Escuela Técnica Superior de Ingeniería Informática

Departamento de Ingeniería de Software y Sistemas Informáticos

TESIS DOCTORAL

MISITILEON (Metodología que Integra Seguridad en ITIL Evolucionada y Orientada a la Normalización)

Elena Ruiz Larrocha
Ingeniera Superior en Informática

2010

UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA

Escuela Técnica Superior de Ingeniería Informática

Departamento de Ingeniería de Software y Sistemas Informáticos

MISITILEON (Metodología que Integra Seguridad en ITIL Evolucionada y Orientada a la Normalización)

Elena Ruiz Larrocha
Ingeniera Superior en Informática

Director:

Jesús María Minguet Melián

A mis padres y mi marido,
sin vuestra insistencia
nunca habría terminado.

ÍNDICE

LISTA DE SÍMBOLOS, ABREVIATURAS Y SIGLAS

AETIC	Asociación de Empresas de Electrónica, Tecnologías de la Información y Telecomunicaciones de España.
ANS	Acuerdo de Nivel de Servicio.
ANSI	*American National Standards Institute.*
BD	Base de Datos.
BDC	Base de Datos de Conocimiento.
BDGC	Base de Datos de Gestión de la Configuración.
BS	*British Standard.*
BSD	Biblioteca de Software Definitivo.
BSI	*British Standard Institute.*
CAB	*Change Advisory Board.*
CAU	Centro de Atención al Ususario.
CCTA	*Central Computer and Telecommunications Agency.*
CI	*Configuration Item.*
CIA	*Confidentiality, Integrity, Availability.*
CMDB	*Configuration Management Data Base.*
CMMI	*Capability Maturity Model Integrated.*
CMS	*Configuration Management System.*
COBIT	*Control Objectives for Information and related Technology.*
CPU	*Central Process Unit.*
CSI	*Computer Security Institute.*

CTN	Comité Técnico de Normalización.
DEA	Diploma de Estudios Avanzados.
DNS	*Domain Name System.*
EA	*European Acreditation.*
EC	Elemento de Configuración.
ETSI	Escuela Técnica Superior de Ingeniería.
EXIN	*Examination Institute for Information Science.*
FAQ	*Frequent Asked Questions.*
FBI	*Federal Bureau of Investigation.*
FTP	*File Transfer Protocol.*
GB	Giga Byte.
GGC	Grupo de Gestión del Cambio.
GITIM	*Government Information Technology Infrastructure Method.*
GPL	*General Public License.*
GSI	Gestor de la Seguridad de la Información.
HTTP	*Hypertext Transfer Protocol.*
IDS	*Intrusion Detection Systems.*
IDXP	*Intrusion Detection Exchange Protocol.*
IEEE	*Institute of Electrical and Electronics Engineers.*
IMAP	*Internet Message Access Protocol.*
IP	*Internet Protocol.*
ISEB	*ITIL Service Management Qualification.*
ISM	*Information Security Management.*
ISMS	*Information Security Management System.*

ISO	*International Standard Organization.*
ISS	*Internet Security System.*
ISSA	*Information Systems Security Association.*
ITIL	*Information Technology Infrastructure Library.*
ITSMS	*Information Technologies Service Management System.*
ITU	*International Telecommunications Union.*
KGI	*Key Goal Indicator*.
KPI	*Key Process Indicator.*
LAN	*Local Area Network.*
MAGERIT	Metodología de Análisis y Gestión de Riesgos de los SI.
MB	Mega Byte.
MIME	*Multipurpose Internet Mail Extensions Encoding.*
MISITILEON	Metodología que Integra ITIL Evolucionada y Orientada a la Normalización.
MOF	*Microsoft Operations Framework.*
MVC	Modelo Vista Controlador.
MTBF	*Mean Time Between Failures.*
OGC	*Office of Government Commerce.*
OHSAS	*Ocupational Health and Safety management Systems.*
OLA	*Operational Level Agreement.*
OTAN	Organización del Tratado Atlántico Norte.
PDC	Petición de Cambio.
PDCA	*Plan Do Check Act.*
POP3	*Post Office Protocol 3.*

POP4	*Post Office Protocol 4.*
PYME	Pequeña y Mediana Empresa.
RAE	Real Academia Española.
RAM	*Random Access Memory.*
RFC	*Request For Change.*
RNS	Requisitos de Nivel de servicio.
SCAMPI	*Standard CMMi Appraisal Method for Process Improvement.*
SCSI	*Small Computer System Interface.*
SDD	*Software Design Document.*
SEDISI	Asociación Española de Empresas de Tecnologías de la Información, Actualmente AETIC.
SEI	*Software Engineering Institute.*
SGSI	Sistema de Gestión de la Seguridad de la Información.
SGSTI	Sistema de Gestión de Servicios de TI.
SKMS	*Service Knowledge Management System.*
SLA	*Service Level Requirement.*
SMTP	*Simple Mail Transfer Protocol.*
SO	Sistema Operativo.
SRD	*Software Requirements Document.*
TCP	*Transmission Control Protocol.*
TQM	*Total Quality Management.*
UML	*Unified Modelling Language.*
UNED	Universidad Nacional de Educación a Distancia.
UPM	Universidad Politécnica de Madrid.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I. INTRODUCCIÓN.

Los hombres aprenden mientras enseñan[1].

En este primer capítulo se presenta la motivación del trabajo de investigación realizado para esta tesis doctoral, así como los objetivos que se han pretendido alcanzar.

Además, en este capítulo se incluye una descripción de la organización de la memoria de esta tesis y algunas consideraciones generales a tener en cuenta.

1. Dedicatoria

Como presentación de este capítulo se ha querido añadir este pequeño apartado, con la intención de esclarecer la duda de algún curioso que haya querido ver algo más allá del nombre de la tesis propuesta. Efectivamente, hay una motivación para haber forzado de alguna manera las siglas de la metodología MISITILEON (Metodología que Integra Seguridad en ITIL Evolucionada y Orientada a la Normalización) y es que el 22 de febrero de 2009 nació el primer hijo de la doctorando, de nombre León, así pues, en su honor se ha elegido el nombre.

[1] Lucio Anneo Séneca (Córdoba 4 a. C. – Roma 65 d. C.).

2. Motivación

El origen del interés de la doctorando por ITIL nace en el año 2001, momento en el que obtiene el certificado en Fundamentos de ITIL (*Foundation Certificate in IT Service Management)* en su versión 2.0 por el EXIN (*Examination Institute for Information Science*). En esa fecha, en España sólo existían unas decenas de acreditaciones. Tras varios años realizando los cursos de doctorado[2] y de trabajar como consultora de riesgos informáticos por cuenta ajena[3], entra a formar parte del personal docente de la UNED (Universidad Nacional de Educación a Distancia) en el año 2003. A partir de entonces y hasta finales de 2005 realiza el Trabajo de Investigación[4] del DEA, relacionado con la mejora de procesos software y por tanto con esta tesis doctoral. Al mismo tiempo, a partir del año 2004 colabora con la Cátedra Iberoamericana de la UPM (Universidad Politécnica de Madrid) en la realización de artículos de investigación[5] basados en ITIL. Durante todo este tiempo, la doctorando dirige diversos Proyectos Fin de Carrera[6] de ITIL por un lado,

[2] Métricas del Software, Gestión y Mejora de Procesos Software, Diseño de Entornos Interactivos de Enseñanza y Aprendizaje Basados en Computador: Principios, tecnologías y Estándares.
[3] La doctorando trabajó como consultora para Arthur Andersen entre los años 2000 y 2002.
[4] AMSPI: Método de Evaluación para la Mejora de Procesos Software.
[5] * E. Ruiz, J. Minguet, G. Diaz, M. Castro, A. Vara. *Filling the gap of Information Security Management inside ITIL: proposals for graduate students*. Premiado en el Congreso Internacional EDUCON 2010 como ***Best Student Paper***.
* E. Ruiz, J. Minguet. *MISITILEON: Propuesta para solucionar las carencias de ITIL en la Gestión de la Seguridad de la Información*. Admitido en: 39JAIIO Jornadas Argentinas de Informática. Caba - Argentina, Septiembre 2010.
* E. Ruiz, G. Gómez, M. Arcilla, J. Calvo-Manzano. *A solution for establishing the Information Technology Service Management processes implementation sequence*. Congreso EUROSPI, 2008.
* E. Ruiz, C. Cerrada, M. Arcilla, G. Gómez, J. Calvo-Manzano, T. San Feliu, A. Sánchez. *Una Propuesta Organizativa de los Procesos SD y SS en ITIL*. Reicis, Volumen 2, Nº2, octubre 2007.
* E. Sancristobal, M. Castro, E. Ruiz, S. Martín, R.Gil, G. Diaz and J. Peire. *Integrating and Reusing of Virtual Labs in Open Source LMS*. REV2008.
[6] Sistema para el Asesoramiento en la Implantación de la norma ISO 20000 en una Organización, Caso práctico de aplicación de ITIL versión 3 en la mejora de los procesos en DESA (empresa de desarrollo de software): ITIL. MY-ITIL. Sistema de Asesoramiento a la Implantación de Procesos ITIL Dentro de una

de Seguridad Informática por otro y también de ambos temas relacionados entre sí, de alumnos de la E.T.S.I. Informática de la UNED. Y añadido a todo lo anterior, la doctorando imparte cursos de formación en ITIL a empresas privadas del sector de las Nuevas Tecnologías[7].

En 2008 obtiene la certificación Fundamentos de ITIL (*ITIL Foundation Examination*) versión 3[8]. Y a lo largo de esos años ha impartido numerosos seminarios y cursos de verano y otoño en la universidad, siempre relacionados con ITIL, ISO 20000 y la Seguridad. Finalmente en diciembre de 2008 se entrega y se admite el Anteproyecto de la presente Tesis Doctoral.

Organización. Mejora de la calidad en la gestión de servicios de TI. Metodologías, Gestión de la Seguridad en ITIL, etc.

[7] Como por ejemplo IECISA (Informática de El Corte Inglés).

[8] Véase [COM08] A esa fecha, más de 3.500 profesionales en España están certificadas en ITIL (pero en su versión anterior, la V2).

3. Ámbito

Esta tesis doctoral se ubica en el ámbito de la Ingeniaría del Software, y concretamente en el área de la mejora de procesos software. El problema que existe a nivel general en el desarrollo de proyectos software, es que la mayoría de ellos fracasan. El porcentaje de los proyectos software fallidos en 2006 era superior al 66% [STA06]; situación que no ha mejorado sensiblemente a día de hoy. La causa se debe a una pobre gestión de los proyectos, escasa usabilidad de los procesos software y escaso uso de las técnicas de la Ingeniería del Software. Añadido a todo esto, está el problema de la Seguridad Informática. En esta tesis se plantea una solución a ambos problemas para mejorar la usabilidad de la metodología ITIL particularmente en los proyectos software, además de incorporar cierto grado de seguridad en todo ello.

La aportación de esta tesis doctoral se realiza en esta área de investigación, dentro del ámbito de la mejora de los procesos software, y concretamente en el entorno de las mejores prácticas de ITIL, proponiendo un marco metodológico de trabajo para mejorar la eficiencia de uso y al mismo tiempo mejorar la seguridad de los procesos.

Como se hablará en numerosas ocasiones a lo largo de esta memoria de las mejores prácticas, se ofrece aquí una definición:

"una manera de hacer las cosas o trabajos, aceptado ampliamente por la industria y que funciona correctamente..."[9]

"Las mejores prácticas" son el mejor acercamiento a una situación basada en observaciones sobre organizaciones efectivas en similares circunstancias de negocio. Un acercamiento a las mejores prácticas significa la búsqueda de ideas y experiencias que han funcionado con aquellos que emprendieron actividades similares en el pasado, para decidir cuáles de esas prácticas son relevantes para la situación actual. Una vez identificadas se prueban, con intención de ver si las mismas funcionan, antes de incorporarlas como prácticas del proceso.

Las mejores prácticas no se refieren a "re-inventar la rueda" sino que es el aprendizaje a través de otros con implementaciones que han sido desarrolladas para que funcionen correctamente [Ref Web 6].

[9] Aidan Lawes, CEO itSMF.

4. Justificación

Sirva como ejemplo que, tan sólo en Estados Unidos las empresas se gastaban cada año 250.000 millones de dólares en 175.000 proyectos de desarrollo de software. Sólo uno de cada seis proyectos se terminó en plazo y con el presupuesto previsto; uno de cada tres se canceló por problemas de calidad y con pérdidas de 81.000 millones de dólares, y la mitad acabó casi duplicando el presupuesto [AMB07].

Las mejores prácticas de la Ingeniería del Software para realizar los procesos software que se llevan a cabo en el desarrollo de proyectos mejoran la productividad, la calidad, la satisfacción del cliente y la predicción del coste y la planificación [WIT00].

La práctica en mejora de procesos software proporciona beneficios como la reducción de costes, el incremento de la productividad, la mejora de la calidad y la satisfacción del cliente [SOM04] [CAP04] [SEI06] [NIA06].

El éxito de la mejora de procesos está asociado con la explotación del conocimiento existente y con la exploración de nuevos conocimientos [DYB05] para alcanzar innovación en las organizaciones, y por tanto, ventajas competitivas frente a la competencia.

Hoy en día, ITIL representa mucho más que una serie de libros útiles sobre Gestión de Servicios TI. El marco de mejores prácticas en la Gestión de Servicios TI representa un conjunto completo de organizaciones, herramientas, servicios de educación y consultoría,

marcos de trabajo relacionados, y publicaciones. Desde 1990, se considera a ITIL como el marco de trabajo y la filosofía compartida por quienes utilizan las mejores prácticas TI en sus trabajos. Gran cantidad de organizaciones se encuentran en la actualidad cooperando internacionalmente para promover el estándar ITIL como un estándar de facto para la Gestión de Servicios TI [Ref Web 12].

ITIL no se plantea objetivos concretos relacionados con servicios concretos, sino que es un marco de referencia de cómo buenas prácticas generales pueden ayudar al negocio. Esta falta de profundización de ITIL en aspectos concretos, como es el de la Seguridad Informática, justifican esta tesis doctoral.

5. Objetivos

En primer lugar se recopiló información sobre los siguientes puntos:

- Estado del arte relacionado con ITIL (en sus versiones 2 y 3).
- Estado del arte de la Seguridad Informática.

Posteriormente se detectaron los puntos débiles de ITIL versión 2 y versión 3, se hizo una comparativa entre ambas versiones de ITIL y se detallaron los puntos comunes entre ITIL e ISO 20000.

El objetivo principal de la Tesis es presentar una nueva metodología original: MISITILEON, basada en ITIL Versión 2 y Versión 3, que las mejore incluyendo puntos fuertes de otras metodologías y estándares (como por ejemplo ISO 20000) y añadiendo Seguridad en sus procesos. A su vez se pretenden lograr, entre otros, los siguientes objetivos:

- reducción del tiempo de desarrollo de los productos
- reducción de costes
- incremento de la productividad
- mejora de ciertos parámetros de calidad

El segundo objetivo es verificar la idoneidad del modelo de metodología propuesto en esta tesis. Para ello, en primer lugar se ha utilizado la experiencia previa de la doctorando, que durante varios años ha podido ver todo el proceso de cambio sufrido en diversas empresas que han implementado ITIL. Y en segundo lugar se ha examinado cuidadosamente el diseño y la implementación de MISITILEON. Para ello, se ha aplicado esta metodología a un caso práctico concreto, estudiando cómo se comporta antes y después de utilizar MISITILEON, y finalmente se han obtenido una serie de datos cuantitativos que comprueban las ventajas de emplear esta metodología.

El tercer objetivo ha sido crear una aplicación (Sistema de Evaluación de Conocimientos MISITILEON) de sencillo manejo y útil para usuarios y expertos. Esta herramienta podrá servir tanto para organizaciones que quieren tener un primer contacto con ITIL (que están barajando la posibilidad de implantar ITIL o alguno de sus procesos, y que aún no lo han decidido) como para usuarios que quieran conocer qué es la librería de mejores prácticas de TI, personas interesadas en conocer más acerca de su implantación o quienes desean iniciar algún tipo de proceso de certificación.

Además esta herramienta puede ser útil para los auditores en los procesos de certificación que lleven a cabo sobre alguna organización. Pueden emplear esta herramienta para realizar una lista de chequeo (a alto nivel) del estado actual de la organización respecto a la gestión de los procesos de TI. También pueden emplear esta lista para identificar dónde hay que centrar los objetivos de la revisión de auditoria y para facilitar la recopilación de evidencias sobre cómo se están siguiendo los procedimientos establecidos en los departamentos auditados.

Por último, se han analizado los resultados obtenidos en las pruebas realizadas con la metodología MISITILEON y se han recopilado las estimaciones y conclusiones extraídas sobre su aplicabilidad.

6. Organización de la tesis

La presente tesis se organiza en los siguientes capítulos y apéndices:

- *Capítulo 1. INTRODUCCIÓN.*

En él se presentan la motivación, el ámbito, la justificación y los objetivos principales de esta tesis doctoral.

- *Capítulo 2. REVISIÓN DEL ESTADO DEL ARTE.*

En este capítulo se presenta ITIL en sus dos versiones (se profundiza mucho más en ellas en el Capítulo 3) así como otros estándares, metodologías y normas muy ligados a estas mejores prácticas. Además se presenta también un estudio del estado del arte de la Seguridad Informática en general. Para no hacer realmente tediosa la lectura de este capítulo, debido a su gran volumen se ha dejado la mayor parte de la documentación realizada en varios de sus anexos[10]. Como aportación original en este capítulo se ofrece una comparativa entre ITIL e ISO 20000.

- *Capítulo 3. REVISIÓN CRÍTICA DE ITIL.*

Se estudia en detalle las dos versiones de ITIL (Versión 2 y Versión 3) y se ofrece una comparativa entre ellas. Esta comparativa es una aportación original de esta tesis.

[10] Anexo 1. Metodologías, Anexo 2. Seguridad y Anexo 3. Ciclos de Vida.

- *Capítulo 4. MISITILEON. METODOLOGÍA QUE INTEGRA SEGURIDAD EN ITIL EVOLUCIONADA Y ORIENTADA A LA NORMALIZACIÓN.*

En este capítulo se presenta, describe y desarrolla la principal aportación de esta tesis doctoral, que pretende ser la solución a los problemas encontrados en los capítulos anteriores: la metodología MISITILEON.

Tras elegir el enfoque de la Seguridad como un servicio más ofrecido por MISITILEON, en este capítulo se detallan los procesos de Seguridad que se incorporan a la metodología.

- *Capítulo 5. CASO PRÁCTICO: SERVICIO DE SEGURIDAD MISITILEON. SISTEMA ANTIVIRUS.*

Se aplica la metodología al caso concreto de la gestión de un sistema antivirus.

- *Capítulo 6. COMPROBACIÓN DE LA METODOLOGÍA.*

En este capítulo se muestran estimaciones, así como datos reales que prueban la eficacia del modelo presentado: la metodología MISITILEON.

- *Capítulo 7. SISTEMA DE EVALUACIÓN DE CONOCIMIENTOS MISITILEON.*

En este capítulo se presenta la aplicación implementada para poder llevar a cabo evaluaciones sobre los conocimientos de las mejores prácticas de TI.

- *Capítulo 8. CONCLUSIONES Y LÍNEAS FUTURAS.*

Para finalizar, en este último capítulo de la tesis doctoral se muestran las conclusiones extraídas de toda la investigación realizada, así como las posibles líneas que quedan abiertas para seguir desarrollando en el futuro.

- *BIBLIOGRAFÍA*
- *ANEXOS*

1. *Metodologías.*
2. *Seguridad.*
3. *Ciclos de Vida.*
4. *ISO/IEC 27002:2005.*
5. *Fuentes y ejecutables de la aplicación "Sistema de Evaluación de Conocimientos MISITILEON" (sólo en formato electrónico).*

7. Observaciones generales

En esta tesis se ha intentado conservar la terminología castellana en la medida de lo posible. Sin embargo, se ha decidido mantener algunos términos en el idioma original de los documentos de referencia utilizados, especialmente para aquellos términos comúnmente extendidos que definen con exactitud un determinado concepto, y cuyo intento de traducción podría confundir, más que esclarecer, en su lectura.

Para la ortografía de esta tesis y las normas de estilo se han utilizado como referencia el Diccionario de la Real Academia Española en su vigésima segunda edición [RAE01], así como la Nueva Gramática de la Lengua Española [RAE09].

CAPÍTULO II. REVISIÓN DEL ESTADO DEL ARTE.

Los que se enamoran de la práctica sin la teoría son como los pilotos sin timón ni brújula, que nunca podrán saber a dónde van[11].

1. Introducción

Según los datos de un estudio presentado en 2008[12] por Dimension Data[13] [Ref Web 14] el 24% (66 de 370) de las organizaciones encuestadas por todo el mundo usaban ITIL. Dicha proporción de uso ha seguido aumentando de forma moderada. Cerca de dos tercios de los 370 responsables de TI (CIO) entrevistados[14] informaron sobre su compromiso con esta metodología. Como consecuencia, los niveles de utilización de otras mejores prácticas cayeron drásticamente después de ITIL.

Por ejemplo, la contratación de MOF y Six Sigma estaban en 17% (47 de 370) y 15% (41 de 370), respectivamente. Las contrataciones de Prince2, ISO, CMMi, CoBIT y TQM eran menores aún, en el rango de 10-12% y metodologías como Super y Agile estaban en el último lugar, con niveles de contratación de menos del 7%.

[11] Leonardo da Vinci.
[12] 24 de abril de 2008, en Madrid.
[13] Dimension Data (LSE:DDT) es un proveedor especializado de servicios y soluciones de Tecnologías de la Información (TI) que ayuda a sus clientes en el diseño, integración y soporte de sus infraestructuras de TI. Dimension Data aplica su experiencia en las tecnologías de redes, seguridad, entornos operativos, almacenamiento y tecnologías de centros de contacto combinadas con su capacidad de consultoría, integración y servicios gestionados para ofrecer soluciones personalizadas ajustadas a las necesidades de sus clientes.
[14] De 14 países de los 5 continentes.

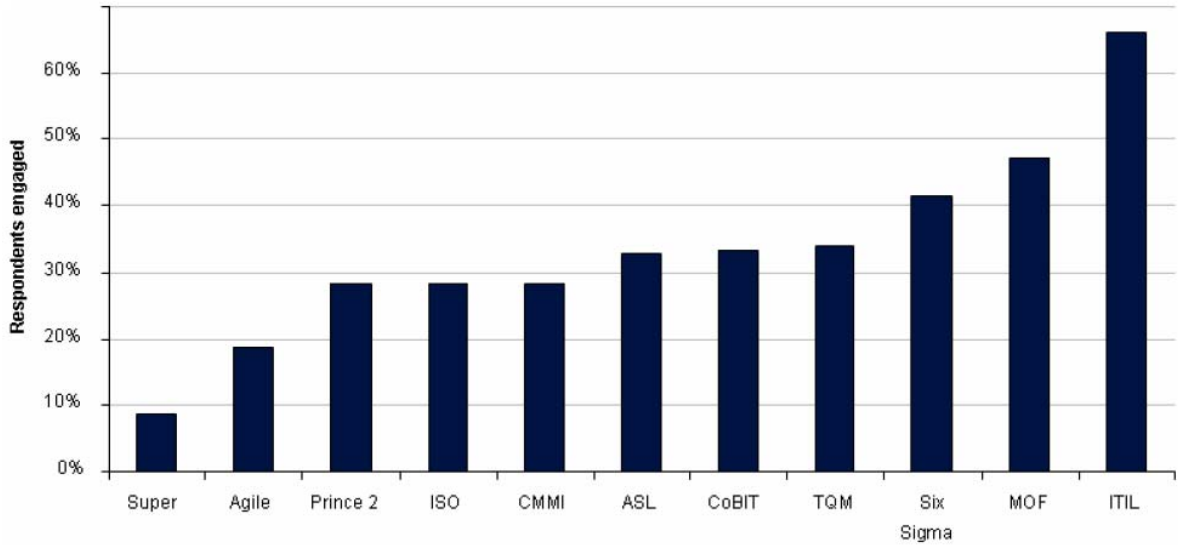


Figura 1.- **Contratación de Metodologías.**
(Fuente: Dimension Data)

Además, cuando a los mismos CIO se les pidió calificar las infraestructuras de mejores prácticas en términos de amplitud, claridad, relevancia y aplicabilidad en una escala del 1 al 5, ITIL sobresalió con una calificación global de 3. Asimismo, entre los resultados destacó que el tamaño de la organización tiene una fuerte influencia en la popularidad de ITIL y la inclinación de sus CIO por implementar esta infraestructura. Empresas con menos de 100 empleados (que típicamente tienen una estructura de TI menos compleja) rara vez contratan ITIL, mientras que el 87% de las empresas con más de 10.000 empleados han contratado esta metodología.

Por su parte, Scott Petty, director de servicios de Dimension Data [Ref Web 14] comenta que "construir vínculos entre los objetivos de negocio y la tecnología es el principal objetivo de las mejores prácticas de los servicios gestionados de TI. En todo el mundo, las organizaciones buscan alcanzar el potencial de estas mejores prácticas y están

examinando con mayor detenimiento dónde y cómo estos estándares pueden mejorar sus esfuerzos de TI".

Pero antes de profundizar en ITIL, se presentan algunos conceptos de vital importancia para entender el contexto en el que se va a trabajar.

2. Conceptos de Metodología

El proceso de construcción del software requiere, como en cualquier otra ingeniería, identificar las tareas que se han de realizar sobre el software y aplicar esas tareas de una forma ordenada y efectiva. El desarrollo del software es realizado por un conjunto coordinado de personas simultáneamente y, por lo tanto, sus esfuerzos deben estar dirigidos por una misma metodología que estructure las diferentes fases del desarrollo.

2.1. Definición de metodología de desarrollo software

El concepto de *metodología*, dentro de la Ingeniería del Software es, sin duda, uno de los que más confusión produce tanto en estudiantes como en profesionales involucrados en procesos de desarrollo de software [Ref Web 13].

En la literatura sobre este tema existen muchas definiciones sobre lo que es una metodología. Aquí se presentan algunas de las más populares.

- Definición de *Metodología* según la RAE: Ciencia del método. Conjunto de métodos que se siguen en una investigación científica o en una exposición doctrinal.

- Definición de *Método de Ingeniería del Software* según Pressman (5ª edición. 2001): Indican cómo construir técnicamente software. Los métodos abarcan una gran gama de tareas que incluyen análisis de requisitos, diseño, construcción de programas, pruebas y mantenimiento. Los métodos de la ingeniería del software dependen de un conjunto de principios básicos que gobiernan cada área de la tecnología e incluyen actividades de modelado y otras técnicas descriptivas.

Definición de *Metodología de Desarrollo Software* según la Wikipedia: Una metodología de desarrollo de software se refiere a un *framework*[15] que es usado para estructurar, planificar y controlar el proceso de desarrollo en sistemas de información.

El común denominador de todas ellas es la siguiente lista de características:

1. Define cómo se divide un proyecto en fases y las tareas que se deben realizar en cada una de ellas.
2. Especifica, para cada una de las fases, cuáles son las entradas que recibe y las salidas que produce.
3. Establece alguna forma de gestionar el proyecto.

[15] Marco de trabajo.

Sintetizando lo anterior, se define metodología de desarrollo software como un modo sistemático de producir software.

"En general aplicar una metodología por simple que sea, dará siempre mejores resultados que no aplicar ninguna"[16].

2.2. Finalidad de una metodología

Usando una metodología se pueden alcanzar los siguientes atributos en el producto final:

1. Eficacia:

El sistema satisface los requisitos del usuario.

2. Mantenibilidad:

Facilidad para realizar cambios una vez que el sistema está funcionando en la empresa del cliente.

3. Usabilidad:

Facilidad de aprender a manejar el sistema por parte de un usuario que no tiene por qué ser informático. (La resistencia de los usuarios a aceptar un sistema nuevo será mayor cuanto peor sea la usabilidad).

[16] Jesús María Minguet Melián.

4. Fiabilidad:

Probabilidad de que no ocurra un error durante un intervalo de tiempo dado. La diferencia con la corrección es que en este atributo interesa el tiempo, es decir, no se trata del número absoluto de defectos en el sistema sino de los que se manifiestan en un intervalo de tiempo.

5. Disponibilidad:

Probabilidad de que el sistema esté funcionando en un instante dado.

6. Corrección:

Baja densidad de defectos.

7. Eficiencia:

Capacidad del sistema de realizar su tarea con el mínimo consumo de recursos necesario.

2.3. Taxonomía de las metodologías

Existen dos grupos de metodologías en función de la mentalidad con la que se aborda un problema:

- Metodologías estructuradas
- Metodologías orientadas a objetos

2.3.1. Metodología estructurada

Constituyó la primera aproximación al problema del desarrollo de software. Está orientada a procesos, es decir, se centra en especificar y descomponer la funcionalidad del sistema.

La mentalidad que subyace al diseño estructurado es: ¿Cómo se puede dividir el sistema en partes más pequeñas que puedan ser resueltas por algoritmos sencillos y qué información se intercambian?

2.3.2. Metodología orientada a objetos

Constituye una aproximación posterior. Está basada en componentes, lo que significa que facilita la reutilización de código. De todos modos, hay que señalar que la reutilización de código es un tema complejo y que requiere en cualquier caso un diseño muy cuidadoso. Una metodología orientada a objetos no garantiza por sí misma la producción de código reutilizable, aunque lo facilita. Además, tiene la ventaja de que simplifica el mantenimiento debido a que los cambios están más localizados.

Este tipo de metodología cuenta con mayor número de desarrolladores y es previsible que termine sustituyendo completamente a la anterior.

La mentalidad que subyace al diseño orientado a objetos es: ¿Cuáles son los tipos de datos que hay que utilizar, qué características tienen y cómo se relacionan?

La orientación a objetos supone un paradigma distinto del tradicional (no necesariamente mejor o peor) que implica focalizar la atención en las estructuras de datos.

3. Metodologías y Normas más usadas

Las infraestructuras de las TI son el cimiento de los servicios del negocio, soportando los servicios TIC que se ofrecen a las organizaciones. A su vez estos servicios TIC deben estar apoyados por procesos de gestión de servicios, de forma que se garantice su entrega y calidad.

Se muestra una figura que esquematiza este escenario:

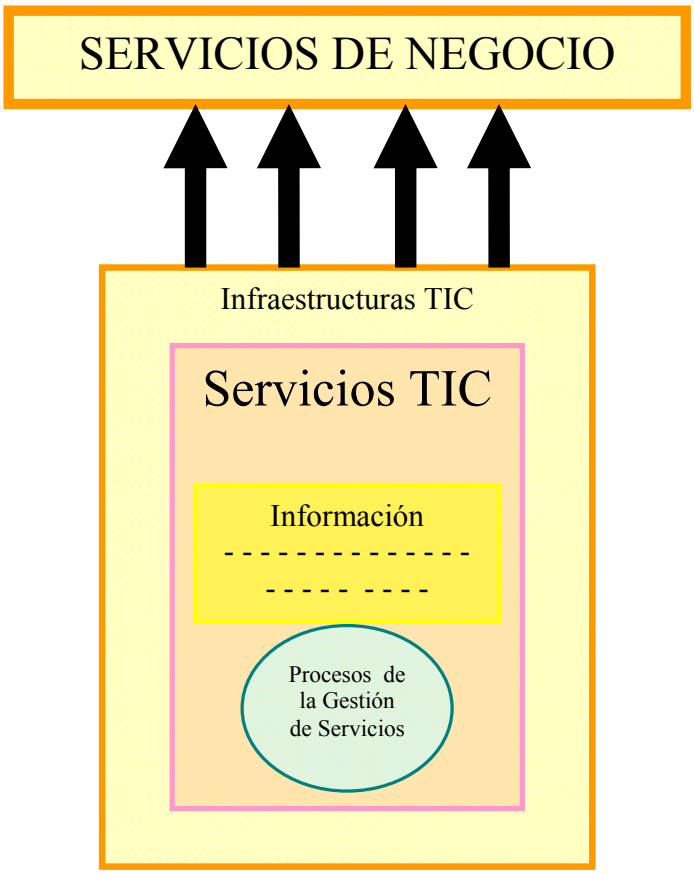


Figura 2.- **Diagrama de gestión de servicios en las TIC.**
(Fuente: propia)

La gestión de los servicios de las TI ve aumentada su complejidad según las infraestructuras, que soportan dichas TI, crecen y se diversifican. Será necesario realizar una gestión adecuada de los servicios, de tal forma que esta gestión permita proporcionarlos cumpliendo las necesidades de calidad especificadas por las organizaciones.

Las metodologías, estándares y buenas prácticas de desarrollo software más usadas actualmente son Orientadas a Objetos, siendo las principales ITIL, CMMi, COBIT.

3.1. ITIL

Lo primero que se debe aclarar es que ITIL no es ni una metodología, ni una norma, sencillamente es un compendio de buenas prácticas**.**

ITIL (*Information Technology Infrastructure Library*). Es un estándar de facto que proporciona un marco de trabajo configurable, basado en un compendio de buenas prácticas, sintetizadas en una serie de procesos consistentes, coherentes y entendibles para la gestión de servicios de las TI.

Seguidamente se describen sus características más importantes:

Estándar de facto: ITIL comenzó como un conjunto de procesos que utilizaba el gobierno del Reino Unido para mejorar la gestión de los servicios TI. Posteriormente ha sido adoptado por la industria como base de una gestión satisfactoria de los servicios TI, proporcionando un lenguaje común a la hora de la gestión de dichos servicios.

Marco de trabajo configurable: ITIL es un marco de trabajo, que describe las fronteras de la gestión de servicio en las organizaciones. Los procesos de ITIL son pensados para ser implantados de tal manera que apoyen pero no dicten los procesos de negocio de las organizaciones, son sólo directrices que permiten a las empresas moldear sus procesos para que se ajusten a sus propios requisitos empresariales

Compendio de buenas prácticas: Realmente es una colección de libros que reúnen una serie de mejores prácticas de la industria en materia de gestión de servicios de las TI.

Sintetizadas en una serie de procesos: La gestión de los servicios se basa en procesos comunes, roles y actividades, con unos objetivos y una referencia de comunicación entre ellos bien establecida, buscando siempre la mayor calidad en el servicio y su justificación en costo.

Gestión de servicios: Es el objetivo final de ITIL, realizar una provisión y soporte de servicios de alta calidad.

El siguiente esquema muestra esta relación entre los procesos de ITIL y la gestión de servicios en las TI.

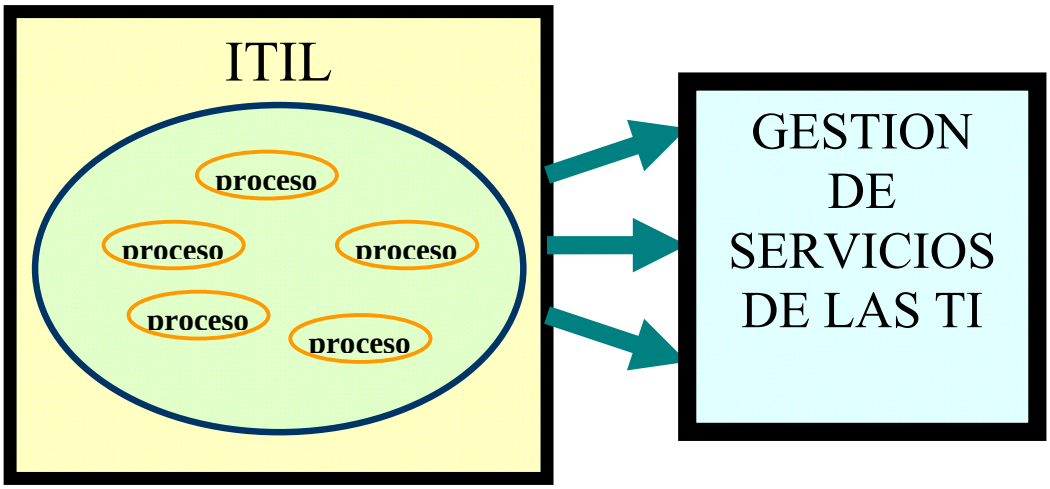


Figura 3.- **Diagrama de gestión de servicios en ITIL.**
(Fuente: propia)

En el siguiente capítulo se estudia ITIL en profundidad, presentando sus dos últimas y más conocidas versiones y se hace una comparativa de ambas, haciendo hincapié en las diferencias y mejoras que ofrece la última versión.

Todo lo relacionado con ITIL se discute en el foro itSMf. El itSMf es un foro internacional independiente y reconocido de Gestión de Servicios de TI, especializado en ITIL. La eurodiputada, catedrática de la UNED y exministra Pilar del Castillo, es la presidenta honorífica de dicha asociación de ITIL en su capítulo español[17].

Recientemente se publicó que la eurodiputada ayudará a introducir la metodología ITIL en el ámbito formativo. Tratará de difundir esta metodología en las universidades, bien sea a través de máster o incorporándolo a la licenciatura, y entre las administraciones

[17] Su página web es la siguiente: www.itsmf.es.

públicas. Según la exministra, España está mal en relación con aquellos países considerados puntales de Europa (Reino Unido, Alemania, Francia e Italia). Existe un problema de formación tecnológica que permita añadir valor añadido a los productos que luego vamos a exportar. Dice Pilar del Castillo que debemos estar en la vanguardia del desarrollo tecnológico, pero para ello es necesario dar un salto cualitativo en la formación [COMP08a].

3.2. CMMi

Capability Maturity Model Integration (CMMi) es un modelo para la mejora de procesos que proporciona a las organizaciones los elementos esenciales para procesos eficaces.

Las mejores prácticas CMMi se publican en los documentos llamados modelos.

La versión actual de CMMi es la versión 1.2. Hay tres constelaciones de la versión 1.2 disponible:

- CMMi para el Desarrollo (CMMi-DEV o CMMi *for Development*) Versión 1.2 fue liberado en agosto de 2006. En él se tratan procesos de desarrollo de productos y servicios.

- CMMi para la Adquisición (CMMi-ACQ o CMMi *for Acquisition*) Versión 1.2 fue liberado en noviembre de 2007. En él se tratan la gestión de la cadena de

suministro, adquisición y contratación externa en los procesos del gobierno y la industria.

- CMMi para Servicios (CMMi-SVC o CMMi *for Services*) está diseñado para cubrir todas las actividades que requieren gestionar, establecer y entregar servicios.

Dentro de la constelación CMMi-DEV, existen dos modelos:

- CMMi-DEV
- CMMi-DEV + IPPD (*Integrated Product and Process Development*)

Independientemente de la constelación/modelo por la que opta una organización, las prácticas CMMi deben adaptarse a cada organización en función de sus objetivos de negocio.

Las organizaciones no pueden ser certificadas en CMMi. Por el contrario, una organización es evaluada (por ejemplo, usando un método de evaluación como SCAMPI[18]) y recibe una calificación de nivel 1-5 si sigue los niveles de Madurez.

Un estudio más detallado de CMMi realizado por la doctorando se encuentra en el Anexo 1. Metodologías / CMMi.

[18] SCAMPI, *Standard CMMi Appraisal Method for Process Improvement.* Se puede ver más información en el Anexo 2. Metodologías / CMMi / SCAMPI.

3.3. COBIT

Como respuesta a las necesidades planteadas en los entornos de las TI, el marco de trabajo COBIT se creó con las características principales de ser orientado a negocios y a procesos, basado en controles e impulsado por mediciones.

COBIT e ITIL no son mutuamente excluyentes y pueden ser combinados para proporcionar un sólido marco de trabajo de gobierno, de control y mejores prácticas en gestión de servicios TI. Las empresas que deseen ampliar su marco de control y gobierno de las TI deberían utilizar COBIT [GAR02].

- ***Orientado al Negocio***

La orientación a negocios es el tema principal de COBIT. Está diseñado para ser utilizado no solo por proveedores de servicios, usuarios y auditores de TI, sino también y principalmente, como guía integral para la gerencia y para los propietarios de los procesos de negocio.

El marco de trabajo COBIT se basa en el siguiente principio: proporcionar la información que la empresa requiere para lograr sus objetivos, la empresa necesita administrar y controlar los recursos de TI usando un conjunto estructurado de procesos que ofrezcan los servicios requeridos de información. El marco de trabajo COBIT ofrece herramientas para garantizar la alineación con los requerimientos del negocio.

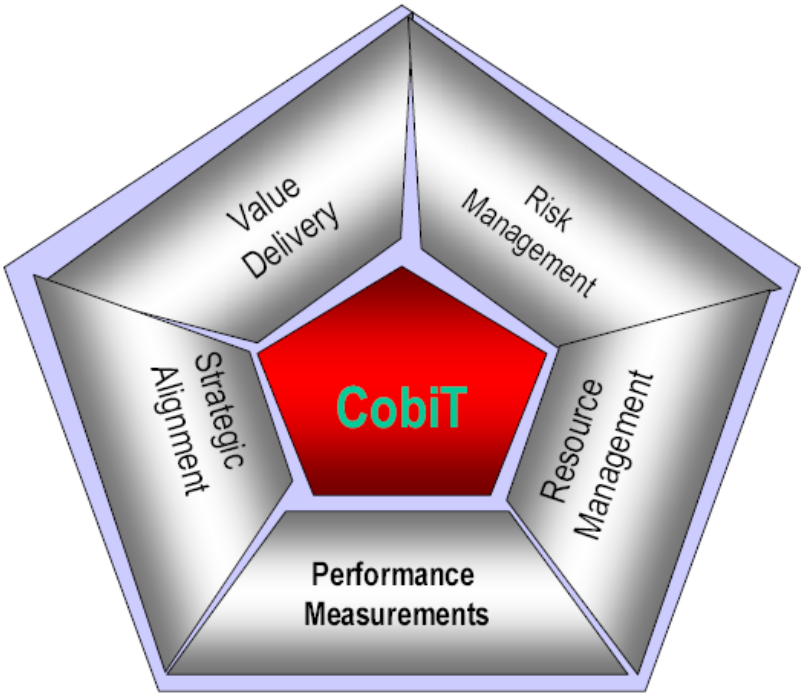


Figura 4.- **Áreas focales de COBIT.**
(Fuente: www.isaca.org/cobit/*)*

- ***Orientado a Procesos***

COBIT define las actividades de TI en un modelo genérico de procesos en cuatro dominios. Estos dominios son Planificar y Organizar, Adquirir e Implementar, Entregar y Dar Soporte y Monitorizar y Evaluar. Los dominios se equiparan a las áreas tradicionales de TI de planificar, construir, ejecutar y monitorizar. El marco de trabajo de COBIT proporciona un modelo de procesos de referencia y un lenguaje común para que cada uno en la empresa visualice y administre las actividades de TI. La incorporación de un modelo operacional y un lenguaje común para todas las partes de un negocio involucradas en TI es uno de los pasos iniciales más importantes hacia un buen gobierno. También brinda un marco de trabajo para la medición y monitorización del desempeño de TI, comunicándose

con los proveedores de servicios e integrando las mejores prácticas administrativas. Un modelo de procesos fomenta el desarrollo de procesos propios, permitiendo que se definan las responsabilidades. Para gobernar efectivamente las TIs, es importante determinar las actividades y los riesgos que requieren ser administrados.

♦ *Criterios de Información de COBIT*

Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT como requerimientos de información del negocio. Con base en los requerimientos de calidad, fiduciarios y de seguridad, se definieron los siguientes siete criterios de información:

• La 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.

• La eficiencia consiste en que la información sea generada optimizando los recursos (más productivo y económico).

• La confidencialidad se refiere a la protección de información sensitiva contra revelación no autorizada.

• La 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.

• La disponibilidad se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne con la protección de los recursos y las capacidades necesarias asociadas.

• El cumplimiento tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.

• La confiabilidad significa proporcionar la información apropiada para que la gerencia administre la entidad y ejercite sus responsabilidades fiduciarias y de gobierno.

Un estudio pormenorizado de COBIT realizado por la doctorando puede verse en el Anexo 1. Metodologías / Cobit.

3.4. ISO 20000

En 1989 la institución británica BSI (*British Standards Institution*) comenzó la definición de un estándar para la gestión de servicios TI, que finalizó con su publicación como estándar BS 15000 en 1995.

A partir de ese año BSI continuó con el desarrollo del estándar trabajando en una segunda parte, con el objetivo de profundizar en los conceptos de la parte 1 ya publicada. En la realización de aquel trabajo se identificó que sería muy beneficioso para el sector TI que las publicaciones que realizase BS estuvieran alineadas con las publicaciones ITIL de buenas prácticas, impulsadas por el Gobierno Británico. Como consecuencia de este interés

se formalizó un acuerdo de alineamiento del que BS 15000 se benefició de los contenidos de ITIL, y posteriormente cuando el estándar pasó a ser ISO/IEC 20000 fue éste quien ejerció su influencia en los contenidos de la nueva versión 3 de ITIL que se publicó en Mayo de 2007.

- ***Organización***

El estándar se organiza en dos partes:

- **Parte 1**: ISO/IEC 20000-1:2005 - Especificación. (Desarrollada por BSI como BS 15000-1)
- **Parte 2**: ISO/IEC 20000-2:2005 - Código de Prácticas. (Desarrollada por BSI como BS 15000-2)

La primera parte (Especificación) define los requerimientos (217) necesarios para realizar una entrega de servicios de TI alineados con las necesidades del negocio, con calidad y valor añadido para los clientes, asegurando una optimización de los costes y garantizando la seguridad de la entrega en todo momento. El cumplimiento de esta parte, garantiza además, que se está realizando un ciclo de mejora continuo en la gestión de servicios de TI. La especificación supone un completo sistema de gestión (organizado según ISO 9001) basado en procesos de gestión de servicio, políticas, objetivos y controles. El marco de procesos diseñado se organiza en base a los siguientes bloques:

- Grupo de procesos de Provisión del Servicio.
- Grupo de procesos de Control.
- Grupo de procesos de Entrega.
- Grupo de procesos de Resolución.
- Grupo de procesos de Relaciones.

A continuación se presenta un diagrama que refleja los distintos grupos de procesos existentes en la norma:

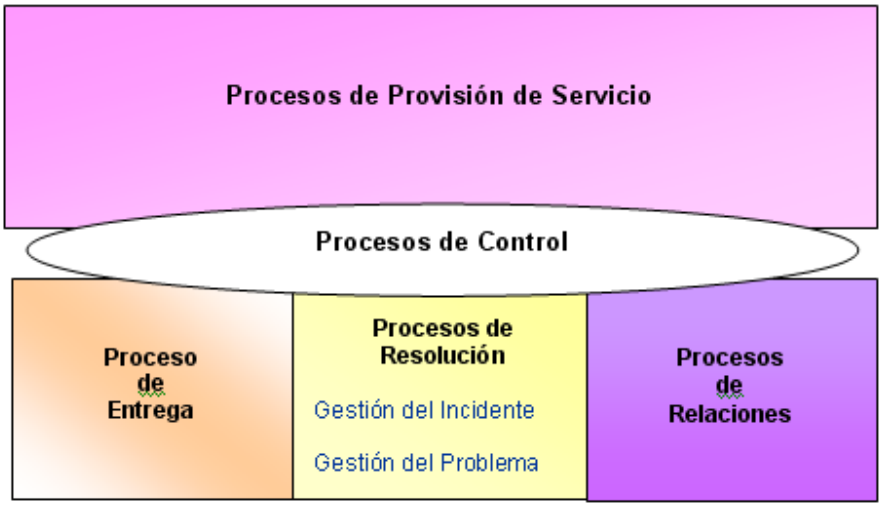


Figura 5.- **Procesos ISO 20000.**
(Fuente: www.itil-iso20000.com/)

La segunda parte (Código de Prácticas) representa el conjunto de mejores prácticas adoptadas y aceptadas por la industria en materia de Gestión de Servicio de TI. Está basada en ITIL y sirve como guía y soporte en el establecimiento de acciones de mejora en el servicio o preparación de auditorías del estándar ISO/IEC 20000-1:2005.

♦ ***Certificación***

La aparición de la serie ISO/IEC 20000, ha supuesto el primer sistema de gestión en servicio de TI certificable bajo norma reconocida a nivel mundial. Hasta ahora, las organizaciones podían optar por aplicar el conjunto de mejoras prácticas dictadas por ITIL (completadas por otros estándares como CMMi o CoBIT) o certificar su gestión contra el estándar local británico BS 15000. La parte 1 de la serie, ISO/IEC 20000-1:2005 representa el estándar certificable. En Febrero de 2006, AENOR[19] inició el mecanismo de adopción y conversión de la norma ISO/IEC 20000 a norma UNE. En Junio de 2006, la organización itSMf[20] hizo entrega a AENOR de la versión traducida de la norma. En el BOE del 25 de julio de 2007 ambas partes se ratificaron como normas españolas[21] con las siguientes referencias:

- UNE-ISO/IEC 20000-1:2007 Tecnología de la información. Gestión del servicio. Parte 1: Especificaciones (ISO/IEC 20000-1:2005).
- UNE-ISO/IEC 20000-2:2007 Tecnología de la información. Gestión del servicio. Parte 2: Código de buenas prácticas (ISO 20000-2:2005).

Un estudio más detallado de ISO 20000 realizado por la doctorando se encuentra en el Anexo 1. Metodologías / ISO 20000.

[19] Asociación Española de Normalización y Certificación. http://www.aenor.es/. Organización delegada en España de ISO/IEC.
[20] *Information Technology Service Management Forum*. http://www.itsmfi.org/. Que, como se explicó en el apartado 3.1.1. de este mismo capítulo, tiene también sede en España. http://www.itsmf.es/.
[21] Estas normas pueden adquirirse a través del portal web de AENOR. Cualquier entidad puede solicitar la certificación respecto a esas normas.

4. Ciclos de Vida

Al igual que otros sistemas de ingeniería, los sistemas de software requieren un tiempo y esfuerzo considerable para su desarrollo y deben permanecer en uso por un periodo mucho mayor. Durante este tiempo de desarrollo y uso, desde que se detecta la necesidad de construir un sistema de software hasta que éste es retirado, se identifican varias etapas (o fases) que en conjunto se denominan Ciclo de Vida del Software. En cada caso, en función de cuáles sean las características del proyecto, se configurará el ciclo de vida de forma diferente. Usualmente se consideran las siguientes fases: especificación y análisis de requisitos, diseño del sistema, implementación del software, aplicación y pruebas, entrega y mantenimiento. Un aspecto esencial (aunque muy olvidado) dentro de las tareas del desarrollo del software es la documentación de todos los elementos y especificaciones en cada fase.

Fases principales en cualquier ciclo de vida:

1. Análisis: se construye un modelo de los requisitos
2. Diseño: partiendo del modelo de análisis se deducen las estructuras de datos, la estructura en la que se descompone el sistema, y la interfaz de usuario.
3. Codificación: se construye el sistema. La salida de esta fase es código ejecutable.
4. Pruebas: se comprueba que se cumplen los criterios de corrección y calidad.
5. Mantenimiento: se asegura que el sistema siga funcionando y adaptándose a nuevos requisitos.

Las etapas se dividen en actividades que a su vez constan de tareas. Como se ha dicho, la documentación es una tarea importante que se realiza en todas las etapas y actividades. Cada etapa tiene como entrada uno o varios documentos procedentes de las etapas anteriores y produce otros documentos de salida según se muestra en la figura 6.

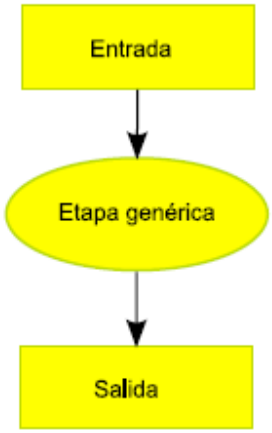


Figura 6.- **Etapa genérica.**
(Fuente: propia)

Algunos autores dividen la fase del diseño en dos partes: diseño global o arquitectónico y diseño detallado. En el primero se transforman los requisitos en una arquitectura de alto nivel, se definen las pruebas que debe satisfacer el sistema en su conjunto, se esboza la documentación y se planifica la integración. En el diseño detallado, para cada módulo se refina el diseño y se definen los requisitos del módulo y su documentación.

Las formas de organizar y estructurar la secuencia de ejecución de las actividades y tareas en las diferentes fases de cada uno de los métodos pueden dar lugar a un tipo de ciclo de vida diferente. Los principales ciclos de vida que se van a presentar a continuación

realizan todas las fases, actividades y tareas. Cada uno de ellos tiene sus ventajas e inconvenientes.

4.1. Ciclos de vida en cascada

El ciclo de vida inicialmente propuesto por Royce en 1970, fue adaptado para el software a partir de ciclos de vida de otras ramas de la ingeniería. Es el primero de los propuestos y el más ampliamente seguido por las organizaciones[22]. La estructura se muestra en la figura 7.

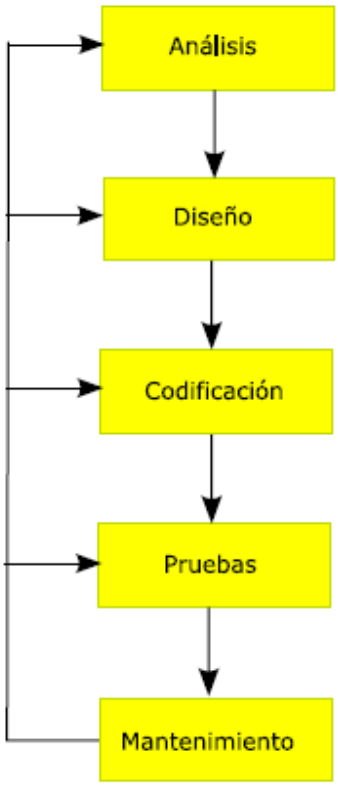


Figura 7.- **Ciclo de vida en cascada.**
(Fuente: propia)

[22] se estima que el 90% de los sistemas han sido desarrollados así.

♦ ***Descripción***

Este modelo admite la posibilidad de hacer iteraciones. Así por ejemplo, si durante el mantenimiento se ve la necesidad de cambiar algo en el diseño, se harán los cambios necesarios en la codificación y se tendrán que realizar de nuevo las pruebas, es decir, si se tiene que volver a una de las etapas anteriores al mantenimiento, se recorrerán de nuevo el resto de las etapas.

Después de cada etapa se realiza una revisión para comprobar si se puede pasar a la siguiente.

Trabaja en base a documentos, es decir, la entrada y la salida de cada fase es un tipo de documento específico. Idealmente, cada fase podría hacerla un equipo diferente gracias a la documentación generada entre las fases. Los documentos son:

- Análisis: Toma como entrada una descripción en lenguaje natural de lo que quiere el cliente. Produce el SRD (*Software Requirements Document*).
- Diseño: Su entrada es el SRD produce el SDD (*Software Design Document*).
- Codificación: A partir del SDD produce módulos. En esta fase se hacen también pruebas de unidad.
- Pruebas: A partir de los módulos probados se realizan la integración y pruebas de todo el sistema. El resultado de las pruebas es el producto final listo para entregar.

- ***Ventajas***

La planificación es sencilla.

La calidad del producto resultante es alta.

Permite trabajar con personal poco cualificado.

- ***Inconvenientes***

Lo peor es la necesidad de tener todos los requisitos al principio. Lo normal es que el cliente no tenga perfectamente definidas las especificaciones del sistema, o puede ser que surjan necesidades imprevistas.

Si se han cometido errores en una fase es difícil volver atrás.

No se tiene el producto hasta el final, esto quiere decir que:

- Si se comete un error en la fase de análisis no se descubre hasta la entrega, con el consiguiente gasto inútil de recursos.
- El cliente no verá resultados hasta el final, con lo que puede impacientarse.
- No se tienen indicadores fiables del progreso del trabajo (síndrome del 90 %[23]).
- Es comparativamente más lento que los demás ciclos de vida y el coste es mayor también.

[23] Consiste en creer que ya se ha completado el 90% del trabajo, pero en realidad queda mucho más porque el 10% del código da la mayor parte de los problemas.

- ***Tipos de proyectos para los que es adecuado***

Aquellos para los que se dispone de todas las especificaciones desde el principio, por ejemplo, los de reingeniería.

Se está desarrollando un tipo de producto que no es novedoso.

Proyectos complejos que se entienden bien desde el principio.

Como el modelo en cascada ha sido el más seguido ha generado algunas variantes. En el Anexo 3 se pueden ver las variantes más conocidas del Ciclo de Vida en Cascada.

4.2. Modelo de ciclo de vida en espiral

Propuesto inicialmente por Boehm en 1988. Consiste en una serie de ciclos que se repiten. Cada uno tiene las mismas fases y cuando termina da un producto ampliado con respecto al ciclo anterior. En este sentido es parecido al modelo incremental, la diferencia importante es que tiene en cuenta el concepto de riesgo. Un riesgo puede ser muchas cosas: requisitos no comprendidos, mal diseño, errores en la implementación, etc.

Una representación típica de esta estructura se muestra en la figura 8.

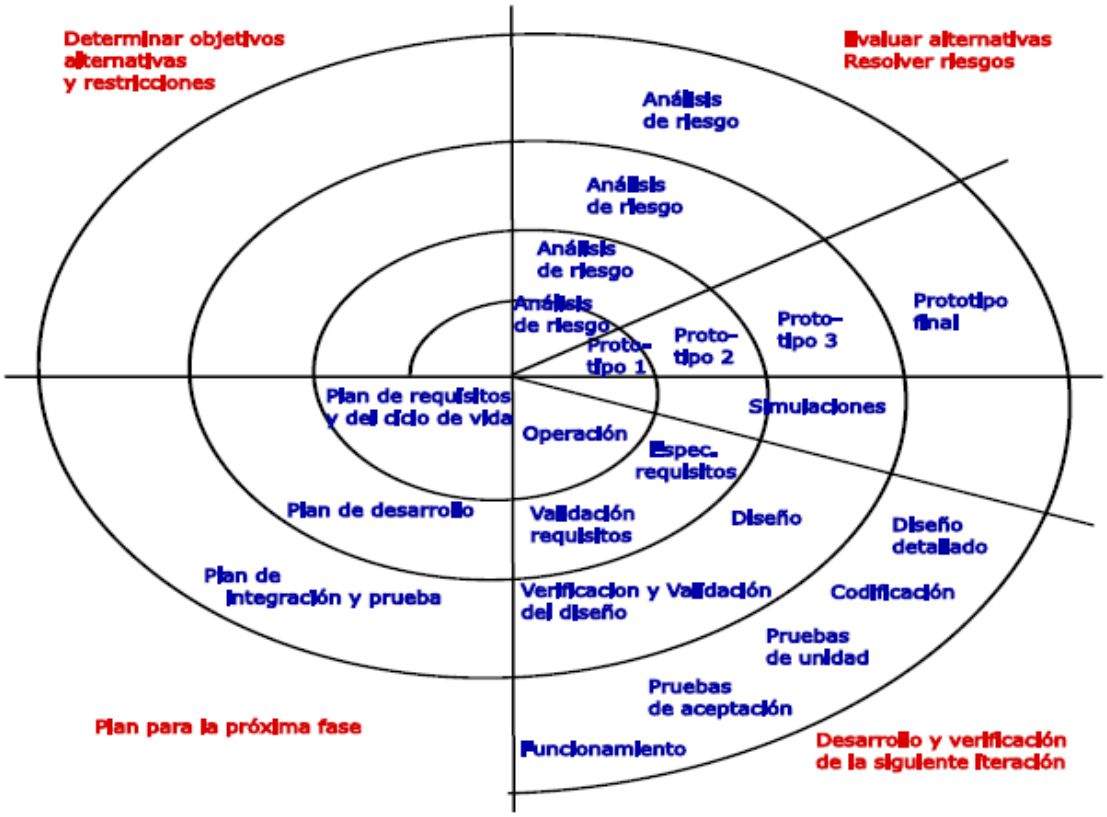


Figura 8.- **Ciclo de vida en espiral.**
(Fuente: propia)

♦ ***Descripción***

En cada iteración Boehm recomienda recopilar la siguiente lista de informaciones:

- Objetivos: se obtienen entrevistando a los clientes, haciendo cuestionarios, etc.
- Alternativas: son las diferentes formas posibles de conseguir los objetivos. Se consideran desde dos puntos de vista:
  - Características del producto.

  - Formas de gestionar el proyecto.
- Restricciones: son condiciones o limitaciones que se deben cumplir. Hay dos tipos:
  - Desde el punto de vista del producto: interfaces de tal o cual manera, rendimiento, etc.
  - Desde el punto de vista organizativo: coste, tiempo, personal, etc.
- Riesgos: es una lista de peligros de que el proyecto fracase.
- Resolución de riesgos: son las posibles soluciones al problema anterior. La técnica más usada es la construcción de prototipos.
- Resultados: es el producto que queda después de la resolución de riesgos.
- Planes: lo que se va a hacer en la siguiente fase.
- Compromiso: son las decisiones de gestión sobre cómo continuar.

Al terminar una iteración se comprueba que lo que se ha hecho efectivamente cumple con los requisitos establecidos; también se verifica que funciona correctamente. El propio cliente evalúa el producto. No existe una diferencia muy clara entre cuándo termina el proyecto y cuándo empieza la fase de mantenimiento. Cuando hay que hacer un cambio, éste puede consistir en un nuevo ciclo.

♦ ***Ventajas***

No necesita una definición completa de los requisitos para empezar a funcionar.

Es más fácil validar los requisitos porque se entregan productos desde el final de la primera iteración.

El riesgo de sufrir retrasos es menor, ya que al identificar los problemas en etapas tempranas hay tiempo de subsanarlos.

El riesgo en general es menor porque, si todo se hace mal, sólo se ha perdido el tiempo y recursos invertidos en una iteración (las anteriores iteraciones están bien).

- ***Inconvenientes***

Es difícil evaluar los riesgos.

Necesita de la participación continua por parte del cliente.

Cuando se subcontrata hay que producir previamente una especificación completa de lo que se necesita, y esto lleva tiempo.

- ***Tipos de proyectos para los que es adecuado***

Sistemas de gran tamaño.

Proyectos donde sea importante el factor riesgo.

Cuando no sea posible definir al principio todos los requisitos.

Los tipos de ciclos de vida que se han detallado hasta ahora en este apartado y en el Anexo 3 se han utilizado sobre todo en proyectos desarrollados con análisis y diseño estructurados.

El desarrollo de sistemas orientados a objetos tiene la particularidad de estar basados en componentes, que se relacionan entre ellos a través de interfaces, o lo que es lo mismo, son más modulares y por lo tanto el trabajo se puede dividir en un conjunto de mini-proyectos. Debido a todo esto, el ciclo de vida típico en una metodología de diseño orientado a objetos es el ciclo de vida en espiral.

Además de lo anterior, hoy en día existe una tendencia a reducir los riesgos y, en este sentido, el ciclo de vida en cascada no proporciona muchas facilidades.

En este memoria (por no hacerlo más extenso de lo necesario) sólo se verá un tipo de ciclo de vida orientado a objetos, que es además el más representativo: el modelo fuente.

4.3. Modelo fuente

Fue creado por Henderson-Sellers y Edwards en 1990. Es un tipo de ciclo de vida pensado para la orientación a objetos y posiblemente el más seguido.

Un proyecto se divide en las fases:

1. Planificación del negocio.

2. Construcción: es la más importante y se divide a su vez en otras cinco actividades: planificación, investigación, especificación, implementación y revisión.

3. Entrega o liberación.

La primera y la tercera fase son independientes de la metodología de desarrollo orientado a objetos.

Además de las tres fases, existen dos periodos:

1. Crecimiento: es el tiempo durante el cual se construye el sistema.

2. Madurez: es el periodo de mantenimiento del producto. Cada mejora se planifica igual que en el periodo anterior, es decir, con las fases de Planificación del negocio, Construcción y Entrega.

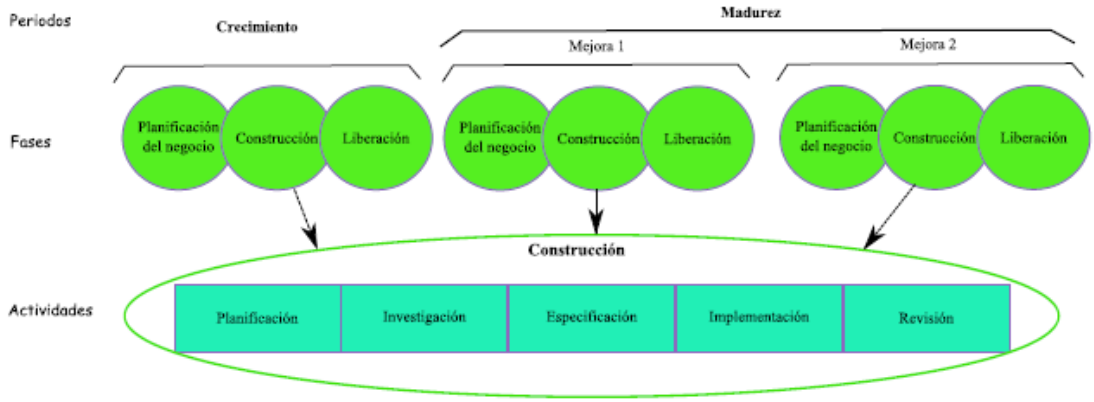


Figura 9.- **Ciclo de vida fuente.**
(Fuente: propia)

Cada clase puede tener un ciclo de vida sólo para ella debido a que cada una puede estar en una fase diferente en un momento cualquiera. La ventaja es que permite un desarrollo solapado e iterativo. En la figura 9 se muestra un esquema de este tipo de ciclo de vida.

5. Seguridad en la TI

Actualmente, la información es un activo de vital importancia para el éxito de cualquier organización, sea cuál sea la entidad de ésta. La dependencia que tienen los negocios de las TIC obliga a la búsqueda de métodos, técnicas y medios que ayuden a mantener la seguridad y el funcionamiento correcto de los SI que utilizan tales tecnologías. Asegurar dicha información, así como la de los sistemas que la soportan o comunican debe ser un objetivo prioritario para la organización.

La seguridad de los SI se apoya principalmente en tres conceptos: disponibilidad, integridad y confidencialidad. Para mantener estos conceptos en un nivel aceptable es necesario dedicar recursos y presupuesto económico, lo que convierte al mantenimiento de la seguridad en una tarea de gestión [TOR05].

La creciente dependencia de las empresas, y de la sociedad en general, de las TIC, así como el entorno cada vez más complejo en que éstas se desarrollan, ha provocado la aparición de vulnerabilidades en los recursos utilizados, que deben minimizarse con las medidas de seguridad oportunas.

Algunos de los aspectos que han contribuido a la mencionada complejidad son entre otros:

- Las soluciones de movilidad (portátiles, PDAs, teléfonos móviles,…).

- La utilización de la red (Internet) para el comercio electrónico.
- La creciente utilización de los sistemas distribuidos.
- La mayor complejidad de los procesos.
- El número de usuarios y su ubicación dispersa.
- La proliferación de intercambio de archivos por correo electrónico.

La dirección de la empresa ha de tomar conciencia de la trascendencia de la seguridad y de los riesgos que supone su ausencia o una "seguridad a medias". El primer paso será saber qué amenazas existen para decidir cómo eliminarlas, disminuir su riesgo y/o su impacto, a través de controles, defensas y protecciones, es decir, mecanismos de salvaguarda en general.

"El concepto de Seguridad debe de estar presente en todas las fases del ciclo de vida, desde el inicio hasta el final[24]".

5.1. El concepto de Seguridad en los Sistemas de Información

En el presente apartado se recopilan las definiciones de "*seguridad*" más extendidas aplicadas a los SI.

En términos generales, la seguridad es una característica de cualquier sistema que indica que dicho sistema está libre de riesgos y que es "invulnerable". No obstante, no se

[24] Jesús María Minguet Melián.

puede garantizar la existencia de sistemas infalibles, por lo que en lugar del término de *seguridad* se debería utilizar el término *fiabilidad*. Entendiendo por fiabilidad la probabilidad de que un sistema de información se comporte de la forma esperada en todo momento.

En realidad se debería hablar de vulnerabilidad, y no de seguridad.

La RAE define seguridad como:

"Dicho de un mecanismo: Que asegura algún buen funcionamiento, precaviendo que este falle, se frustre o se violente."

A pesar de todo lo anterior, aunque sea incorrecto hablar de seguridad, en esta tesis doctoral se hablará de seguridad (por ser de uso común).

El estándar internacional ISO/IEC 9126 define la *seguridad* en los sistemas de información como:

"La capacidad del producto software para proteger información y datos, de forma que personas y sistemas no autorizados no puedan leerlos o modificarlos, y no se niegue el acceso a éstos a personas y sistemas autorizados."[25]

[25] Traducción propia del texto original [ISO01].

Otra interesante definición de seguridad es la de Tomas Olovsson[26] extraída de su informe [OLO92]:

"la seguridad se define como la posibilidad de un sistema de proteger objetos con respecto a la confidencialidad e integridad."[27]

Donde un *objeto* se define como un componente pasivo del sistema que engloba la información y los recursos del sistema asociados a esta información[28].

La definición de seguridad más extendida es la que presentó Charles P. Pfleeger[29] en 1997; en su libro defiende [PFL97]:

Para que un SI pueda permanecer "seguro" es necesario que éste presente sus tres propiedades esenciales. Estas propiedades se denominan comúnmente CIA[30]:

[26] Tomas Olovsson ocupa el cargo de CTO en la compañía "*AppGate Network Security*", cuyo negocio está orientado a ofrecer soluciones VPN (*Virtual Private Network*), para extender el concepto de e-security a empresas, redes, y sistemas en Internet. Además, Olovsson ejerce como "*Research Assistent*" en el departamento de "*Computer Engineering*" de la universidad *Chalmers University of Technology* (Göteborg, Suecia). Algunas de sus publicaciones más conocidas son "A *quantitative Model of the Security Intrusion Process Based on Attacker Behavior*" y "*A Structured Approach to Computer Security* " (ver [OLO92]).

[27] Traducción propia extraída a partir del documento original "*A Structured Approach to Computer Security*", ver página 4 de [OLO92].

[28] Como por ejemplo CPU, espacio en disco, espacio en memoria, programas, etc.

[29] Charles P. Pfleeger ha ocupado, desde 1997, el cargo de "Master Security Architect" en la compañía Exodus Communications Inc (Vienna, VA), en la cual desempeña funcionas de análisis y consultoría sobre seguridad para clientes comerciales y gubernamentales. Anteriormente, Charles P. Pfleeger ocupó diferentes cargos relacionados con la seguridad. En particular de 1988 a 1992 fue profesor en el departamento de "*Computer Science*" en la universidad de Tennessee (Knoxville, TN). En 1997 Pfleeger publicó el libro "*Security in Computing*" ([Pfl97]), considerado el libro de texto estándar para los cursos de seguridad de la información en las universidades americanas.

[30] Confidencialidad, Integridad y Disponibilidad (*Confidentiality, Integrity, Availability*).

• *Confidencialidad*

La confidencialidad es la propiedad de la seguridad que permite que los objetos de un sistema solo sean accesibles por elementos autorizados.

• *Integridad*

La integridad es la propiedad que permite que los objetos de un sistema sólo puedan modificarse por elementos autorizados.

• *Disponibilidad*

La disponibilidad es la propiedad que indica que los objetos de un sistema deben ser accesibles para los elementos autorizados.

Además, en los SI conectados en red se deben garantizar dos propiedades adicionales:

• *Autentificación*

La autentificación es la propiedad que permite garantizar formalmente la identidad de las entidades participantes en una transacción.

• *No-repudio.*

El no-repudio es la propiedad que evita que las entidades de una transacción puedan negar su participación en la misma.

Por tanto, la seguridad se podría considerar como el conjunto de mecanismos y procedimientos que garantizan esas cinco propiedades de los elementos del SI.

No obstante, otros estudios [OLO92], [LAP92] desglosan la seguridad en sólo dos características elementales: *confidencialidad* e *integridad*. Siendo la *disponibilidad*, la *confiabilidad* y la *precaución* características de un nivel de abstracción superior denominado *formalidad*. Donde la *precaución* se define como la probabilidad de que un sistema desempeñe las funciones esperadas o falle sin provocar consecuencias catastróficas y la *formalidad* se describe como la calidad del servicio proporcionado por el sistema de información.

Además de estas características generales, los SI para mantener un nivel adecuado de seguridad han de cumplir en mayor o menor grado los siguientes requisitos:

- Responsabilidad. El sistema de seguridad debe ser capaz de asociar positivamente un proceso con su fuente de autorización, de modo que los usuarios sean los responsables de las acciones que realizan.

- Auditabilidad (Rastreabilidad). Todos los sistemas de seguridad deben proporcionar estadísticas acerca de entradas al sistema, uso de recursos, las acciones por cada usuario, etc.
- Reclamación de origen. Constituye la contrapartida del servicio anterior, en el sentido de que permite probar quién es el creador de un determinado documento.
- Reclamación de propiedad. Este servicio permite probar que un determinado documento electrónico es de propiedad de un usuario particular. Se usa en transacciones mercantiles, donde la posesión de un documento concede determinados derechos a su poseedor.
- Certificación de fechas. En las comunicaciones electrónicas este servicio es el equivalente al certificado de fecha y/u hora a la que se ha realizado o entregado un determinado documento.

El nivel de seguridad requerido por un SI estará en función de factores tales como:

- Localización geográfica de los usuarios.
- Topología de la red de comunicaciones.
- Instalaciones o salas donde residen los equipos informáticos.
- Equipo físico que soporta el SI.
- Configuración del equipo lógico básico.
- Tipo y estructura de las bases de datos.
- Forma de almacenamiento de los datos.

- Número y complejidad de los procesos a realizar.

Después de todo lo comentado, finalmente se podría afirmar que:

"Un sistema es seguro cuando realiza el objetivo para el cual ha sido diseñado, sin fallo."[31]

No obstante, en esta tesis se adopta el enfoque clásico de Charles P. Pfleeger por ser éste el más extendido.

5.2. Normativas y Estándares de Seguridad

Es incuestionable que para poder mantener una adecuada gestión de la seguridad de la información es necesario disponer de un sistema que normalice dicha gestión, de forma que estén claramente evaluados los riesgos a los que está sometida la información en la organización, así como que esos riesgos sean correctamente traducidos en objetivos de seguridad. Finalmente, estos objetivos deberán cumplirse mediante las consiguientes funciones de seguridad que los materialicen.

Con estas premisas, las organizaciones ISO[32] e IEC[33] elaboran una serie de estándares que pretenden cubrir el apartado de la gestión de la seguridad en las organizaciones.

[31] Aportación de Jesús Mª Minguet Melián, profesor titular de "Ingeniería del Software y Sistemas Informáticos" de la Universidad Nacional de Educación a Distancia.

5.2.1. Serie ISO/IEC 27000

Es un conjunto de estándares desarrollados, o en fase de desarrollo, por ISO e IEC, que proporcionan un marco de gestión de seguridad de la información utilizable por cualquier tipo de organización, ya sea, pública o privada, y cualquiera que sea su entidad.

La responsable del nacimiento de estas normas fue BSI[34], organización británica, que se jacta de ser la primera entidad de normalización a nivel mundial (desde 1901), y que es la responsable de la publicación de normas tan importantes como:

- BS 5750 de 1979[35], ahora ISO 9001.
- BS 7750 de 1992[36], ahora ISO 14001.
- BS 8800 de 1996[37], ahora OHSAS 18001 (*Occupational Health and Safety Management Systems*).

Para encontrar las raíces de la serie 27000 hay que remontarse al 1995 y la norma BS7799 de la propia BSI, cuyo principal objetivo era dotar a las empresas de un conjunto de buenas prácticas que aplicar, a la hora de gestionar la seguridad de la información.

La norma BS 7799, se subdivide en dos normas, según la fecha de publicación:

- BS 7799-1 de 1995, que establece una guía de buenas prácticas, pero que no constituye un esquema de certificación.

[32] *International Organization for Standardization.*
[33] *International Electrotechnical Comisión.*
[34] *British Standards Institution*.
[35] Normativa de gestión de la calidad.
[36] Normativa de gestión ambiental.
[37] Normativa de gestión y seguridad en el trabajo.

- BS 7799-2 de 1998, donde ya sí, se establecen los requisitos de un SGSI (Sistema de Gestión de Seguridad de la Información)[38] para que éste pueda ser certificado como tal.

La norma BS 7799, en sus dos partes, sigue evolucionando, y es sometida a una revisión en 1999, de forma que la norma BS 7799-1 es adoptada por ISO como la norma ISO 17799, sin cambios fundamentales.

Posteriormente la norma BS 7799-2 es nuevamente revisada, en el 2002, para adaptarse a la filosofía adoptada por ISO en materia de sistemas de gestión.

Es así que en el 2005 nace, a partir de la norma BS 7799-2, la norma ISO 27001, como estándar de certificación, así como se revisa y actualiza la norma ISO 17799, renombrándose ésta como ISO 27002:2005. Véase un esquema que aclare esta evolución:

[38] En inglés "*Information Security Management System*", ISMS.

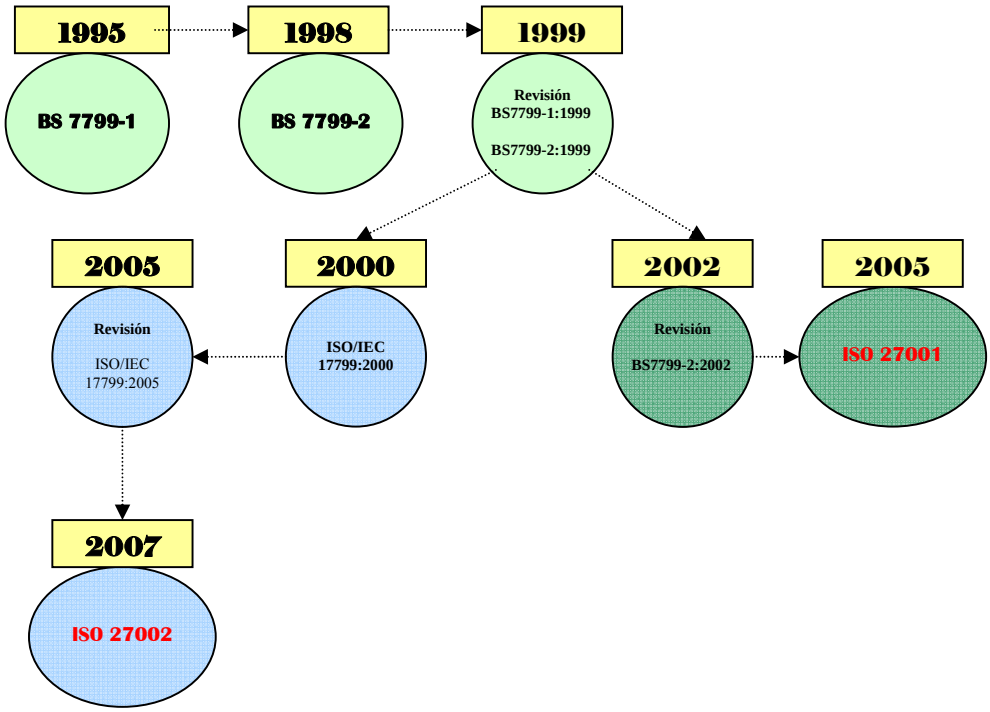


Figura 10.- **Diagrama de evolución de las normas ISO 27001 e ISO 27002.**
(Fuente: ISO27000)

La serie ISO/IEC 27000 está constituida por una serie de estándares, todos ellos referidos a la seguridad de la información, reservándose dicha numeración: 27000 para tal propósito.

- Las normas, muchas de las cuales están en desarrollo, van desde la especificación de requisitos para poder acreditar un sistema, hasta guías técnicas específicas de conceptos como la gestión de riesgos o el uso de sistemas de telecomunicaciones. Seguidamente, y considerando que son de especial interés los contenidos de cada una de ellas, se presenta una breve descripción de toda la serie ISO 27000 [Ref Web 15].

- **ISO 27000:** Su fecha prevista de publicación es Noviembre de 2008. Contendrá términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión[39].

- **ISO 27001:** Publicada el 15 de Octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. Sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 (nueva numeración de ISO 17799:2005 desde el 1 de Julio de 2007), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados. Desde el 28 de Noviembre de 2007, esta norma está publicada en España como UNE-ISO/IEC 27001:2007 y puede adquirirse online en AENOR (Asociación Española de Normalización y Acreditaciones).

- **ISO 27002:** Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que

[39] Como dato curioso, considerar que esta norma está previsto que sea gratuita, a diferencia de las demás de la serie, que tienen un coste.

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. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO 27002:2005.

- **ISO 27003:** Su fecha prevista de publicación es Mayo de 2009. Consistirá en una 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. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

- **ISO 27004:** Su fecha prevista de publicación es Noviembre de 2008. Especificará las métricas y las 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:** Su fecha prevista de publicación es Mayo de 2008. Consistirá en una guía de técnicas para la gestión del riesgo de la seguridad de la información y servirá, por tanto, de apoyo a la ISO27001 y a la implantación de un SGSI. Recogerá partes de ISO/IEC TR 13335.

- **ISO 27006:** Publicada el 1 de Marzo de 2007. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA[40]-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma[41].

- **ISO 27007:** Su fecha prevista de publicación es Mayo de 2010. Consistirá en una guía de auditoría de un SGSI.

- **ISO 27011:** Su fecha prevista de publicación es Enero de 2008. Consistirá en una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU (Unión Internacional de Telecomunicaciones).

- **ISO 27031:** Su fecha prevista de publicación es Mayo de 2010. Consistirá en una guía de continuidad de negocio en cuanto a TI y comunicaciones.

- **ISO 27032:** Su fecha prevista de publicación es Febrero de 2009. Consistirá en una guía relativa a la *ciberseguridad*.

[40] *European Accreditation*.
[41] En España, esta norma aún no está traducida. El original en inglés puede adquirirse en ISO.org.

- **ISO 27033:** Su fecha prevista de publicación es entre 2010 y 2011. 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 puertas de acceso, acceso remoto, aseguramiento de comunicaciones en redes mediante Redes Privadas Virtuales y diseño e implementación de seguridad en redes. Provendrá de la revisión, ampliación y renumeración de ISO 18028.

- **ISO 27034:** Su fecha prevista de publicación es Febrero de 2009. Consistirá en una guía de seguridad en aplicaciones.
- **ISO 27799:** Su fecha prevista de publicación es 2008. Es un estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 17799 (actual ISO 27002).[42]

A continuación se presenta una tabla con las principales normas de la serie ISO/IEC 27000, publicadas o en fase de desarrollo, en el momento de este trabajo:

[42] Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215.

Norma	Descripción	Publicación
ISO 27000	Términos y definiciones de la serie 27000	**Noviembre 2008**
ISO 27001	Requisitos de un Sistema de Gestión de Seguridad de la Información (SGSI)	**Octubre 2005**
ISO 27002	Guía de buenas prácticas de la seguridad de la información	**Julio 2007**
ISO 27003	Guía de implementación de un SGSI	**Mayo 2009**
ISO 27004	Métricas y técnicas de medidas de la eficacia de un SGSI y controles relacionados	**Noviembre 2008**
ISO 27005	Guía de técnicas para la gestión del riesgo de la seguridad de la información	**Mayo 2008**
ISO 27006	Requisitos para la acreditación de entidades de auditoría y certificación de SGSI	**Marzo 2007**
ISO 27007	Guía de auditoría de un SGSI	**Mayo 2010**
ISO 27011	Guía de la gestión de la seguridad de la información especifica para telecomunicaciones	**Enero 2008**
ISO 27031	Guía de continuidad del negocio referida a las TI	**Mayo 2010**
ISO 27032	Guía relativa a la *ciberseguridad*	**Febrero 2009**
ISO 27033	Guía de la gestión de la seguridad en redes	**2010-2011**
ISO 27034	Guía de seguridad en aplicaciones	**Febrero 2009**
ISO 27799	**Guía de la gestión de seguridad en el sector sanitario**	**2008**

Tabla 1 .- Normas ISO/IEC 27000.
(Fuente: ISO27000)

5.2.2. ISO 27001 (SGSI)

La norma ISO 27001 tiene su origen en la norma BS 7799-2:2002 y se publicó en Octubre del 2005.

Se podría decir que es la norma principal de la serie, ya que tiene una completa descripción de los Sistemas de Gestión de Seguridad de la Información, pudiendo considerar actualmente a dichos sistemas, como el mejor medio para asegurar la calidad de la seguridad de la información.

En esta norma, además del Objeto, campo de aplicación, terminología y definiciones, se define de forma clara cómo crear, implantar, operar, supervisar, revisar, mantener y mejorar el SGSI, así como los requisitos de documentación y control de dichos sistemas.

Importante también es, la descripción de las responsabilidades de la dirección, en cuanto a gestión de provisión de recursos, concienciación y formación del personal y gestión del proceso periódico de revisiones.

En la norma ISO 27001 también se definen la forma de realizar auditorias internas a los SGSI, así como acciones correctivas y preventivas para su mejora continua.

Un SGSI, trata de ser un proceso sistemático, documentado y conocido por toda la organización, para gestionar la seguridad de la información desde un enfoque de riesgo empresarial.

Garantizar un nivel de protección total, la llamada seguridad plena, es prácticamente imposible, por tanto, el propósito del sistema de gestión de seguridad, debe ser, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización, todo esto, de forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Para realizar estas funciones, y en el ámbito de la gestión de la calidad (ISO 9001), podría decirse que un SGSI está formado por el siguiente modelo:

Figura 11.- **Modelo de niveles de un SGSI.**
(Fuente: ISO27000)

Estos niveles se pueden desglosar en las siguientes funcionalidades:

Nivel del documento	Descripción del nivel
1	**Estratégico: alcance, objetivos, responsabilidades, políticas y directrices principales.**
2	**Operativo: referentes a la planificación, operación y control de los procesos de seguridad de la información.**
3	**Técnico: describiendo las tareas y actividades a realizar.**
4	**Registro: evidencia objetiva del cumplimiento de los objetivos del SGSI.**

Tabla 2 .- Funcionalidades de los niveles de un SGSI.
(Fuente: ISO27000)

La forma de establecer y gestionar un SGSI, siempre tomando como referencia la norma ISO 27001, es utilizando el ciclo continuo PDCA:

P: *Plan→* (**Planificar**: establecer el SGSI).

D: *Do→* (**Hacer**: implementar y utilizar el SGSI).

C: *Check→* (**Verificar**: monitorizar y revisar el SGSI)

A: *Act→* (**Actuar**: mantener y mejorar el SGSI)

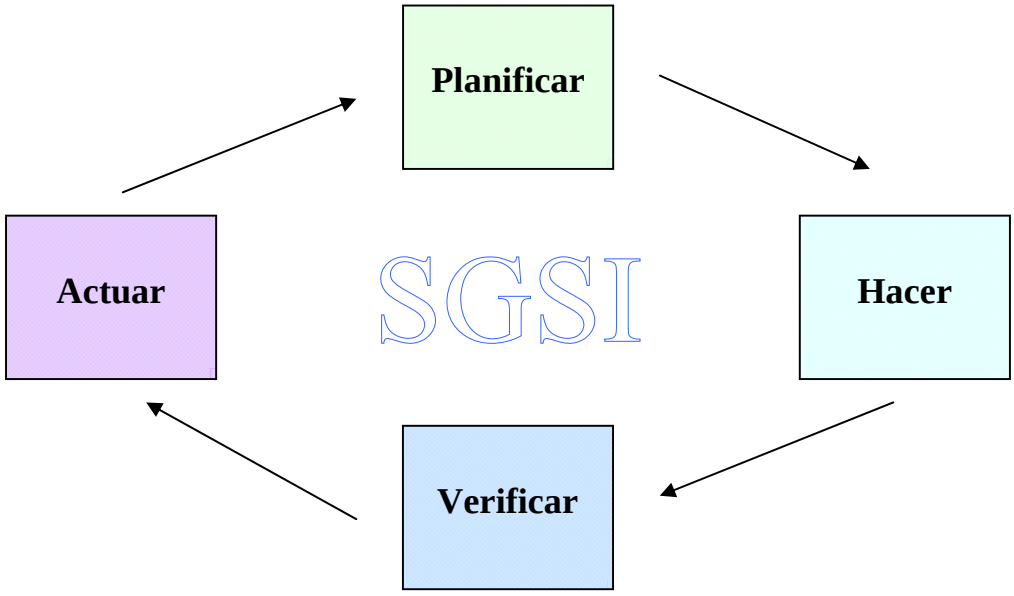


Figura 12.- **Ciclo PDCA de un SGSI.**
(Fuente: www.ISO27001security.com)

Como consecuencia del entendimiento de que ITIL no toma como uno de sus focos principales la gestión de la seguridad de la información, y la ya contrastada aceptación de la norma ISO 27001 (ésta sí, orientada específicamente hacia dicha gestión de la seguridad) parece evidente la necesidad de establecer una clara relación entre ambas. De esta forma, además de resultar dos enfoques complementarios, aquellas organizaciones que hayan optado por implantar un modelo ITIL, verán facilitada de forma significativa la implantación de su SGSI, así como los controles de seguridad que se deriven.

Esta asociación ITIL-SGSI se deriva de diversos puntos comunes en ambos planteamientos, y facilita entre otros la adopción de un enfoque consistente y unificado de identificación y control de riesgos, uno de los principales pilares sobre los que descansa el éxito en la implantación de un SGSI.

Concretando en este beneficio obtenido en la Gestión de riesgos, es de destacar un elemento fundamental que mana de la gestión ITIL: El conocimiento actualizado y suficientemente detallado de TODOS los activos de la organización, así como las relaciones, pesos y dependencias entre ellos. Estos activos son manejados en ITIL, desde el proceso de la Gestión de Configuración (Soporte de Servicio) y mediante el uso de la base de datos global para toda la TI denominada CMDB (*Configuration Management Data Base*).

Disponer de un repositorio actualizado de activos, la CMDB, facilita el Análisis de Riesgos, parte fundamental en la fase de Planificación del SGSI, y que se utilizará como elemento de medida clave, a la hora de definir y evaluar los controles de seguridad a implantar.

Véase un gráfico que representa esta relación entre SGSI e ITIL:

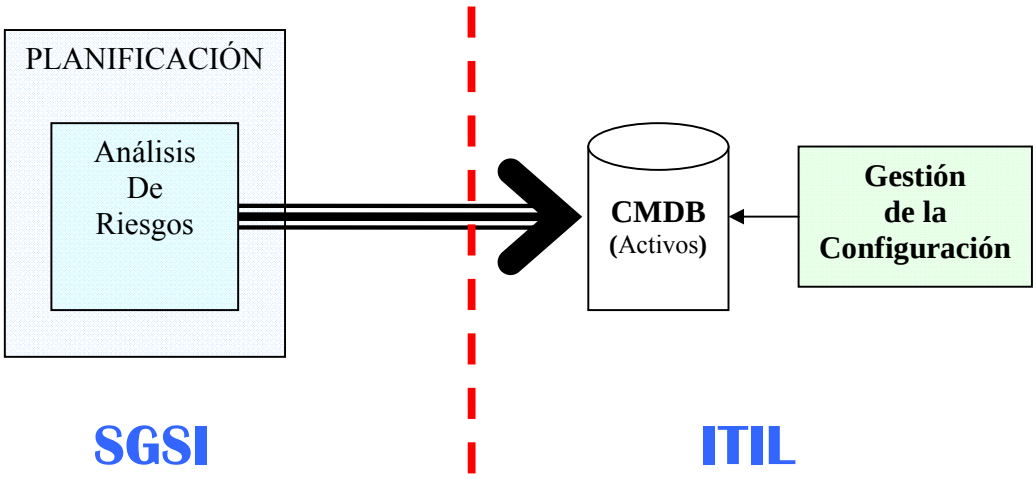


Figura 13.- **Relación entre SGSI e ITIL.**
(Fuente: propia)

5.2.3. ISO 27002 (ISO/IEC 17799)

La norma ISO/IEC 17799, desde Julio del 2007, se denomina ISO 27002, aunque mantiene el año de edición de la primera, esto es, 2005. En España, existe una publicación nacional UNE-USO/IEC 17799, elaborada por el AEN/CTN 71 (Comité Técnico de Normalización) y titulada: *Código de buenas prácticas para la Gestión de la Seguridad de la Información*.

Se hace referencia concreta a esta norma por su especial correlación con ITIL, es así que, al igual que éste, contiene una guía de buenas prácticas para la gestión de la seguridad de la información, si bien, ISO 27002 está orientada al desarrollo, implantación y mantenimiento de un SGSI, mientras que, como ya sabemos ITIL se constituye en un concepto más amplio de la gestión del servicio de las TI.

La norma ISO 27002 se basa principalmente en la definición de una serie de objetivos de control, así como de los controles de seguridad necesarios para poder cumplir dichos objetivos de control de la seguridad. Concretamente define 39 objetivos de control y 133 controles de seguridad, distribuidos por las siguientes 11 secciones, también llamadas dominios:

- Política de seguridad
- Aspectos organizativos para la seguridad
- Clasificación y control de activos
- Seguridad ligada al personal
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de accesos
- Desarrollo y mantenimiento de sistemas
- Gestión de incidentes de seguridad de la información
- Gestión de continuidad de negocio
- Conformidad

El detalle de la norma se puede consultar en el Anexo 4. Normativa ISO/IEC 27002:2005.

5.3. Tipos de Virus Informáticos

Todos los virus tienen en común una característica, y es que crean efectos perniciosos. A continuación se presenta una clasificación de los virus informáticos, basada en el daño que causan y efectos que provocan.

- ***Caballo de Troya***

Es un programa dañino que se oculta en otro programa "legítimo", y que produce sus efectos perniciosos al ejecutarse este último. En este caso, no es capaz de infectar otros archivos o soportes, y sólo se ejecuta una vez, aunque es suficiente (en la mayoría de las ocasiones) para causar su efecto destructivo.

- ***Gusano o Worm***

Es un programa cuya única finalidad es la de ir consumiendo la memoria del sistema. Se copia así mismo sucesivamente, hasta que desborda la RAM, siendo ésta su única acción maligna.

- ***Virus de macros***

Los virus de macros[43] afectan a archivos y plantillas que los contienen, haciéndose pasar por una macro y actuando hasta que el archivo se abra o utilice.

[43] Una macro es una secuencia de órdenes de teclado y ratón asignadas a una sola tecla, símbolo o comando. Son muy útiles cuando este grupo de instrucciones se necesitan repetidamente.

- ***Virus de sobreescritura***

Este tipo de virus sobreescribe en el interior de los archivos atacados, haciendo que se pierda el contenido de los mismos.

- ***Virus de programa***

Comúnmente infectan archivos con extensiones .exe, .com, .ovl, .drv, .bin, .dll, y .sys (los dos primeros son atacados más frecuentemente por que se utilizan más).

- ***Virus de boot***

Son virus que infectan sectores de inicio y "booteo" (*Boot Record*) de los diskettes y el sector de arranque maestro (*Master Boot Record*) de los discos duros; también pueden infectar las tablas de particiones de los discos.

- ***Virus residentes***

Se colocan automáticamente en la memoria de la computadora y desde ella esperan la ejecución de algún programa o la utilización de algún archivo.

- ***Virus de enlace o directorio***

Modifican las direcciones que permiten, a nivel interno, acceder a cada uno de los archivos existentes; como consecuencia no es posible localizarlos y trabajar con ellos.

- ***Virus mutantes o polimórficos***

Son virus que mutan, es decir cambian ciertas partes de su código fuente haciendo uso de procesos de encriptación y de la misma tecnología que utilizan los antivirus. Debido a estas mutaciones, cada generación de virus es diferente a la versión anterior, dificultando así su detección y eliminación.

- ***Virus falso o Hoax***

Los denominados virus falsos en realidad no son virus, sino cadenas de mensajes distribuidas a través del correo electrónico y las redes. Estos mensajes normalmente informan acerca de peligros de infección de virus, los cuales en su mayoría son falsos y cuyo único objetivo es sobrecargar el flujo de información a través de las redes y el correo electrónico de todo el mundo.

- ***Virus Múltiples***

Son virus que infectan archivos ejecutables y sectores de "booteo" simultáneamente, combinando en ellos la acción de los virus de programa y de los virus de sector de arranque.

El vertiginoso avance de las comunicaciones, la conexión entre las computadoras, las posibilidades de transmisión de datos entre ellas, y sobre todo la creación y uso de la red Internet, hace de los virus informáticos uno de los principales riesgos a los que está sometida la seguridad de la información en las organizaciones.

Especial relevancia toma este aspecto si se tiene en cuenta que el ritmo de crecimiento es de diez nuevos virus por día, y no existe ningún programa detector de virus que sea perfecto, capaz de proteger totalmente a un sistema, es decir, no existe un algoritmo universal que detecte y elimine todo tipo de virus.

Parece obvio que, unos de los servicios de seguridad más importantes a aportar a la organización, será la implantación y mantenimiento de un completo sistema antivirus que proteja a los sistemas de dicha organización de cualquier software dañino o malicioso.

Como se acaba de señalar, debido a la continua creación y propagación de nuevo software malicioso, un sistema antivirus requiere tanto de una correcta definición y configuración, como de una serie de funciones de mantenimiento y actualización continuadas, que mantengan los sistemas lo más protegidos posible.

Aun así, estos sistemas antivirus no son perfectos, por propia definición existe el virus antes que el antivirus, por lo tanto es necesario definir procedimientos de actuación inmediata ante la aparición de virus, así como procedimientos de contingencia y recuperación, para el caso de que produzcan efectos perniciosos en la organización.

Es importante reseñar que un sistema antivirus, como casi todos los sistemas relacionados con la seguridad, requiere de la concienciación y colaboración del usuario, ya que una de las principales técnicas utilizadas por los virus es la ingeniería social, por ejemplo, “tentando” al usuario a abrir un fichero, un correo con nombre o algún otro motivo sugestivo. Debe incluirse, por tanto, dentro del sistema antivirus, así como reflejarse

en la política general de la empresa, un procedimiento de actuación del usuario ante la evidencia o sospecha de que un virus puede haberse introducido en la organización.

CAPÍTULO III. REVISIÓN CRÍTICA DE ITIL.

Hemos aprendido a vivir en un mundo de errores y productos defectuosos como si fueran necesarios para vivir. Es hora de adoptar una nueva filosofía…[44]

Un estudio dado a conocer por CA (*Computer Associates*) [COM08b] ha revelado que la implantación de las buenas prácticas de ITIL en las organizaciones redunda en un aumento general del rendimiento de los departamentos de TI encuestados, especialmente en lo referido a cambios, configuraciones y versiones. Igualmente, el informe ofrece argumentos que apoyan la adquisición de tecnologías que permitan la aplicación de estas mejores prácticas en gestión de servicios TI, incluyendo una CMDB[45], herramientas de seguridad de las operaciones o aplicaciones de gestión de versiones.

Así, las ventajas que se obtienen como resultado de las mejores prácticas tienen que ver con una mayor utilización de los recursos TI, mayor satisfacción del usuario final y la reducción del riesgo global que conlleva la gestión de cambios.

De acuerdo con el estudio, el mayor impacto de ITIL se produce en el ámbito del proceso de desarrollo, prueba y recuperación de estados anteriores de las versiones. Y es que el control y la supervisión de los cambios por sí solos no son suficientes para asegurar la gestión efectiva del servicio TI; hace falta ir más allá y centrarse en unas prácticas de gestión de versiones más rigurosas.

[44] W. Edwards Deming (1900-93).
[45] *Configuration Management Data Base*, Base de Datos de Gestión de la Configuración.

Por su parte, si se cuenta con una implantación de procesos de gestión de cambios e incidentes basados en una CMDB, se resuelven un 28 por ciento más de incidentes dentro de los plazos de los acuerdos de nivel de servicio, ya que supone una gestión efectiva de las TI en aspectos como cambios de configuración no autorizados, ratio de versiones recuperadas o ratio de incidentes resueltos dentro de los límites de los acuerdos de nivel de servicio.

Además, para crear una cultura que gire en torno a los procesos, las organizaciones que han obtenido los mejores resultados en el citado estudio han gestionado diligentemente las excepciones a los procesos, y sus directivos TI aplican la máxima de que seguir un proceso es algo básico que se espera de todos los miembros del departamento de TI.

Finalmente, una configuración efectiva del sistema (que suele alcanzarse cuando se identifican y utilizan sólo las configuraciones aprobadas de los sistemas de producción) es otro de los factores característicos de un entorno informático estable y seguro. Todo ello sin olvidar el control de accesos, que también es una mejor práctica clave para los roles y responsabilidades, segregación de tareas adecuada y un acceso restringido al entorno de producción [COM08b].

A continuación se presenta un estudio pormenorizado, realizado a lo largo de los años de estudio de la doctorando, de qué es ITIL.

1. ITIL

La *Information Technology Infrastructure Library* (Biblioteca de Infraestructura de Tecnologías de Información), abreviada como ITIL, es un marco de trabajo configurable, basado en un compendio de las **mejores prácticas**, destinadas a facilitar la entrega de servicios de TI de alta calidad.

Una definición de mejores prácticas podría ser la de Aidan Lawes[46] [Ref web 33]: "*una manera de hacer las cosas o un trabajo, aceptado ampliamente por la industria y que funciona correctamente...*"

A pesar de no poder considerar a ITIL como el modelo de referencia perfecto para la Gestión de Servicios TI, sí se puede decir que es el **estándar de facto** a nivel mundial y que ha sido adoptado por grandes compañías de gestión de servicios de ámbito nacional e internacional[47]. Además ITIL está empezando a aparecer por fin en los planes de estudio de muchas universidades de todo el mundo.

En la Figura 14 se especifica la ubicación de ITIL en un entorno de TI.

[46] CEO de itSMf.
[47] Como por ejemplo multinacionales como IBM, HP, Microsoft, etc.

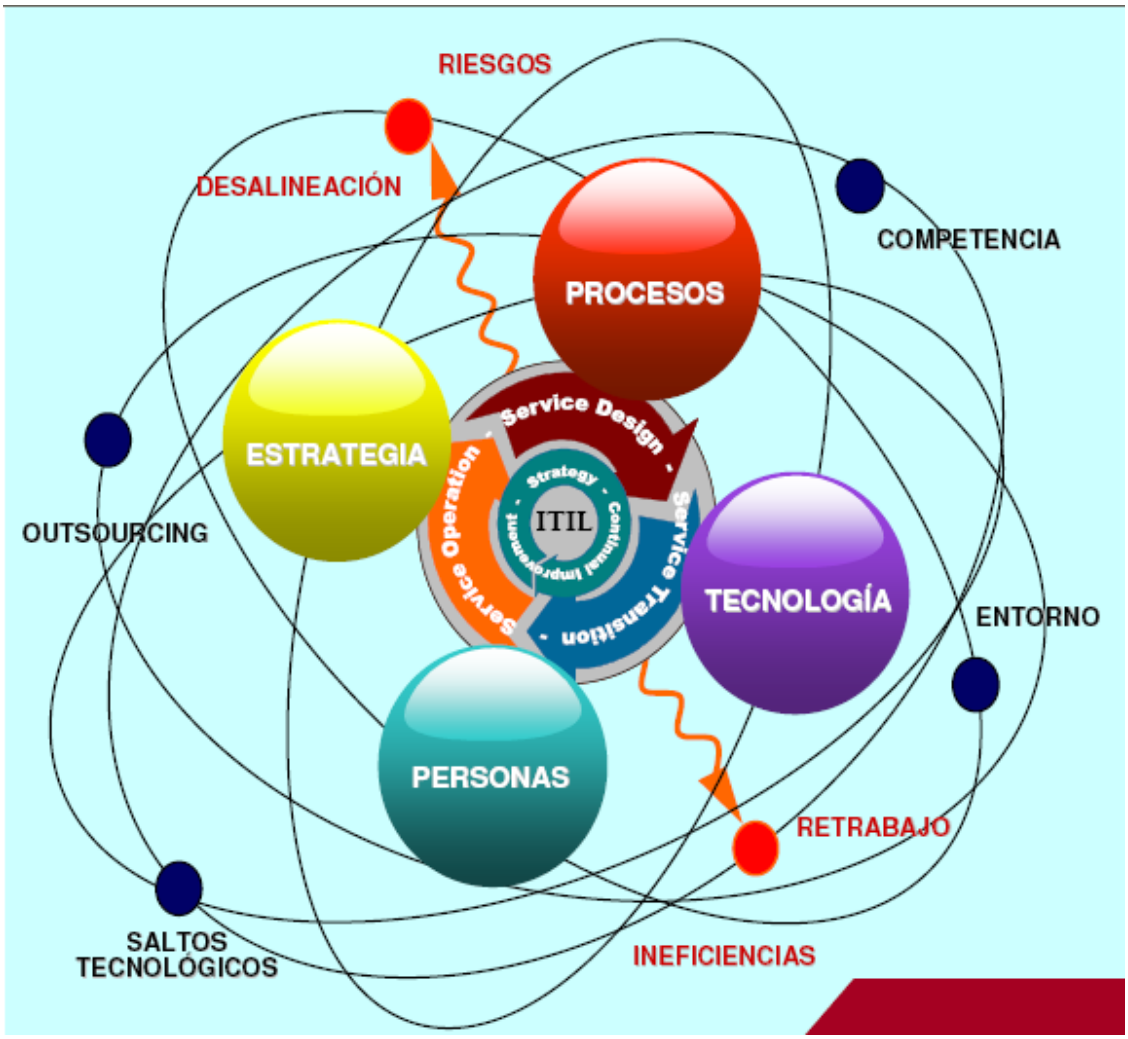


Figura 14.- **ITIL.**
(Fuente: OGC)

1.1. Historia de ITIL

Las recomendaciones de ITIL fueron desarrolladas en los años 80 por la CCTA[48] del gobierno británico como respuesta a la creciente dependencia de las TI y al reconocimiento de que sin prácticas estándar, los contratos de las agencias estatales y del sector privado creaban independientemente sus propias prácticas de gestión de TI y

[48] *Central Computer and Telecommunications Agency.*

duplicaban esfuerzos dentro de sus proyectos TIC[49], lo que resultaba en mayor número de errores y mayores costes [Ref Web 16].

Realmente los principios de ITIL nacen cuando el gobierno británico se planteó la necesidad de convertir en externas algunas de las áreas de informática de ciertas organizaciones gubernamentales. En ese momento se dieron cuenta de que no había nada que permitiera expresar claramente qué servicios querían hacer externos y cómo querían que se organizara esa provisión de servicios y la relación entre los proveedores, los responsables del gobierno y los usuarios de los servicios.

Así que comenzaron a desarrollar una serie de recomendaciones al respecto de cómo se debía organizar un área de informática alrededor del concepto de servicio TI y enfocada a la provisión de estos servicios TI al usuario final.

Esta biblioteca ha ido evolucionando y mejorando con el paso del tiempo. Poco a poco ha ido ganando seguidores y se ha ido consolidando su uso en organizaciones de todo tipo y tamaño.

[49] Nótese cómo en este párrafo el autor diferencia el concepto TI del concepto ampliado, TIC.

ITIL se construyó en torno al modelo de control y de gestión de las operaciones atribuido a Deming,[50] y fue publicado como un conjunto de libros, cada uno dedicado a un área específica dentro de la Gestión de TI.

Lo que actualmente se conoce como ITIL versión 1 surgió a principios de los 80, desarrollado bajo el auspicio de la CCTA, se tituló Método de Infraestructura de la Tecnología de Información del Gobierno[51], y durante varios años terminó expandiéndose hasta 31 libros[52]. Las publicaciones cambiaron de título, principalmente motivado por el deseo[53] de que fueran vistas como una guía y no como un método formal, y como resultado del creciente interés que había fuera del gobierno británico.

Para hacer a ITIL más accesible y menos costoso, para aquellos que deseasen explorarlo, uno de los objetivos del proyecto de actualización (la versión 2) fue agrupar los libros según unos conjuntos lógicos destinados a tratar los procesos de administración que cada uno cubre. De esta forma, diversos aspectos de los sistemas de TIC, de las aplicaciones y del servicio se presentan en conjuntos temáticos.

[50] William Edwards Deming (14 de octubre de 1900 - 20 de diciembre de 1993). Estadístico estadounidense, profesor universitario, autor de textos, consultor y difusor del concepto de calidad total. Su nombre está asociado al desarrollo y crecimiento de Japón después de la Segunda Guerra Mundial.
[51] En inglés "*Government Information Technology Infrastructure Method",* GITIM.
[52] dentro de un proyecto inicialmente dirigido por Peter Skinner y John Stewart.
[53] Fundamentalmente de Roy Dibble de la CCTA.

En diciembre de 2005, la Oficina de Comercio Gubernamental[54] (OGC) anunció la actualización a ITIL versión 3, publicándose ésta en mayo de 2007. La publicación de ITIL versión 3 incluye cinco libros principales, concretamente: Estrategia del Servicio (*Service Strategy*), Diseño del Servicio (*Service Design*), Transición del Servicio (*Service Transition*), Operación del Servicio (*Service Operation*) y Mejora Continua del Servicio (*Service Improvement*) consolidando buena parte de las prácticas actuales de la versión 2 en torno al Ciclo de Vida del Servicio.

Los nombres ITIL e *IT Infrastructure Library* son marcas registradas de la OGC, una división del Ministerio de Hacienda del Reino Unido [Ref Web 16].

1.2. Certificaciones

ITIL es una certificación para individuos y por tanto permite a una persona estar acreditada en sus distintos grados. Prueba que un individuo puede recibir un curso, entender los procesos y luego articular sus habilidades de forma adecuada en un examen.

[54] En inglés *Office of Government Commerce.*

Por lo tanto, una organización o sistema de gestión no puede certificarse como «conforme a ITIL», aunque si ha implementado las guías de ITIL sobre Gestión de los Servicios de TI puede lograr certificarse bajo la ISO/IEC 20000[55].

Los particulares pueden conseguir varias certificaciones oficiales ITIL. Hasta el año pasado, los estándares de calificación ITIL eran gestionados por la ICMB (*ITIL Certification Management Board*) que agrupaba a la OGC, a *itSMF International* (*IT Service Management Forum*) y a los dos Institutos Examinadores existentes hasta entonces: EXIN[56] (*Examination Institute for Information Science*) e ISEB[57] (*ITIL Service Management Qualification*). Actualmente todo el entorno de certificación lo gestiona APM Group Limited, quedando EXIN e ISEB como meros intermediarios.

Hasta el año 2000 se habían emitido unos 60.000 certificados de ITIL, y en el año 2006 ya se había llegado a una cifra de 500.000 certificados [ITS08].

Existen tres niveles de certificación para profesionales en ITIL versión 2:

a) *Foundation Certificate* (Certificado Básico):

Acredita un conocimiento básico de ITIL en gestión de servicios de TI y la comprensión de la terminología propia de ITIL. Está destinado a aquellas personas que deseen conocer las buenas prácticas especificadas en ITIL.

[55] De la que se ha hecho una síntesis detallada en el capítulo anterior.
[56] Con sede en los Países Bajos.
[57] Con sede en el Reino Unido.

b) *Practitioner's Certificate* (Certificado de Responsable):

Destinado a quienes tienen responsabilidad en el diseño de procesos de administración de departamentos de TI y en la planificación de las actividades asociadas a los procesos.

c) *Manager's Certificate* (Certificado de Director):

Garantiza que quien lo posee dispone de profundos conocimientos en todas las materias relacionadas con la administración de departamentos de TI, y lo habilita para dirigir la implantación de soluciones basadas en ITIL.

En cambio para certificarse en ITIL versión 3, el sistema es bastante más complejo. Existe un curso "puente", el *Foundation Bridging Course,* para aquellos profesionales que ya están certificados en Fundamentos de la versión anterior.

También pueden obtenerse hasta 11 certificaciones específicas para esta versión[58], pero los 4 niveles principales son los siguientes:

◊ Nivel Fundamentos

◊ Nivel Intermedio

◊ Experto en ITIL

◊ Profesional Avanzado de Gestión de Servicios de TI

[58] Se puede consultar toda esta información en www.exin.nl.

En cambio, con ISO 20000 es la organización la que alcanza ese nivel de acreditación de que puede ofrecer calidad y valor. ISO 20000 es también un estándar de relevancia en el caso del outsourcing de servicios. Probablemente una organización no externalice toda su TI, pero puede que sí lo haga con algunas redes, *mainframes*, almacenamiento, etc, así que dicha organización quiere calidad de los suministradores que le están ayudando con su red de valor. Lo puede medir con métricas (que seguramente lo hará) pero también quiere una acreditación de que tienen procesos de calidad. Y ahí es donde entra ISO 20000 porque permite vincular a los suministradores de la red de valor con la organización, de forma que puede garantizar que los servicios que finalmente ofrece dicha compañía tienen calidad [STR09].

A continuación se desarrollan las dos versiones más importantes de ITIL hasta la fecha, la versión 2, por ser hasta el momento la más extendida[59], y la versión 3 que representa el presente más actual, aunque parece que pronto va a quedar atrás porque ya se está hablando mucho de la inminencia de la futura versión 4 de ITIL. Además, itSMf ha anunciado que a partir del mes de junio de 2010 no certificarán más en ITIL versión 2.

[59] La OGC está considerando y evaluando un plazo para retirar (terminar) las certificaciones de ITIL v2. Los certificados seguirán siendo válidos después de la fecha que se acuerde, pero no será posible hacer exámenes en dicha versión. En 2008 se había acordado terminar las certificaciones de v2 el último día de junio de 2009, no obstante muchas regiones han reclamado que todavía requieren de la v2 y OGC está considerando dos opciones: eliminar la v2 en una sola fecha, o hacerlo en fechas diferentes según el territorio. Para tomar la decisión ha pedido a itSMf Internacional que le ayude a responder a una encuesta en la que se procesarán los resultados por región. [Ref Web 6]

2. ITIL v2

En este apartado se presenta la versión más conocida y extendida de ITIL: ITIL v2[60].

2.1. Historia

A principios de la primera década del 2000 comienza la publicación de la segunda versión de ITIL (ITIL Versión 2) consolidando su posicionamiento en el mercado.

Las mejores prácticas ITIL ofrecen un conjunto completo de prácticas que abarca no sólo los procesos y requisitos técnicos y operacionales, sino que se relaciona con la gestión estratégica, la gestión de operaciones y la gestión financiera de una organización moderna, aunque es importante aclarar que el tema de Gestión de Servicios (Soporte del Servicio y Entrega del Servicio) es el más ampliamente difundido e implementado.

Donde más se desarrolla ITIL v2 es en los libros de Entrega del Servicio[61] y Soporte del Servicio[62]. En estos dos libros se plantea un modelo de procesos que tiene que dar lugar a una provisión y soporte de servicios TIC ordenada y alineada con las necesidades del

[60] aunque su retirada ha sido anunciada para finales de este año 2010.
[61] En Inglés *Service Delivery*.
[62] En Inglés *Service Support*.

negocio, de tal forma que el área de Informática centre su atención y sus esfuerzos en aquello que realmente es importante para la organización. De la lectura de dichos libros se derivan dos posibles enfoques u orientaciones:

1º.- Desde el punto de vista del **proceso**, como síntesis de las buenas prácticas descritas en ITIL.

2º.- Desde el punto de vista del **cliente**, es decir, de aquel que demanda el servicio, y por tanto la calidad acordada de dicho servicio.

2.2. Orientación a Procesos

En este aspecto, los libros centrales de Soporte y Provisión de Servicios plantean un modelo de procesos compuesto por 10 procesos centrales que se encargan de realizar todas las actividades relativas al soporte de los servicios (en un planteamiento muy operativo y orientado al día a día) y a la provisión de los servicios (en un planteamiento un poco más táctico y con visión de futuro).

PROCESOS ITIL v2 (Soporte y Entrega del Servicio)	
Castellano	***Inglés***
Gestión de la Configuración	*Configuration Management*
Gestión del Incidente	*Incident Management*
Gestión del Problema	*Problem Management*
Gestión del Cambio	*Change Management*
Gestión de la Versión	*Release Management*
Gestión Financiera	*Financial Management*
Gestión de la Capacidad	*Business capacity Management*
Gestión de la Disponibilidad	*Availability Management*
Gestión de la Continuidad	*Business Continuity Management*
Gestión del Nivel de Servicio	*Service Level Management*

Tabla 3 .- Principales procesos ITIL.
(Fuente: propia)

2.3. Orientación a Clientes

Clientes y Usuarios ITIL		
	Cliente	**Usuario**
Objetivo	Buscan la mejor relación calidad-precio	**Buscan la mejor prestación del servicio**
Punto de Contacto	**Gestión del Nivel de Servicio**	**Centro de Atención al Usuario**

Tabla 4 .- Diferencias entre Usuario y Cliente ITIL.
(Fuente: propia)

Bajo este punto de vista, ITIL proporciona dos instrumentos de vital importancia: el CAU[63] (Centro de Atención al Usuario) y el Proceso de Gestión del Nivel de Servicio.

El CAU es el punto único de contacto con el usuario final, donde los mencionados usuarios pueden llamar para solicitar cualquier actividad por parte del departamento de

[63] A lo largo de esta memoria a parecerá indistintamente CAU o *HelpDesk*.

Informática. Aquí no sólo se pueden registrar incidencias, sino también solicitar documentación, pedir cambios en la infraestructura, plantear una queja o una mejora, etc.

El otro instrumento clave es el proceso de Gestión del Nivel de Servicio, profundamente orientado a establecer las relaciones con los clientes y que debe gestionar sus expectativas, de tal forma que se definan claramente los objetivos que debe plantearse la organización TI para satisfacer mejor las necesidades de sus clientes.

Como se puede observar, se produce una diferenciación entre el término Cliente y el término Usuario, esta diferencia no es casual, sino que marca una clara distinción funcional. Se hablará de Clientes cuando se desee aludir a las personas que encargan, "pagan" y son dueños de los servicios TI, mientras que se nombrará a los Usuarios cuando se quiera hacer mención a aquellos que utilizan la aplicación a diario. El primer punto de contacto de un Cliente, será el Gerente del Nivel de Servicio, mientras que el primer punto de contacto de los usuarios, siempre será el CAU. Dependiendo de qué es lo que falle, tendrá incidencia sobre uno u otro; así un proceso de Gestión del Incidente que falla, tendrá especial relevancia sobre los Usuarios, mientras que un servicio que tenga una mala relación calidad-precio, o un fallo en el proceso de Gestión del Nivel de Servicio, tendrá un mayor impacto sobre los Clientes.

Aunque los intereses de clientes y usuarios están relacionados en cuanto a prestación de servicios, sus objetivos pueden ser incluso contradictorios; así un usuario

siempre va a buscar la mayor disponibilidad de sus sistemas, mientras que los clientes buscarán la mejor relación calidad-precio. Es preciso, buscar el equilibrio entre dichos objetivos, favoreciendo los flujos de información y la definición conjunta de aquellos procesos clave para ambas partes.

2.4. Soporte del Servicio

Volviendo a ITIL como conjunto de procesos, se podría definir el Soporte del Servicio como un conjunto de procesos integrados, a los que se une una función vital en toda infraestructura ITIL que es el CAU.

Los procesos más importantes que integran el Soporte de Servicio son:

- Gestión del Incidente.
- Gestión del Problema.
- Gestión de la Configuración.
- Gestión del Cambio.
- Gestión de la Versión.

No hay que olvidar que estos procesos están íntimamente relacionados, y junto al citado CAU proporcionan un servicio de cierta calidad, servicio que conlleva toda una infraestructura de TI.

Otro elemento fundamental en dichas relaciones es la CMDB, que contiene todos los datos importantes de los activos de la organización, y que está implicada en todos los pasos de la gestión ITIL, y debería estar disponible para todo el grupo de Soporte de Servicio.

Seguidamente, se presenta una descripción de algunas de las relaciones entre procesos en el Soporte de Servicio:

Se entiende la Gestión de la Configuración como parte integrante de todos los demás procesos de la gestión de servicios de TI.

Todas las solicitudes de cambio, de la Gestión del Cambio, deberían entrar en la CMDB y los registros de ésta se irán actualizando según progrese el cambio.

El proceso de la Gestión del Cambio, depende de la exactitud de los datos de la CMDB, para así evaluar correctamente el impacto de dicho cambio.

La gestión de la entrega se relaciona, por una parte con la gestión de la configuración, y por otro lado con la gestión del Cambio, ya que cualquier avance en esta implica notificaciones a ambos procesos de Gestión.

Así, se encuentra una primera estrecha relación: Configuración-Entrega-Cambio.

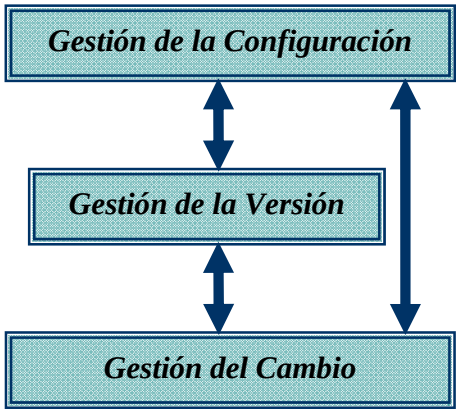


Figura 15.- **Relación entre procesos ITIL I.**
(Fuente: Soporte de Servicio de la OGC)

Los detalles del cambio deben de llegar al CAU antes de su entrega. Esto es así, porque incluso después de unas pruebas completas, existen posibilidades de que dicho cambio ocasione problemas, bien porque el cambio no funciona como se esperaba, bien porque existen dudas sobre la funcionalidad de éste.

Evidentemente, el cambio va a producir una modificación en la CMDB de los activos de la organización implicados.

La Gestión del Incidente recomienda que los registros de incidentes estén recogidos en la misma CMDB que los registros de problemas, de errores conocidos o de cambios.

El proceso de la gestión de problemas exige un exacto y completo registro de incidentes, ya que estos son la base para poder valorar y decidir que realmente existe el problema y por lo tanto implica una gestión.

El CAU, como único punto de contacto diario entre el proveedor de los servicios TI y los usuarios, debe mantener informados a dichos usuarios de las eventualidades producidas en los propios servicios, así como de los cambios producidos.

Véase una nueva relación entre distintos procesos ITIL:

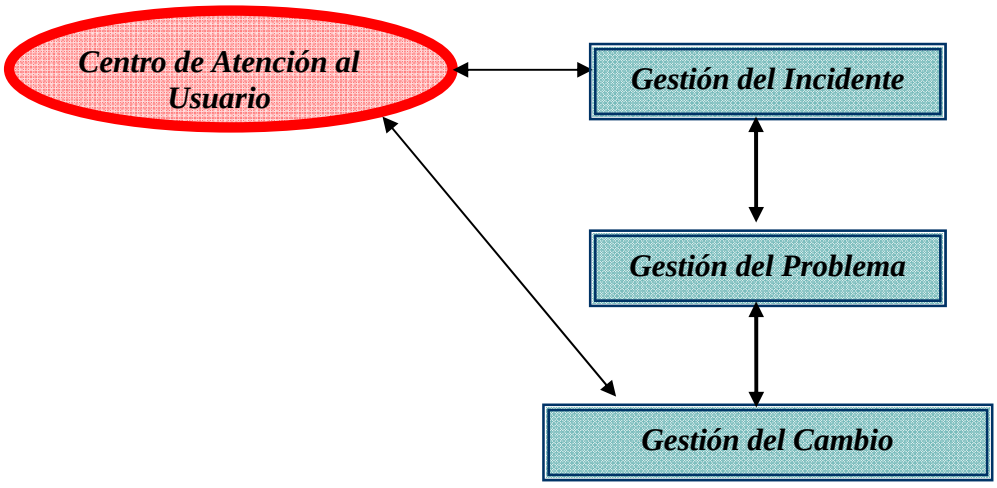


Figura 16.- **Relación entre procesos ITIL II.**
(Fuente: Soporte de Servicio de la OGC)

Todas estas relaciones, que por propia naturaleza de ITIL, son muy numerosas, se podrían resumir en el siguiente esquema:

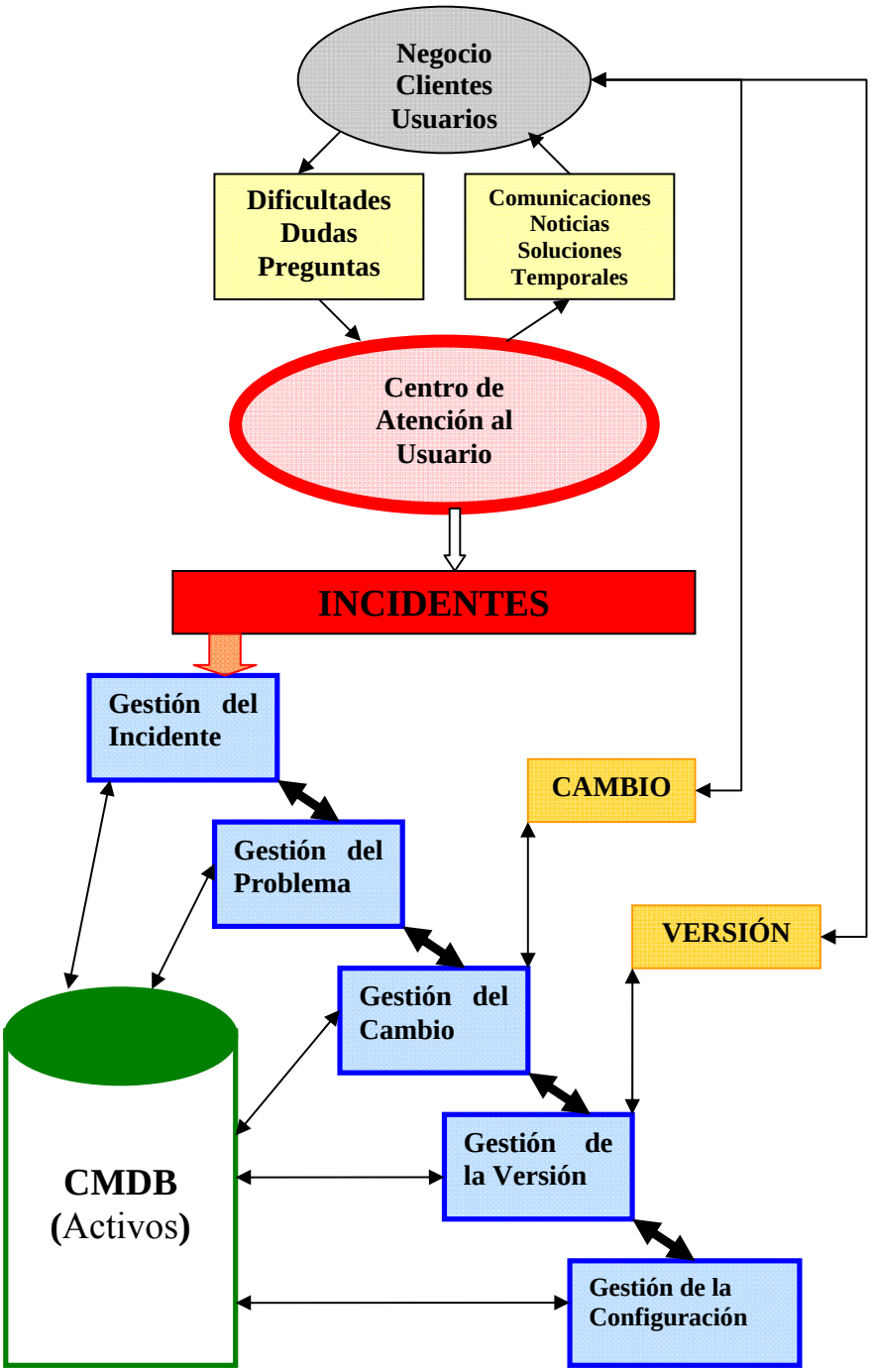


Figura 17.- **Esquema de relaciones ITIL.**
(Fuente: Soporte de Servicio de la OGC)

3. ITIL v3

Con ITIL v3 se avanza un paso más en el desarrollo de una librería de buenas prácticas iniciada con ITIL v1.

En esta evolución de ITIL se pretende mostrar la idea del **Ciclo de Vida** de un servicio de las TI. Dicho ciclo de vida podría desarrollarse de la siguiente manera:

- 1ª Fase: Diseño del servicio.
- 2ª Fase: Desarrollo de dicho servicio.
- 3ª Fase: Implantación del servicio.
- 4ª Fase: Operación del servicio.

- Todas estas fases estarán dirigidas por una Estrategia.
- A su vez están sometidas a una Mejora Continua.

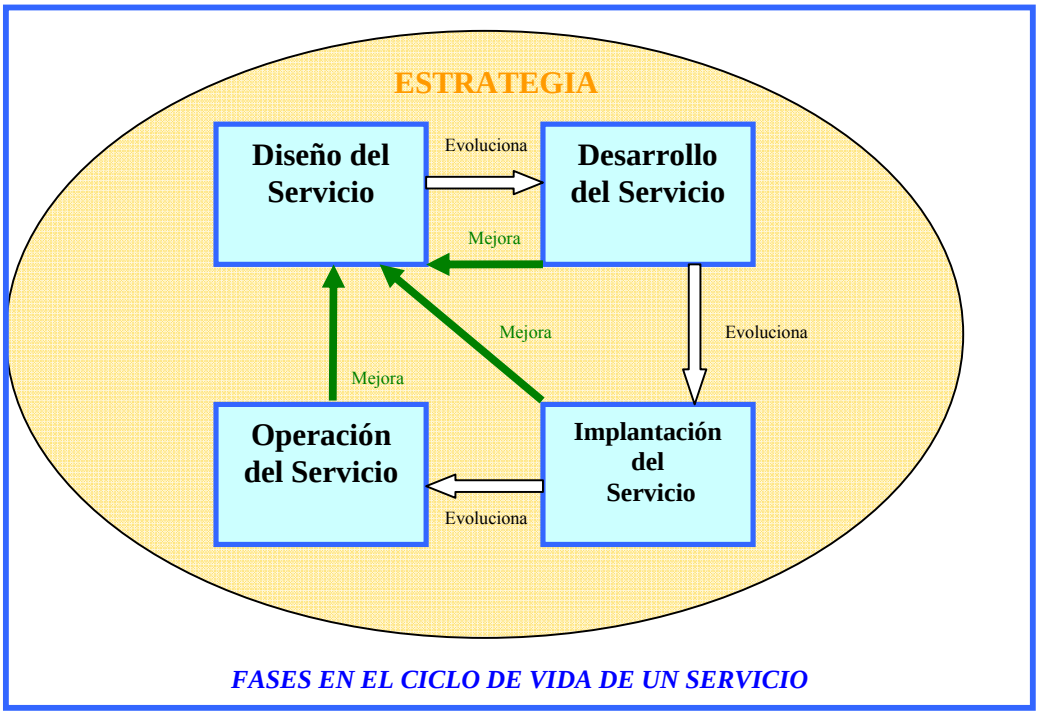


Figura 18.- **Fases del ciclo de vida de un servicio.**
(Fuente: propia)

ITIL v3 consta de cinco libros que forman una estructura articulada en torno al concepto de ciclo de vida del servicio de las TI. Se trata de establecer un marco de referencia único para todos los libros, de forma que éstos no sólo tengan sentido por sí mismos, sino que además se puedan percibir como un todo. Este nexo de unión, es el ciclo de vida del servicio TIC.

Parece necesario, por tanto, definir lo que para ITIL es un servicio TIC:

Servicio TIC: Es el resultado de desarrollar un valor para un cliente, de forma que éste consiga realizar la acción que desea, sin ser responsable de los costes y riesgos específicos de dicho desarrollo.

Es decir, el cliente solicita realizar una acción (lógicamente relacionada con las TIC) y las propias TIC le proporcionan lo necesario para realizar esa acción. Al cliente no le interesan las tareas necesarias para poder proporcionar el servicio, simplemente le interesa poder realizar la acción proporcionada por el servicio con una calidad determinada.

Por ejemplo, un cliente necesita leer el correo electrónico desde su puesto de trabajo, en principio, al cliente no le interesará toda la infraestructura necesaria para que él pueda realizar dicha acción (no le interesará si es necesario conectar el equipo a Internet, si esa acción conlleva unos ciertos riesgos, etc). El cliente demanda el servicio TIC: leer el correo en su estación de trabajo, y una buena gestión de servicios TIC le proporcionará esa facilidad.

En el párrafo anterior se ha introducido algo muy relacionado con este trabajo: para aportar el servicio de correo electrónico, posiblemente habrá que conectarse a Internet, y la conexión a Internet conlleva un riesgo, pues bien, ese riesgo es necesario tratarlo dentro de toda la infraestructura de la TIC creada, por tanto será necesario gestionarlo correctamente, generando nuevos procesos integrados en el sistema de gestión. Evidentemente, si se está

utilizando ITIL como base de la gestión de servicios, parece necesaria una integración con la gestión de la seguridad.

ITIL v3 está basado en el servicio y su ciclo de vida, pero desafortunadamente parece que deja de lado en dicho ciclo de vida los aspectos de seguridad, no profundiza en ellos y son tratados de forma muy generalizada, entendiéndose que es quién desarrolle la infraestructura quién debe integrar dicha gestión de seguridad en ITIL.

Ya se plantean aquí dos posibles enfoques que se desarrollarán en el capítulo siguiente:

- Por un lado, la seguridad como un servicio más dentro del portfolio ofrecido. Si se entiende la seguridad como un servicio más, siempre se pueden aplicar las buenas prácticas propuestas por ITIL para desarrollar el ciclo de vida que implique dicho servicio de seguridad.
- Por otro lado, incluir seguridad en todos los procesos y servicios ofrecidos.

Seguidamente se presenta el gráfico que modela el ciclo de vida y la descripción de cada una de las fases (que se corresponde con cada uno de los libros) [ITSV307].

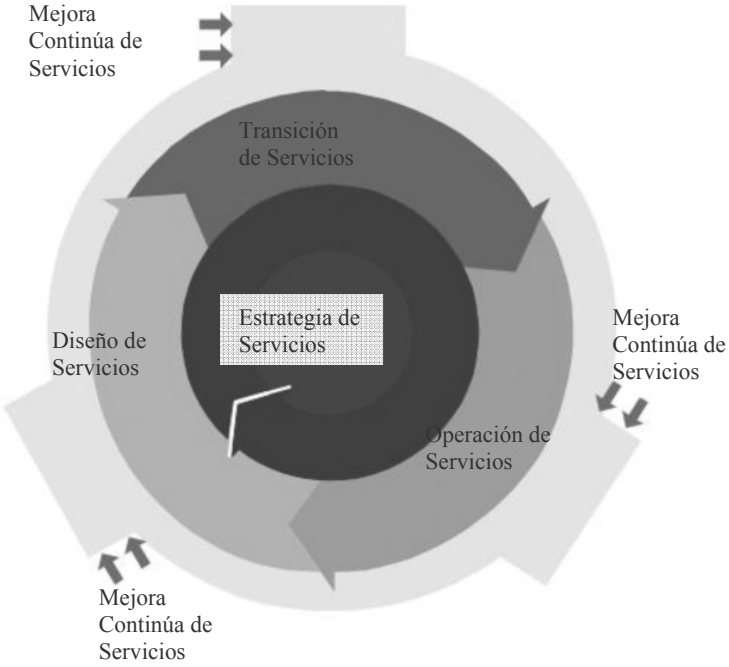


Figura 19.- **Ciclo de vida de un servicio según libros ITIL v3.**
(Fuente: An Introductory overview of ITIL v.3 de itSMF)

3.1. Estrategia del Servicio

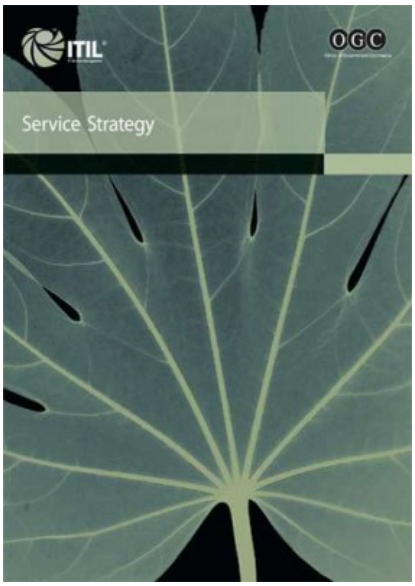


Figura 20.- **Portada del libro "Estrategia del Servicio" de ITIL v3.**
(Fuente: OGC)

Como se puede observar en el gráfico de figura 19, este volumen es el eje director sobre el que giran el resto de los libros.

La Estrategia del Servicio en ITIL se basa en el conocimiento de que un cliente no compra un producto, un cliente lo que compra es la satisfacción adecuada de cierta necesidad. Para conseguir aportar al cliente lo que éste demanda, es necesario tener un claro conocimiento de las necesidades de dicho cliente, en términos tales como: ¿Qué? ¿Dónde? y ¿Porqué? se demanda un determinado servicio.

La Estrategia del Servicio busca la relación entre el negocio y la TI. Tiene como fin el alineamiento entre dichos conceptos, aportando cada uno al otro lo necesario para la continuidad del propio negocio, fin que por otra parte ya estaba claramente referenciado en ITIL v2.

Para crear una buena Estrategia del Servicio será necesario tener claros los siguientes conceptos:

- Qué servicios deberían ser ofrecidos.
- A quién deben ofrecerse esos servicios.
- Cómo el cliente percibirá y medirá el valor de los servicios.
- Todo lo referido a la competencia de mercado en el soporte de servicios.

- Tipos de proveedores de servicios y cómo el cliente elige su proveedor.
- Decisiones a nivel de gestión financiera para la creación de los valores aportados por los servicios.
- El aprovechamiento de recursos disponibles para el desarrollo de los servicios.
- Cómo se desarrollará la medición de la ejecución del servicio.

ITIL considera el valor de los servicios desde dos perspectivas:

- **Utilidad del servicio**: Resultados obtenidos.
- **Garantía del servicio**: Disponibilidad, capacidad, continuidad y seguridad.

En la Estrategia del Servicio existen una serie de actividades y procesos clave, que se encargan de generar y gestionar la propia estrategia de servicios implantada en la organización. En la siguiente tabla se muestran dichas actividades y procesos clave:

Actividades y Procesos clave en la Estrategia del Servicio	
Gestión financiera	**Gestión presupuestaria, contable, y honoraria.**
Gestión de la cartera de servicios (SPM)	**Gestión del ciclo de vida de los servicios, incluyendo catalogación y retirada de estos.**
Gestión de necesidades	**Entender e influir al cliente en sus necesidades y proveer los recursos necesarios de estas necesidades**

Tabla 5 .- Actividades y Procesos clave en la Estrategia del Servicio ITIL v3.
(Fuente: propia)

3.2. Diseño del Servicio

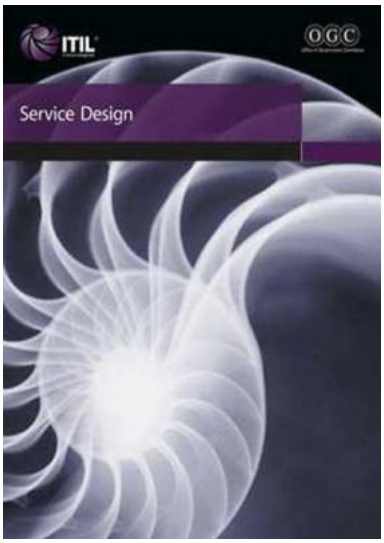


Figura 21.- **Portada del libro "Diseño del Servicio" de ITIL v3.**
(Fuente: OGC)

El diseño es una fase esencial en la globalidad del ciclo de vida del servicio. Comprende el diseño de la arquitectura, es decir, de los procesos, políticas y documentación, implícitos en el diseño de un buen servicio.

Las metas y objetivos del diseño de un servicio son:

- Diseñar servicios que concuerden con el objetivo de negocio.
- Diseñar procesos que soporten el ciclo de vida del servicio.
- Identificar y gestionar riesgos.
- Diseñar métodos y métricas de medida.
- Producir y mantener planes, procesos, políticas, estándares, arquitecturas, marcos de trabajo y documentos que soporten diseños de soluciones TI de calidad.

Existen cinco aspectos individuales del Diseño del Servicio:

1º.- Cambios o novedades en el servicio.

2º.- Sistemas de gestión del servicio y herramientas.

3º.- Sistemas de gestión y tecnologías.

4º.- Procesos, roles y capacidades.

5º.- Métricas y métodos de medida.

Las actividades y procesos clave en esta fase del Diseño del Servicio, son las siguientes:

Actividades y procesos clave en el Diseño del Servicio	
Gestión del Catálogo de Servicios (SCM)	**Como única y consistente fuente de información para todos los servicios acordados.**
Gestión del Nivel de Servicio (SLM)	**Controla que el operacional del servicio y su construcción son medidos de forma consistente.**
Gestión de Capacidades	**Como punto de control para gestionar todas las capacidades relacionadas con los recursos y servicios.**
Gestión de la Continuidad del Servicio	**Mantiene la recuperación de la capacidad de los servicios necesaria para la continuidad del negocio.**
Gestión de la Seguridad de la Información (ISM)	**Alineamiento de la seguridad TI con el negocio garantizando la seguridad de la información en todas las actividades de los servicios y de la gestión de los servicios.**
Gestión de Proveedores	**Asegura que se mantienen los contratos, en los términos y condiciones, acordados con los proveedores.**
Gestión de la Disponibilidad	**Como punto de control para gestionar toda la disponibilidad de recursos, componentes y servicios.**

Tabla 6 .- Actividades y procesos clave en el Diseño del Servicio ITIL v3.
(Fuente: propia)

3.3. Transición del Servicio

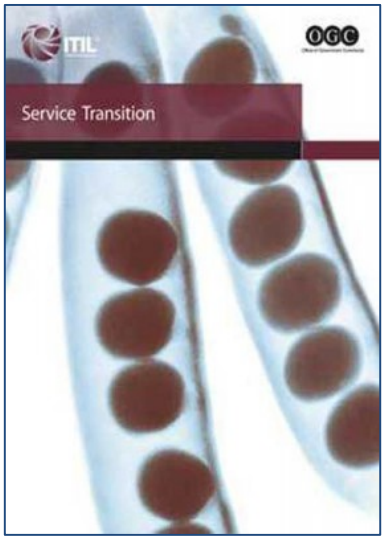


Figura 22.- **Portada del libro "Transición del Servicio" de ITIL v3.**
(Fuente: OGC)

Su función reside en desarrollar los servicios que han sido requeridos en el uso operacional del negocio.

Esta fase recibe información de la fase de Diseño del Servicio y se va desarrollando según la fase de Operación del Servicio lo va necesitando. Si las circunstancias o requisitos de diseño cambian, posiblemente esos cambios se reflejarán en la fase de Transición del Servicio.

La principal misión de esta fase es gestionar eficaz y eficientemente la creación o el cambio de los servicios. Para poder cumplir dicha misión, las actividades y procesos clave son los siguientes:

Actividades y procesos clave en la Transición del Servicio	
Gestión del Cambio	**Asegura que los cambios son registrados, evaluados, autorizados, priorizados, planificados, probados, implementados, documentados y revisados de forma controlada.**
Gestión de Configuraciones y Activos	**Identifica, controla y contabiliza los activos y elementos de configuración (CI) pertenecientes a los servicios.**
Gestión del Conocimiento	**Asegura que las personas debidas tienen el conocimiento debido, en el momento adecuado.**
Soporte y Planificación de la Transición	**Planifican y coordinan recursos e identifican, gestionan y controlan riesgos.**
Gestión de Despliegue de Versiones	**Cubre el ensamblaje e implementación de los nuevos servicios o cambios en éstos.**
Validaciones y Pruebas de los Servicios	**Controlan que los cambios o los nuevos servicios mantengan lo acordado en las SLAs.**
Evaluación	**Aseguran que el servicio será útil para el negocio.**

Tabla 7 .- Actividades y procesos clave en la Transición del Servicio ITIL v3.
(Fuente: propia)

3.4. Operación del Servicio

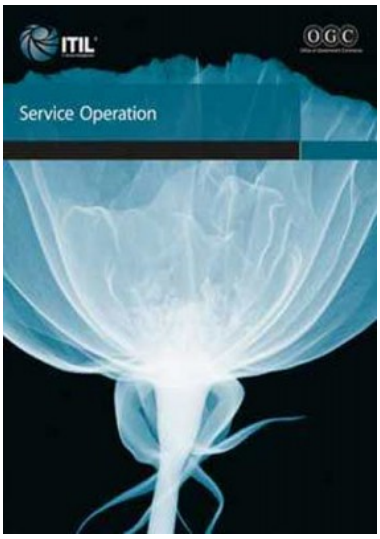


Figura 23.- **Portada del libro "Operación del Servicio" de ITIL v3.**
(Fuente: OGC)

Su propósito es proporcionar el nivel de servicio acordado con los usuarios y clientes, así como gestionar las aplicaciones, tecnologías e infraestructuras de la TI para dar soporte al desarrollo del servicio.

En esta fase se utilizan conceptos existentes en los libros Soporte del Servicio y Entrega del Servicio de la versión 2 de ITIL, con el fin de asegurar su integración con el resto de libros e incorporar el conocimiento anterior.

Un aspecto importante, tratado en esta fase, es el estudio de las posibles contradicciones y conflictos asociados entre los siguientes conceptos:

- Visión interna de la TI contra visión externa.
- Estabilidad contra Responsabilidad.
- Calidad del servicio contra Coste del servicio.
- Política reactiva contra preactiva.

Las actividades y procesos clave asociados a esta fase de Operación del Servicio son:

Actividades y procesos clave en la Operación del Servicio	
Proceso de Gestión de Eventos	**Considerando que un evento es un cambio en el estado de algo que tiene significado para los campos de gestión y configuración del servicio.**
Proceso de Gestión del Incidente	**Considerando Incidente como una interrupción de un servicio o reducción de la calidad de éste de forma no planificada.**
Proceso de cumplimiento de solicitudes	**Una solicitud es una petición de un usuario, que requiere información, consejo, cambio estándar o acceso a un servicio.**
Proceso de Gestión de Acceso.	**Provee de los derechos adecuados para que un usuario acceda a un servicio, o grupo de servicios.**
Proceso de Gestión del Problema	**Entendiendo como problema la causa de uno o más incidentes.**

Tabla 8 .- Actividades y procesos clave en la Operación del Servicio ITIL v3.
(Fuente: propia)

Además, la Operación del Servicio incluye una serie de actividades que no son parte de los procesos antes descritos, estas actividades son las siguientes:

- Monitorización y control: Detectar el estado de los servicios y los Elementos de Configuración, y tomar las acciones correctivas necesarias.
- Consola de Gestión: Punto central de coordinación, monitorización y gestión de servicios.
- Infraestructura de gestión: Bases de datos, almacenamiento, servicio de directorio y otro software.
- Aspectos operacionales de los procesos desde otras etapas del ciclo de vida: Cambios, configuraciones, revisiones y desarrollos, disponibilidad, capacidad, conocimiento, gestión de la continuidad del servicio, etc.

Dentro de la Operación del Servicio, existe una función clave, ya conocida en la anterior versión de ITIL: Centro de servicio al usuario (también denominado HelpDesk).

El CAU registra y gestiona todos los incidentes, peticiones y accesos a servicios, siendo el único punto de contacto con el cliente/usuario, además de proporcionar relaciones con el resto de procesos y actividades de la operación del servicio.

3.5. Mejora Continua del Servicio

Figura 24.- **Portada del libro "Mejora Continua del Servicio" de ITIL v3.**
(Fuente: OGC)

Elemento, que junto con la Estrategia del Servicio, inspira todo el conjunto de ITIL, ya que la Mejora Continua es un componente intrínseco en la orientación a proceso dentro de una gestión de calidad (ITIL versión 2), evidentemente es parte fundamental en el ciclo de vida de dicho servicio (ITIL versión 3).

El propósito fundamental de la Mejora Continua del Servicio (CSI[64]), es mantener el valor del servicio para el cliente, en base a la continua evaluación y mejora de la calidad del los servicios.

CSI combina principios, prácticas y métodos de gestión de calidad, gestión del cambio y mejora de la capacidad, trabajando para mejorar cada etapa del ciclo de vida.

CSI define tres procesos clave para una efectiva implementación de la mejora continua:

Procesos clave en la Mejora Continua del Servicio	
Mejora en siete pasos	**Comprende todos los pasos para realizar una mejora efectiva.**
Medida de servicios	**Con el fin de validar antes de tomar decisiones, dirigir actividades, justificar acciones requeridas e intervenir en el punto adecuado para tomar medidas.**
Informe del servicio	**Recopilar los datos interesantes de toda la colección obtenida en las medidas.**

Tabla 9 .- Procesos clave en la Mejora Continua del Servicio ITIL v3.
(Fuente: propia)

La mejora en 7 pasos es un proceso que comprende todos los pasos requeridos para recolectar los datos, analizarlos y presentar la información a los gestores, para que éstos procedan a priorizar, realizar los acuerdos y las implementaciones que se consideren necesarias, para una mejora continua en la prestación de los servicios a la organización.

Véase un esquema donde se describe el proceso de los siete pasos de mejora:

[64] *Continual Service Improvement.*

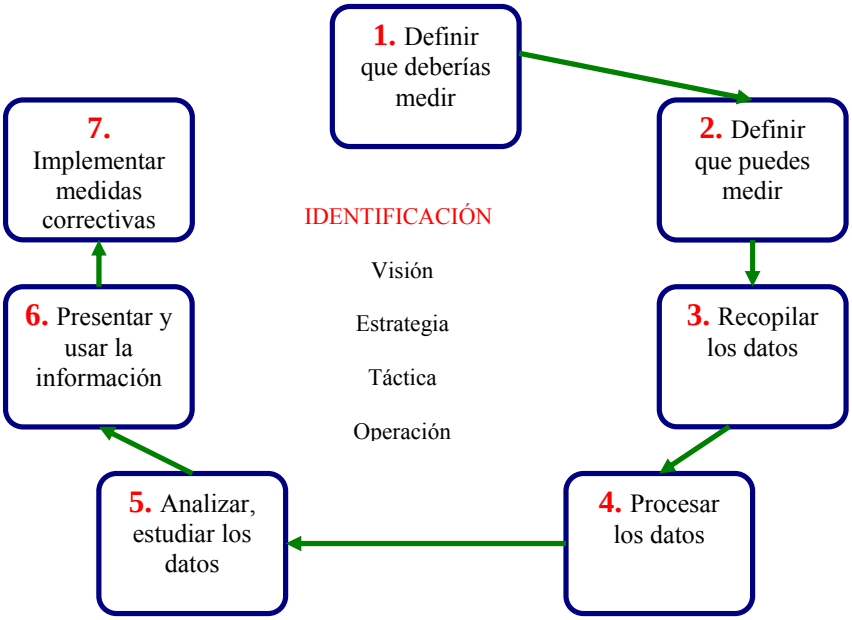


Figura 25.- **Proceso de Mejora Continua del Servicio en 7 pasos.**
(Fuente: propia)

Existen tres tipos de medidas, que deben realizarse en cualquier organización, para dar soporte a las actividades del proceso de Mejora Continua del Servicio:

- **Medidas tecnológicas**: Asociadas a los componentes y aplicaciones.
- **Medidas de los procesos**: Capturando datos en las actividades de factores críticos de los sucesos, indicadores clave de ejecución y métricas de actividades.
- **Medidas de los servicios**: Medidas de componentes y tecnología que son usadas para medir los servicios.

Como ya se ha repetido en varias ocasiones, ITIL es un marco de trabajo que debe ser especializado para cada organización, en función de sus posibilidades y pretensiones empresariales, así como de la capacidad de dicha organización para desplegar las TI. Aún así, ITIL v3 muestra una visión de alto nivel de lo que podría ser un modelo del servicio:

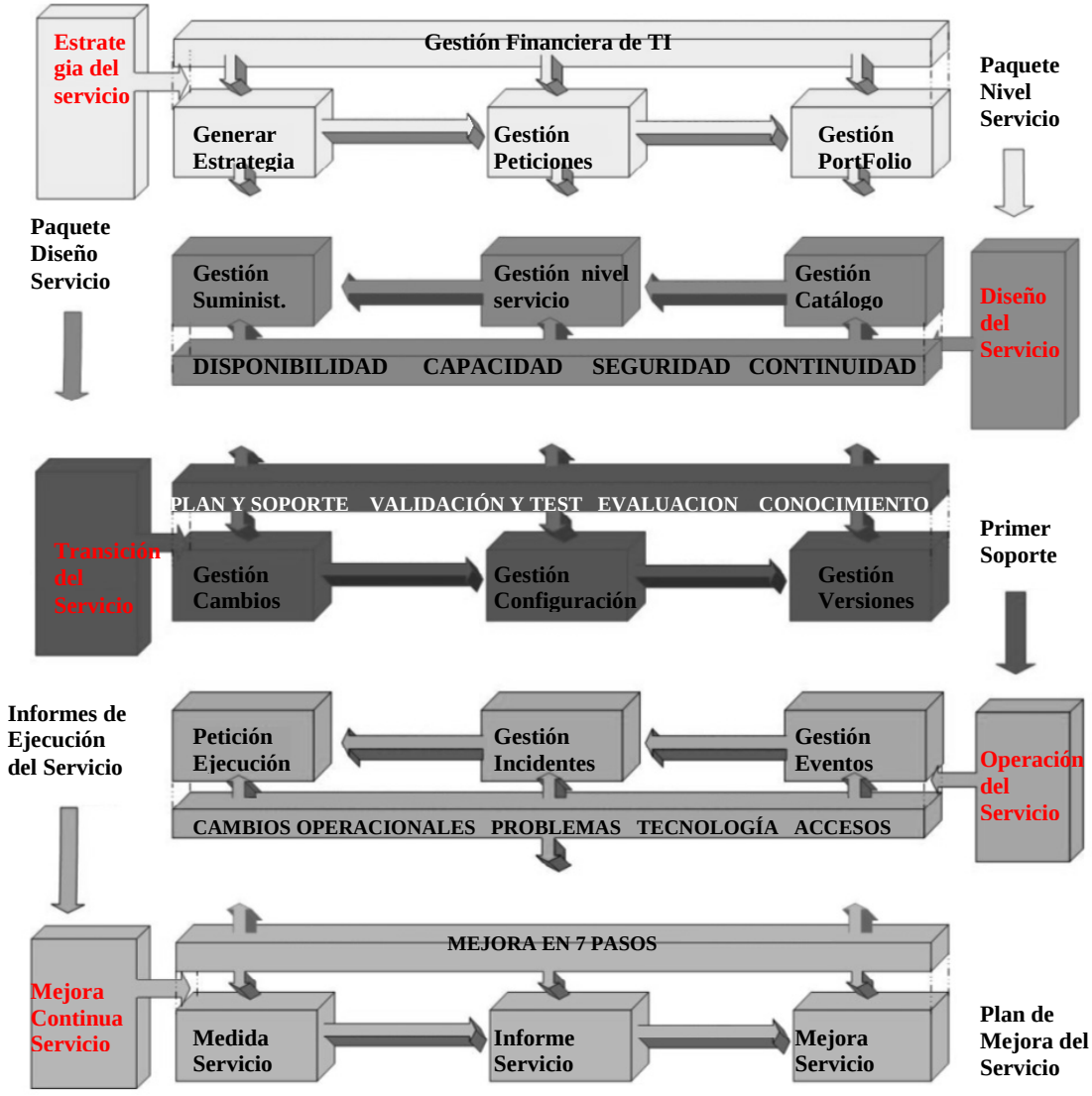


Figura 26.- **Modelo de Servicio según ITIL v3.**
(Fuente: An Introductory overview of ITIL v.3 de itSMF)

4. V2 vs V3

Como ya se ha recalcado en apartados anteriores de este mismo capítulo, la principal diferencia entre las versiones 2 y 3 de ITIL está en la visión del Ciclo de Vida del servicio, que se introduce en la versión 3. Mientras que bajo el alcance de los fundamentos de la versión 2 se ponía el foco en prácticas sencillas agrupadas en Provisión y Soporte, bajo el alcance de la versión 3 se tiene en cuenta el Ciclo de Vida completo del servicio.

El continuo desarrollo de mejores prácticas ha llevado a la desaparición de varios términos entre las versiones 2 y 3 de ITIL, así como a la adición de un gran número de nuevos términos en la versión 3 [ITS08].

Algunos ejemplos de cambios en el significado o desaparición de términos son los siguientes:

1. Catálogo es ahora Portfolio.

   En la primera versión de ITIL se hace mención a la necesidad de tener una fuente de información donde se disponga de los servicios definitivos, etc pero no se le daba aún ningún nombre. En la V2 se le llamó Catálogo y en la V3 se habla de Portfolio.

2. Gestión de la Disponibilidad y Gestión de la Continuidad eran 2 procesos perfectamente diferenciados en V2, son tratados conjuntamente en V3 en el libro de Diseño del Servicio.
3. ITIL V3 usa nuevos conceptos como SKMS (*Service Knowledge Management System*) y CMS (*Configuration Management System*).
4. ITIL V3 usa nuevos términos como: Activos de servicio.

A continuación se exponen de manera resumida las mejoras de ITIL v3 respecto de su versión anterior.

4.1. Mejoras en la estructura

Como se ha explicado en el apartado anterior, los libros se reducen a cinco, y lo que es más importante, éstos tendrán una estructura única para cada capítulo, es decir, todos los capítulos tendrán el mismo índice, consiguiendo una mejor y más rápida comprensión y aplicación de los mismos.

4.2. Mejoras en el contenido

A continuación se enumeran las mejoras más significativas que se han encontrado haciendo esta revisión crítica de ITIL:

1. Se muestran estructuras de organización para la gestión de servicios TI.
2. Se trata el tema de intercambio cultural.[65]
3. Desarrollo de ITIL en entornos con múltiples modelos de subcontratación de proveedores y servicios.
4. Alineamiento con otros marcos de referencia, tales como CobIT (explicado en el capítulo II apartado 3.3 de esta memoria), CMMi (explicado en el capítulo II apartado 3.2 de esta memoria), Six Sigma, eTom, etc.
5. Evaluación de herramientas.
6. Tratamiento más a fondo de las métricas, y ejemplos de algunas de ellas.
7. Se preservan los conceptos principales de los baluartes de la versión anterior: *Soporte del Servicio* y *Entrega del Servicio.*

[65] Referencias a otras prácticas, relación con otros modelos de referencia, inclusión de casos prácticos y plantillas, y alineamiento con el gobierno de las TI.

5. Diferencias entre ITIL v3 e ISO/IEC 20000

En este apartado se ha hecho una labor comparativa, buscando las grandes diferencias que separan a ITIL e ISSO/IEC 20000.

Durante algunas años la estrecha relación entre ITIL v2 y la BS 15000 (y por lo tanto la ISO/IEC 20000) ha beneficiado a ambos conjuntos de documentos y a aquellos que han confiado en ellos. Las reglas para el desarrollo de estándares en Reino Unido hizo que el alineamiento entre la BS 15000 e ITIL fuera un hecho, sin que la OGC (dueña de ITIL) o BSI (dueña de BS 15000) ejerciesen un control directo. La BS 15000 fue escrita de tal manera que otras mejores prácticas (además de las de ITIL) fueron incluidas como requisitos para lograr alcanzar la certificación en dicha norma.

En cualquier caso, la ruta más fácil para llegar a cumplir los requerimientos de la ISO/IEC 20000 sigue siendo vía ITIL, es decir, siguiendo sus indicaciones. De hecho, a menudo se habla de la norma ISO/IEC 20000 como "el estándar de ITIL"; y frecuentemente vemos a proveedores de servicios que adoptan la ISO/IEC 20000 para demostrar que han adoptado los consejos de ITIL de una manera efectiva.

ITIL v3 como ya se ha comentado con anterioridad, se publicó en mayo de 2007 y con el paso del tiempo reemplazará completamente a ITIL v2, aunque por el momento ambos coexisten. Uno de los objetivos para el proyecto de ITIL V3 fue mantener y, donde fuese apropiado, mejorar el alineamiento con la norma ISO/IEC 20000. Por ello, hay menos diferencias entre ISO/IEC 20000 e ITIL v3 que con ITIL v2. Los cambios más relevantes

entre ITIL v2 a ITIL v3 tienen que ver con el ciclo de vida del servicio en la v3, el cual está más alineado con el planteamiento de ciclo de vida en ISO/IEC 20000.

A continuación se presentan las diferencias más notables que se han hallado entre ITIL v3 y la ISO/IEC 20000:

1. En primer lugar hay que señalar que se ha querido hacer esta comparativa, pero ISO 20000 sí es un estándar e ITIL es una colección de libros.

2. Como segunda puntualización, decir que como se ha explicado en el apartado anterior, ITIL V3 es posterior a ISO 20000 por lo que esta norma ha influido en la nueva versión de ITIL.

3. El término “actividad”.

En ITIL V3 el significado de esta palabra es: conjunto de acciones diseñadas para alcanzar un resultado concreto. Las actividades normalmente se definen como parte de los procesos y planes y se documentan en procedimientos.

En cambio, el término actividad no tiene un significado espacial en ISO/IEC 20000. En cualquier caso, como este término si se usa en otros estándares internacionales como ISO/IEC 12207/15288/15504 podría haber cambios en la próxima versión de ISO/IEC 20000.

4. El término “activo”.

En ITIL V3 los activos se usan tanto para capacidades como para recursos, dependiendo del contexto. Los activos incluyen cualquier cosa que pueda contribuir a la entrega del servicio. Un activo puede ser de gestión, de organización, de proceso, de conocimiento, de personas, de información, de aplicaciones, de infraestructura o financieros. En cambio en ISO/IEC 20000 la palabra activo se usa para temas financieros.

5. La CMDB.

Como se explica en apartados anteriores la CMDB es la base de datos que contiene todos los detalles relevantes de cada elemento de configuración, así como los detalles de las relaciones entre ellos.

En ITIL V3 la CMDB se usa para almacenar los registros de configuración a lo largo de su ciclo de vida. Además ITIL V3 usa el término CMS (*Configuration Management System*) como un conjunto de bases de datos, herramientas para gestionar los datos de configuración y datos tales como incidentes, problemas, datos del personal, etc. Por tanto CMS no es una nueva denominación para la CMDB, ya que un CMS puede contener varias CMDBs así como herramientas y una gran variedad de tipos de datos recogidos para muy diversos propósitos.

En cambio ISO/IEC 20000 no especifica dónde deben ser almacenados los datos usados para la gestión de servicios o qué nombre debería dársele a dicho almacén (lógico).

6. El término “incidente”.

Cualquier evento que no es parte de la operativa normal de un servicio y que puede causar una interrupción del servicio.

7. La Gestión de Eventos en ITIL V3 se cubre en ISO/IEC 20000 con el apartado 6.3 de gestión de la disponibilidad y el apartado 8.2 de gestión del incidente. Así pues, un único proceso o actividad de ITIL V3 puede ser “mapeado” a través de varios apartados de ISO 20000.

8. Gestión de la Continuidad y Gestión de la Disponibilidad.

ISO 20000 no requiere que los dos procesos se combinen entre sí, aunque se encuentran en el mismo apartado.

9. La Gestión de Eventos de ITIL V3 se cubre en los apartados 6.3 (Gestión de la Disponibilidad) y 8.2 (Gestión del Incidente) de ISO 20000.

10. Los Activos de Servicios.

Este término no se usa ni en ITIL V2 ni en ISO 20000.

Aunque como se ha detallado existen numerosas diferencias entre el estándar de facto y la norma, ambos (ITIL e ISO 20000) comparten, entre otros, los siguientes objetivos:

– Maximizar la Calidad del servicio

– Alinear los servicios de TI a las necesidades del negocio

– Reducir Costes

– Aumentar la satisfacción del Cliente

– Visión clara de la capacidad del departamento de TI

– Minimizar el tiempo de ciclo de cambios y mejorar resultados en base a métricas

– Toma de decisiones en base a indicadores de negocio y de TI

6. Crítica general a ITIL

La experiencia adquirida por la doctorando indica que el escepticismo del mercado español hacia la nueva versión de ITIL es muy alto a pesar de los esfuerzos realizados en su comunicación.

La aplicación de ITIL en una organización concreta, cuando se quieren implantar de golpe y simultáneamente la totalidad de sus mejores prácticas, puede resultar una experiencia traumática. Los proyectos de este tipo requieren una importante dotación de recursos, pueden implicar una mayor burocracia en los procesos de servicio TI (como por ejemplo las solicitudes/peticiones de servicio) y períodos de implantación prolongados de hasta varios años, requiriendo la adaptación a los procedimientos de ITIL no sólo del área TI, sino de todo el resto de la organización [VER08].

Lo cierto es que durante su primer año de vida ITIL v3 generó unas expectativas muy altas, pero luego según apuntó Manuel López[66] existe un cierto escepticismo en las empresas por el problema del retorno de la inversión debido al gran esfuerzo de formación. En el año 2008 se diseñó un esquema de formación y certificación amplio, extenso y muy lucrativo para las empresas de formación, pero que asusta a dichas compañías [GOM08].

Para el director adjunto de Sopra Profit, Bonifacio Villalobos [GOM08], la principal deficiencia de la nueva versión es que está muy orientada a empresas de servicios y pierde

[66] en el congreso de itSMf en noviembre de 2008, Manuel López, socio de Accenture.

nivel de detalle respecto a la anterior, por lo que para su utilización en clientes requiere una adecuación importante.

Según Jesús Gómez "Para que ITIL versión 3 funcione realmente en España y dé el consabido cambio cultural vamos a necesitar muchas generaciones. ITIL versión 3 es impracticable en nuestro país" [GOM08].

Así pues, la mayor parte de las empresas españolas encuentran la solución en la certificación ISO 20000, "ya que les aporta un sello que las diferencia en el mercado. Además, es un objetivo más pragmático que alcanzar el nivel de madurez marcado por ITIL v3" dice José Luis Castellanos, consultor ITIL de Steria [GOM08].

Debido a todo lo anterior, los factores coste y tiempo para implementar una solución ITIL deja irremediablemente fuera de juego a las PYMES. Por ello, en esta tesis doctoral se ofrece una solución que pretende corregir o mitigar, en la medida de lo posible, todas las deficiencias presentadas en ITIL, especialmente para las PYMES.

6.1. Implantación secuencial de ITIL en las empresas españolas.

La necesidad de mejorar la gestión de los servicios TI, en los que el responsable ha pasado de ser meramente un técnico a un gestor imprescindible para cualquier organización, está siendo cada vez más visible también en las empresas españolas. En este

sentido, éstas también se han interesado en metodologías como ITIL y en los beneficios que éstas pueden aportarles.

La transformación del departamento TI, de centro de coste en centro de beneficio, no puede abordarse, sin embargo, sin la implantación de unas prácticas de gestión que permitan conocer su funcionamiento actual, sus carencias y puntos de mejora. Esta necesidad de las empresas se ha visto reflejada, en los últimos tiempos, en una clara evolución del perfil de CIO[67], desde un cargo con capacidades eminentemente técnicas, hacia un perfil de Gestor, al igual que en el creciente interés de las organizaciones hacia metodologías, como ITIL, y hacia los beneficios que éstas pueden ofrecerles.

6.2. Los peligros de un enfoque global de ITIL.

La aplicación de ITIL en una organización concreta, cuando se quieren implantar de golpe y simultáneamente la totalidad de sus mejores prácticas, puede resultar una experiencia traumática. Los proyectos de este tipo requieren una importante dotación de recursos, pueden implicar una mayor burocracia en los procesos de servicio TI (como, por ejemplo, las solicitudes o peticiones de servicio) y períodos de implantación prolongados de hasta varios años, requiriendo la adaptación a los procedimientos de ITIL no sólo del área TI, sino de todo el resto de la organización.

[67] Responsable de TI.

La implantación global de ITIL resulta, de este modo, más fácil en grandes organizaciones con capacidad de "imponer" a sus empleados el cumplimiento de ciertas prácticas y en empresas pequeñas o de reciente creación, donde todavía no existe una forma de hacer las cosas arraigada. Resulta, sin embargo, tremendamente difícil en un sinfín de PYMES, acostumbradas a una forma de trabajar determinada, donde choca con fuerte resistencias.

6.3. Causas del fracaso de los proyectos de "implantación" de ITIL.

ITIL es una herramienta de trabajo muy valiosa para gestionar servicios TI pero debe ser utilizada adecuadamente. El exceso de celo o la falta de criterio en su aplicación, han hecho que en la práctica haya más fracasos que éxitos en su utilización.

Las principales causas del fracaso de los proyectos de "implantación" de ITIL son las siguientes:

- Falta de reflexión sobre el concepto "servicio".
- "Parálisis por análisis". Procedimientos excesivamente complejos para ser aplicables.
- Falta de instrucciones de trabajo claras y detalladas.
- Foco en los indicadores, y no en el resultado del proyecto y su calidad.
- Exceso de ambición. Las implantaciones globales han demostrado ser un fracaso.

- Falta de compromiso. La gestión de servicios basada en ITIL no es un proyecto, sino un cambio cultural, y como tal debe abordarse.
- Falta de formalización. Algunos conceptos se utilizan indistintamente a lo largo de los libros de ITIL V3, dando lugar a confusiones.
- Complejidad excesiva. ITIL V3 abarca un espectro de recomendaciones que supera con creces las necesidades “normales” de organizaciones “normales”.

7. Crítica a la Seguridad en ITIL

Como ya se ha expuesto ampliamente en capítulos anteriores, hablar de seguridad en el campo de las TI es hablar de los SGS (Sistemas de Gestión de la Seguridad), sistemas que por otra parte, aparecen ampliamente desarrollados en la familia de normas ISO 27000. Aunque los SGS forman parte fundamental de esta tesis, ésta no se centra exclusivamente en la normativa ISO, como sucede con ITIL y muchos otros marcos de trabajo similares, sino que esta tesis pretende mejorar ITIL en este aspecto, incluyendo los SGS dentro del propio marco de trabajo MISITILEON.

Si se hace un estudio pormenorizado de ITIL, como es necesario para llevar a cabo una tesis doctoral, se puede descubrir que, a pesar de hablar de la Gestión de la Seguridad en varios de sus libros, Gestión de la Seguridad[68] (*Security Management)* en su versión 2 y Diseño del Servicio[69] (*Service Design)* en la versión 3, en realidad se puede afirmar que ITIL pasa por encima del tema de la Seguridad de la Información. Un sistema que implemente una automatización en la gestión de los servicios y que no tenga en cuenta la seguridad es un sistema incompleto. ITIL no tiene en cuenta expresamente a la Seguridad de la Información.

Como curiosidad y crítica se quiere destacar el hecho de que los libros de esta nueva versión de ITIL son sólo cinco, pero realmente extensos[70]; pues bien, de Gestión de la

[68] Pequeño libro que no forma parte del *core* de ITIL versión 2.
[69] Sólo en a penas 8 páginas de dicho libro se habla de la seguridad.
[70] Aproximadamente 300 páginas cada libro (unas 1.500 páginas en total).

Seguridad sólo se habla en 8 páginas. Con esto se pretende resaltar que la importancia que se le da a dicha cuestión parece realmente ínfima.

ITIL no se plantea objetivos concretos relacionados con servicios concretos porque no trata de servicios concretos. Es un marco de referencia de cómo buenas prácticas generales pueden ayudar al negocio.

La esencia de esta tesis es la siguiente: si se está utilizando un modelo de gestión contrastado, como puede ser ITIL ¿por qué no utilizar la base y principios del propio ITIL para lograr una adecuada aplicación de seguridad en una organización?

En el apartado de ITIL v3 en el que se habla de seguridad[71], se dice que el objetivo de la ISM (*Information Security Management*) es alinear la seguridad de la TI con la seguridad del negocio y asegurar (valga la redundancia) que la seguridad de la información se gestiona con eficacia en todos los servicios y actividades de la gestión de servicios. Pues bien, lo que se va a lograr con MISITILEON es poner en práctica las actividades, métodos, técnicas y mecanismos necesarios para cumplir dicho objetivo.

La seguridad no es una meta para las organizaciones, sino una necesidad para poder alcanzar los objetivos de cada entidad [OGCSM99].

[71] Apartado 4.6 del libro Diseño del Servicio.

CAPÍTULO IV. MISITILEON. METODOLOGÍA QUE INTEGRA SEGURIDAD EN ITIL EVOLUCIONADA Y ORIENTADA A LA NORMALIZACIÓN.

¿Por qué esta magnífica tecnología científica, que ahorra trabajo y nos hace la vida más fácil, nos aporta tan poca felicidad? La repuesta es esta, simplemente: porque aún no hemos aprendido a usarla con tino[72].

En este cuarto capítulo es donde se presenta la solución novedosa que constituye el núcleo de esta tesis doctoral: la metodología MISITILEON.

1. Introducción

La utilización de las mejor prácticas en los proyectos software mejora la productividad de las organizaciones, la planificación, la calidad de sus productos, la satisfacción del usuario y reducen los costes [WIT00].

Gracias al estudio y a los trabajos previos realizados por la doctorando (como por ejemplo la traducción oficial *ITIL Heroes' Handbook*[73]) se decidió que MISITILEON no debía ir de complicados y estrictos mapas de procesos. Por ello se ha intentado que quien vaya a usar esta metodología no tenga que seguir el proceso de otros o los procesos definidos en un libro. Una vez que las personas de cualquier empresa aprendan MISITILEON, no deberán estar dibujando detallados mapas de procesos para cada módulo,

[72] Albert Einstein (1879-1955).
[73] "ITIL Manual de Héroes. ITIL para aquellos que no tienen tiempo".

preguntando a consultores si están alineados con las especificaciones de ITIL. La verdad es que los consultores difícilmente pueden ayudar a las organizaciones sin entender cómo es la operativa diaria del negocio.

La mayoría de las soluciones ITIL que existen en el mercado, tanto español como internacional, son muy complicadas. Véase como ejemplo de dicha complicación un caso perfectamente real donde un cliente quiere implementar una solución ITIL. En primer lugar, los clientes tienen que conseguir una consultoría en ITIL para definir los procesos de ITIL y alinearlos con sus objetivos de negocio. La siguiente tarea es comprar software ITIL[74] (la mayoría de soluciones ITIL ofrecen gestión de incidentes, gestión de problemas y gestión de cambios como módulos diferentes). Incluso después de elegir el software, tarea que requiere su estudio y su tiempo, a los consultores les lleva meses implementar el proceso.

1.1. Introducción a la Gestión de la Seguridad.

La meta del proceso de Gestión de la Seguridad de la Información es alinear la seguridad de TI con el negocio y garantizar una gestión eficaz de la misma.

Sus objetivos son:

- Garantizar que la información esté disponible y se pueda usar cuando se necesite (disponibilidad).

[74] EasyVista Service Management, Service One, Numara Footprints, Process Worx ITIL, etc.

- Garantizar que la información esté disponible exclusivamente para personas autorizadas (confidencialidad).
- Garantizar que la información sea completa, precisa y esté protegida contra cambios no autorizados (integridad).
- Garantizar la confidencialidad de las transacciones y el intercambio de información entre empresas y asociados (autenticidad y no repudio).

1.2. Ámbito de Gestión de la Seguridad.

La Gestión de la Seguridad de la Información debe cubrir toda la información de TI y del negocio. Entre otras cosas esto incluye:

- La política y los planes actuales y futuros de seguridad.
- Los requisitos de seguridad.
- Los requisitos legales.
- Las obligaciones y las responsabilidades.
- Los riesgos y su gestión para TI y el negocio.

El proceso de Gestión de la Seguridad de la Información debería incluir los siguientes elementos:

- Elaboración, mantenimiento, distribución y fortalecimiento de una Política de Seguridad de la información.

- Entendimiento de los requisitos de seguridad, actuales y futuros que se hayan acordado.
- Implementación y documentación de controles que faciliten la Política de Seguridad de la información y gestionen riesgos.
- Gestión de proveedores de servicios de TI y de contratos, en lo referente a la seguridad de acceso al sistema.
- Mejora proactiva de los sistemas de control de la seguridad.

1.3. Valor para el Negocio

Antes de desarrollar el modelo de MISITILEON desde el punto de vista de los procesos, es importante hacer referencia a otra perspectiva de la seguridad de la información aplicada a la organización: la perspectiva de objetivo de negocio.

La Gestión de la Seguridad de la Información garantiza que la política sobre seguridad de la información cumple la política general de la empresa sobre seguridad y los requisitos legales. Genera un proceso de concienciación interna sobre la necesidad de seguridad en los servicios y activos. La alta dirección es responsable de la información de la empresa y debe dar respuesta a cualquier asunto que afecte a su protección. El comité de dirección debería considerar la seguridad de la información como una parte integral de su cometido. En este sentido, todos los proveedores de servicios de TI deben garantizar el establecimiento de una política bien definida de gestión de la seguridad de la información, al objeto de monitorizar y fortalecer las políticas de seguridad corporativas.

Se puede decir que el desarrollo y éxito de una organización depende de que los servicios TI conozcan las necesidades de negocio, y por ende, los procesos de negocio que generan estas necesidades.

Entendiendo la seguridad de la información como un servicio más de la infraestructura TI, se puede deducir que esta seguridad está principalmente enfocada a que la organización pueda lograr sus objetivos.

Por otra parte, no toda la información, ni los sistemas que la soportan, son igual de importantes, será necesario evaluar el nivel de seguridad que le corresponde a cada información, de forma que exista un equilibrio adecuado entre las medidas de seguridad adoptadas y el coste que supone aplicarlas. Sería ilógico, y muy contraproducente invertir grandes esfuerzos o recursos en proteger información pública o sin importancia, mientras que otra información, más relevante, pudiera quedar desprotegida.

El concepto de la seguridad de la información hay que entenderlo como el de alcanzar un nivel aceptable de riesgos, la seguridad absoluta es un nivel inalcanzable, pero será necesario un nivel intermedio que proteja el valor de la información en función de la importancia de ésta.

La Gestión de la Seguridad no es un proceso aislado, debe estar gobernada por una política corporativa, por tanto será una decisión corporativa, y de alto nivel, el tiempo y recursos que se dedicarán a dicha seguridad.

De igual forma, no es un proceso limitado en el tiempo, sino una sucesión continua, en la que habrá que evaluar y mejorar en cada paso, para llegar a poder implantar las medidas de seguridad que se ajusten al nivel de seguridad decidido de forma corporativa.

Las medidas de seguridad finales, por lo general, deben limitar los riesgos y vulnerabilidades del valor de la información a proteger. Se presenta una descripción de los diferentes tipos de posibles medidas de seguridad:

El gráfico que muestra un modelo de seguridad en la organización, desde el punto de vista del negocio, sería el siguiente:

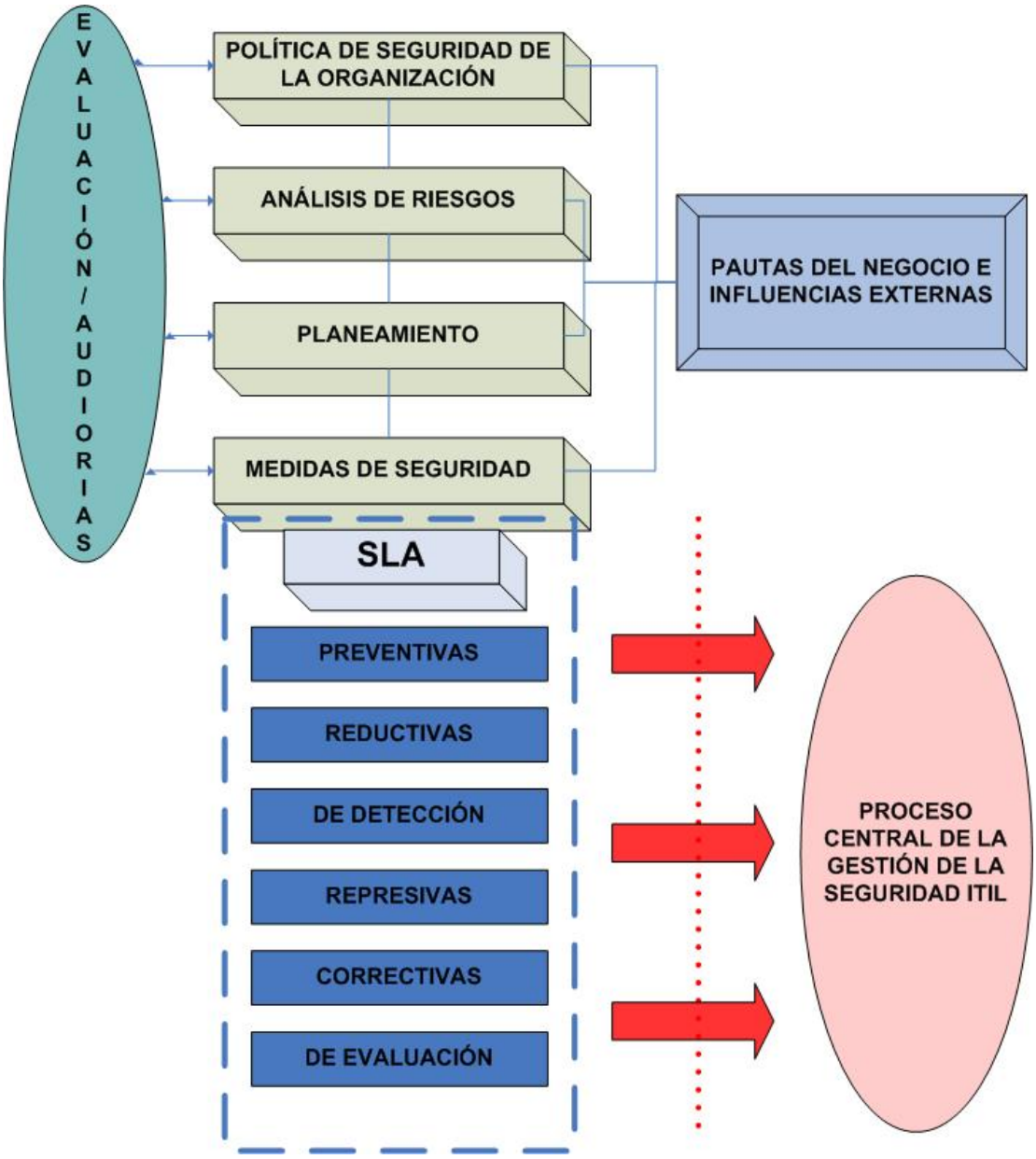


Figura 27.- **Modelo de seguridad desde el punto de vista del negocio.**
(Fuente: propia)

Las medidas de seguridad definen la seguridad demandada para la TI y, tras un acuerdo Cliente-Proveedor, denominado ANS (Acuerdos del Nivel de Servicio)[75] se define

[75] En inglés *Service Level Agreement*.

el Nivel de Requisitos del Servicio de seguridad, como uno más de los aportados a la organización.

En la figura 27 se observa cómo no se han definido procedimientos de Análisis de riesgos o Auditorias, de hecho, en ITIL, se precisa, que tanto la política de seguridad global de la organización, como el análisis de riesgos, sean una responsabilidad del cliente.

Aun así, dentro de las medidas de seguridad, que en definitiva, van a formar los procesos de seguridad, se encuentran aquellas del tipo *detección* o *evaluación,* muy relacionadas ambas con el análisis de riesgos o la auditoria, de hecho, se podría decir que muchos de los procesos que se generan a partir de estas medidas (como pueden ser, los sistemas de monitorización, la gestión de eventos o el análisis forense) van a nutrir a estas actividades, en principio no consideradas servicios proporcionados por ITIL.

1.4. Dos Posibles Enfoques para el tratamiento de la Seguridad.

Cuando surge la idea de realizar esta tesis se plantean varias posibilidades de enfocar el concepto de Seguridad dentro de la "tecnología" ITIL.

Se trata de profundizar en los posibles puntos de vista de la simbiosis entre la seguridad y la gestión de los servicios, considerando ambas disciplinas complementarias, de forma que el desarrollo de cualquiera de ellas facilitará la gestión e implantación de la otra.

Nacen así dos posibles enfoques para MISITILEON:

1º.- La seguridad de los distintos procesos y de sus relaciones.

2º.- La seguridad como uno de los servicios gestionados por este marco de trabajo.

Aunque están fuertemente conectados, en esta tesis se ha optado por el segundo de los enfoques. Los dos son igualmente importantes y se encuentran conexiones continuas entre ambos.

Se ha elegido el segundo enfoque por dos razones:

- la más importante, porque a pesar de hablar de gestión de la seguridad, en ITIL no existe un servicio de seguridad como tal.

- porque este enfoque parece más adecuado a la hora de presentarlo en forma de experimentación, y conseguir así, un trabajo más práctico.

Se propone el primer enfoque como línea de investigación futura, para así conseguir un estudio complementario a la tesis aquí presentada. Con el fin de ayudar en esa hipotética línea de investigación, se presenta con mayor detalle en el apartado de Líneas Futuras del Capítulo 8.

2. Conceptos Básicos de Seguridad

El marco de trabajo y el proceso de la Gestión de la Seguridad de la Información incluyen:

- Política de seguridad de la información.
- Sistema de Gestión de la Seguridad de la Información (ISMS[76]).
- Estrategia de seguridad exhaustiva (relacionada con la estrategia y los objetivos de negocio).
- Estructura organizativa de seguridad efectiva.
- Conjunto de controles de seguridad que apoyen la política.
- Gestión del riesgo.
- Procesos de monitorización.
- Estrategia de comunicación.
- Procesos de comunicación.
- Estrategia de formación y concienciación.

2.1. Terminología

Basándose en el trabajo de la Comisión de Seguridad de SEDISI (Asociación Española de Empresas de Tecnologías de la Información), y completando algunos conceptos, se ha redactado este apartado para "normalizar" algunos términos:

[76] *Information Security Management System,* en castellano SGSI.

- **Sistema de información.** Son los Recursos Informáticos (Físicos y Lógicos) y Activos de Información de que dispone la empresa u organización para su correcto funcionamiento y la consecución de los objetivos propuestos por su Dirección.

- **Amenaza.** Cualquier evento que pueda provocar daño en los Sistemas de información, produciendo a la empresa pérdidas materiales, financieras o de otro tipo. Las amenazas son múltiples desde una inundación, un fallo eléctrico o una organización criminal o terrorista.

- **Vulnerabilidad.** Cualquier debilidad en los Sistemas de Información que pueda permitir a las amenazas causarles daños y producir pérdidas. Generalmente se producen por fallos en los sistemas lógicos, aunque también corresponden a defectos de ubicación e instalación.

- **Riesgo.** Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del Sistema Informático, causando un impacto en la empresa. Evidentemente el riesgo es característico para cada amenaza y cada sistema, pudiéndose disminuir tomando las medidas adecuadas.

- **Incidente de seguridad.** Cualquier evento que tenga, o pueda tener, como resultado la interrupción de los servicios suministrados por un Sistema de Información y/o pérdidas físicas, de activos o financieras. En otras palabras la materialización de una amenaza,

pues como no existe el riesgo cero siempre es posible que una amenaza deje de ser tal para convertirse en una realidad.

- **Impacto.** Es la medición y valoración del daño que podría producir a la organización un incidente de seguridad. La valoración global se obtendrá sumando el coste de reposición de los daños tangibles y la estimación, siempre subjetiva, de los daños intangibles tales como la calidad del servicio y la imagen de la organización.

- **Defensa.** Cualquier medio, físico o lógico, empleado para eliminar o reducir un riesgo. Debe realizarse una valoración cuantitativa de su coste. Muchas veces se la conoce como **medida de seguridad o prevención**. Su objetivo es reducir el riesgo o el impacto.
- **Defensa activa** o **medida de seguridad activa.** Cualquier medida cuyo objetivo sea anular o reducir el riesgo de una amenaza como la instalación de un programa antivirus o el cifrado de la información.

- **Defensa pasiva** o **medida de seguridad pasiva.** Cualquier medida cuyo objeto sea. si se produce un incidente de seguridad, reducir el impacto. El ejemplo típico es el uso de las copias de seguridad de la información.

- **Recurso de recuperación.** Recurso necesario para la recuperación de las operaciones en caso de desastre, como las cintas magnéticas de salvaguarda o los equipos de respaldo.

- **Acción de contingencia.** Acción a realizar en caso de un incidente de seguridad. Por ejemplo cambiar el servidor de la red a otro equipo.

2.2. Sistema de Gestión de la Seguridad de la Información

El ISMS proporciona la base para el desarrollo eficiente de un programa de seguridad de la información que favorezca los objetivos de negocio.

La ISO 27001 es la norma formal con la que las organizaciones podrían contrastar y certificar su ISMS.

2.3. Gobierno de la Seguridad

El gobierno de la seguridad de TI debe realizarse según seis criterios:

- Alineación estratégica
    - Los requisitos de seguridad deben surgir a partir de requisitos empresariales.
    - Las soluciones de seguridad deben ajustarse a los procesos de la empresa.
- Creación de valor
    - Establecer un conjunto estándar de prácticas de seguridad.
    - Distribuir el esfuerzo con una prioridad adecuada sobre aquellas áreas con mayor impacto y rendimiento de negocio.
- Gestión del riesgo

  - Establecer perfiles de riesgo.
  - Priorización de los riesgos en función del impacto.
- Gestión del rendimiento
  - Definir métricas bien definidas, acordadas y significativas.
  - Establecer procesos de medición que ayuda a identificar carencias.
- Gestión de recursos
  - Documentar los conocimientos.
  - Documentar los procesos de seguridad.
- Aseguramiento de procesos de negocio
  - Mejorar la eficacia, eficiencia e integridad.
  - Obtener el mejor retorno de las inversiones.

El Gestor de la Seguridad de la Información (GSI) debe ser consciente de que la seguridad no es sólo un paso más en el ciclo de vida y de que la tecnología por sí sola no puede garantizarla. La seguridad de la información es un proceso continuo que requiere una gestión continuada, y debe ser una parte integral de todos los servicios (y sistemas).

Una amenaza puede causar una incidencia que produce daños. Para evitarlos o reducir su impacto se pueden tomar medidas de distinta naturaleza:

- Medidas preventivas

  Previenen que un incidente de seguridad ocurra, para ello necesitan una serie de requerimientos.

Ejemplo: Limitar el acceso a la información a un grupo de usuarios.

Medida: Creación de roles, y asignación de éstos a los usuarios.

- Medidas reductivas

  Minimizan la cuantía del impacto.

  Ejemplo: Hacer un backup de datos importantes.

  Medida: Disponer de procedimientos de actuación ante desastres bien definidos.

- Medidas de detección

  Ayudan a descubrir, lo antes posible, que el incidente ha ocurrido.

  Ejemplo: Sistema de monitorización.

  Medida: Procedimientos de alerta, envío de mensajes por diferentes vías.

- Medidas limitadoras

  Tratan de evitar que un incidente de seguridad se repita en el tiempo.

  Ejemplo: Bloquear una cuenta de usuario tras tres intentos fallidos de acceso.

  Medida: Correlación de eventos, para detección de problemas ocultos.

- Medidas correctivas

  Tratan de corregir el daño lo antes posible.

Ejemplo: Restaurar un backup tras un desastre.

Medida: Restauración de sistemas operativos por imágenes.

- Medidas de evaluación

  Determinan qué falló y cuál fue la causa del incidente, con objeto de prevenirlo en un futuro. Es importante, que no se limiten únicamente a incidentes graves, sino que traten de mantener un control y evaluación del resto de medidas aplicadas.

  Ejemplo: Mantenimiento de un registro de eventos en un sistema, por un tiempo definido.

  Medida: Equipo de análisis forense.

3. Características de MISITILEON

Una característica fundamental de MISITILEON es que hace un "ITIL más sencillo" para que cualquier organización, grande, mediana o pequeña, pueda beneficiarse de esta nueva metodología.

MISITILEON simplifica los procesos de ITIL para que no se requiera de carísimos consultores o despliegues que no son a la medida del cliente. La idea es que cuando una organización se decante por esta nueva metodología, comience por usar los procesos: Gestión del Incidente, Gestión del Problema, Gestión del Cambio y Gestión de la Versión, construidos entorno a la Base de Datos de Gestión de la Configuración (BDGC).

Cualquier organización puede comenzar con MISITILEON desde el primer día, con un mínimo de configuraciones para adaptarse a sus necesidades. Porque lo que pretende esta metodología es simplificar al máximo sus procesos.

MISITILEON ha tomado todo lo bueno de ITIL (las buenas prácticas que ya habían demostrado ser eficaces en distintas industrias y diferentes países) eliminando lo que no es realmente importante o necesario y ha añadido mejoras.

Otra de sus características (tal vez la más significativa ya que da nombre a esta metodología) es que se centra mucho más que ITIL en la Gestión de la Seguridad. Como se verá en siguientes apartados, MISITILEON plantea dos enfoques para la seguridad, para

finalmente decantarse por tratar la seguridad como un servicio más dentro de los ofertados por MISITILEON.

La última característica importante de MISITILEON es que incorpora una aplicación (desarrollada a medida) para evaluar los conocimientos de los usuarios en dicha metodología: Sistema de Evaluación de Conocimientos MISITILEON. Esta aplicación se explicará en detalle en el Capítulo 7 y su código se encuentra en el Anexo 5 (únicamente en soporte informático).

4. Estructura de MISITILEON.

La estructura general de MISITILEON toma la idea de ITIL v3 respecto a adaptarse al ciclo de vida, pero de una manera muy distinta, ya que en lugar de tomar el ciclo de vida en espiral ha adoptado la estructura del modelo Fuente planteado en los 90 por Henderson-Sellers y Edwards[77]. A pesar de tener dicha estructura, MISITILEON se centra en la mayoría de los procesos que formaban el núcleo de los módulos principales de ITIL versión 2: Soporte del Servicio y Entrega del Servicio.

Se ha elegido como ciclo de vida el modelo Fuente ya que realmente es el más representativo de los lenguajes orientados a objetos y por tanto más adecuado que el ciclo de vida en espiral. Se ha descartado el ciclo de vida en espiral propuesto por ITIL versión 3 ya que presenta el inconveniente de que con dicho modelo es más difícil evaluar los riesgos.

El ciclo de Vida MISITILEON consta de dos periodos:

1. Crecimiento: es el tiempo durante el cual se construye.
2. Madurez: es el periodo de mantenimiento en el cual se lleva a cabo la mejora.

Además de estos dos periodos existen 3 fases:

[77] véase apartado 4.3 del capítulo 2 de esta memoria.

1. Planificación del negocio.

2. Construcción: es la más importante aquí es donde se encuentran los procesos y funciones.

3. Entrega o liberación.

Este modelo es iterativo e incremental.

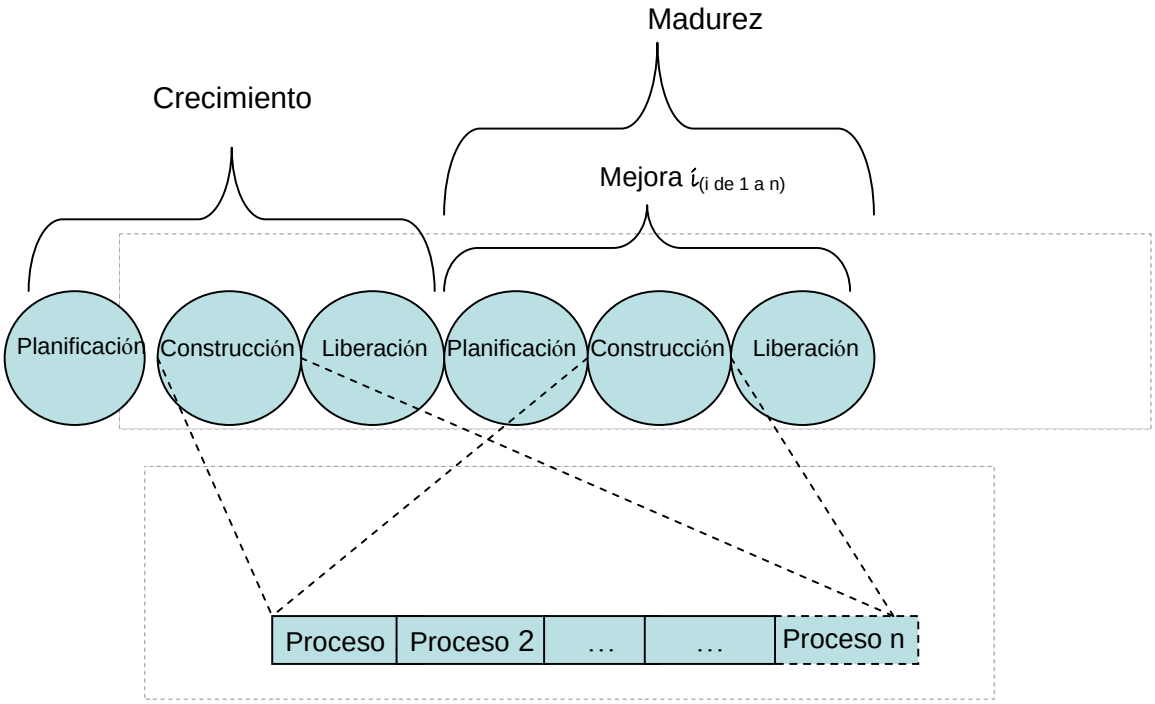


Figura 28.- **Ciclo de Vida Modelo Fuente MISITILEON.**
(Fuente: propia)

La figura 28 representa la estructura que tiene la metodología MISITILEON.

Cada proceso puede tener un ciclo de vida sólo para él debido a que cada uno puede estar en una fase diferente en un momento cualquiera. Una de las ventajas de esta característica del modelo Fuente es que permite un desarrollo solapado e iterativo.

5. Componentes de MISITILEON

En este apartado se presentan en detalle los procesos, la función y la base de datos que componen MISITILEON y que se encargan de ofrecer, de forma controlada y eficaz, los servicios TI a la organización. Dichos componentes son los siguientes:

Procesos relacionados con la Gestión de la Seguridad	
CAU (función)	**Punto de contacto de los usuarios para comunicar incidentes.**
Gestión del Nivel de Servicio	**Proceso responsable de negociar y asegurar el cumplimiento de los ANSs.**
Gestión del Incidente	**Proceso responsable de la gestión de todo el ciclo de vida de los incidentes.**
Gestión del Problema	**Proceso responsable de la gestión de todo el ciclo de vida de los problemas.**
Gestión del Cambio	**Proceso responsable del control del ciclo de vida de los cambios, sobre todo la gestión de la ejecución de los cambios con el mínimo impacto a los servicios TI.**
Gestión de la Versión	**Proceso responsable de la planificación y control de la gestión de versiones, así como de su paso a producción.**
Gestión de la Configuración	**Proceso responsable de mantener la información sobre los elementos de configuración (EC) requeridos para la provisión de un servicio TI.**

Tabla 10 .- Relación de los Procesos con la Gestión de la Seguridad.
(Fuente: propia)

Véase un esquema general donde pueden estar representados todos los procesos, anteriormente descritos:

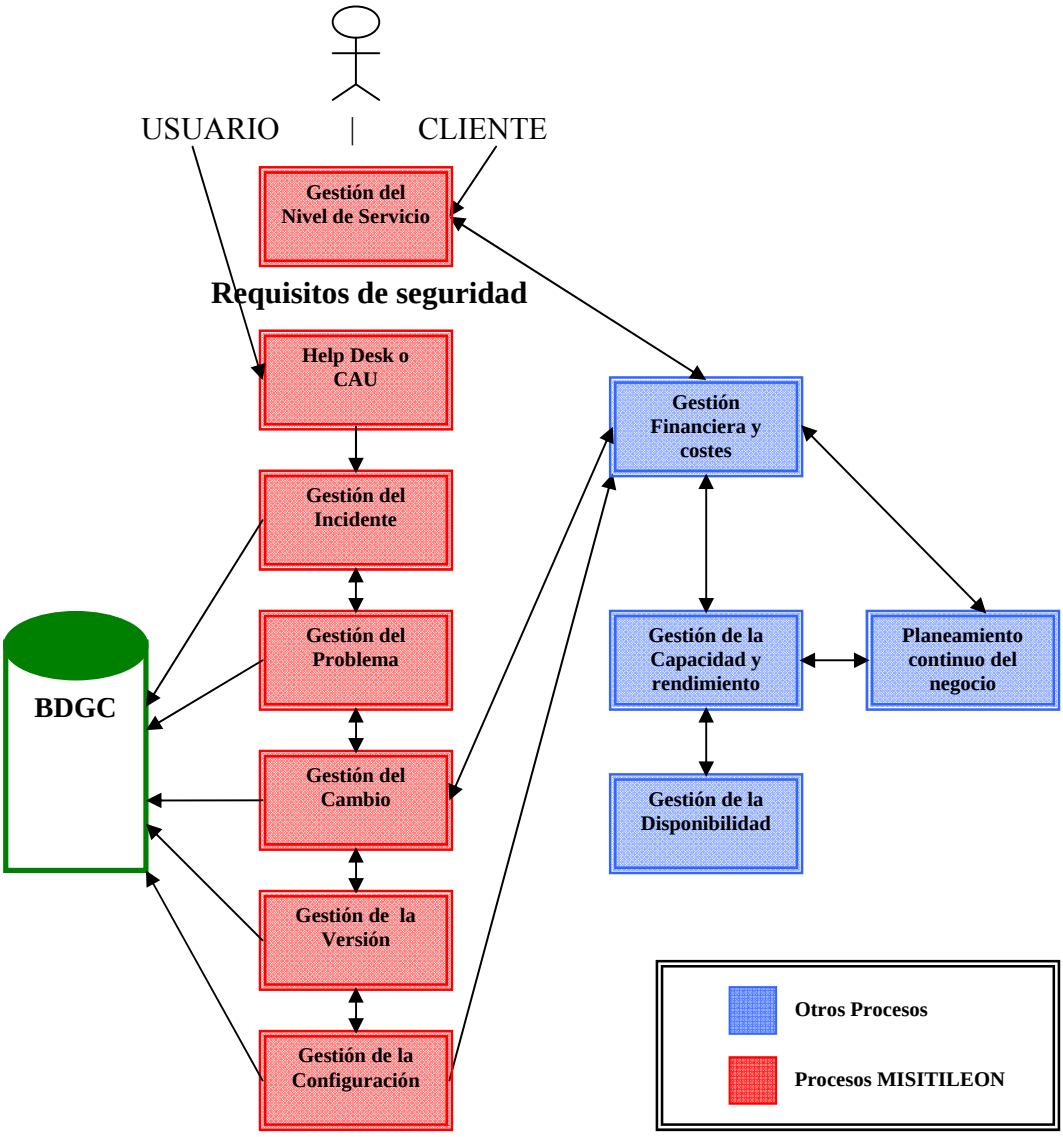


Figura 29.- **Procesos ITIL relacionados con la Gestión de la Seguridad.**
(Fuente: propia)

Además de estos procesos hay que hacer mención a la BDGC.

La figura 30 presenta un gráfico donde se puede observar cómo interactúan estos procesos con la función de *HelpDesk* y la CMDB en ITIL.

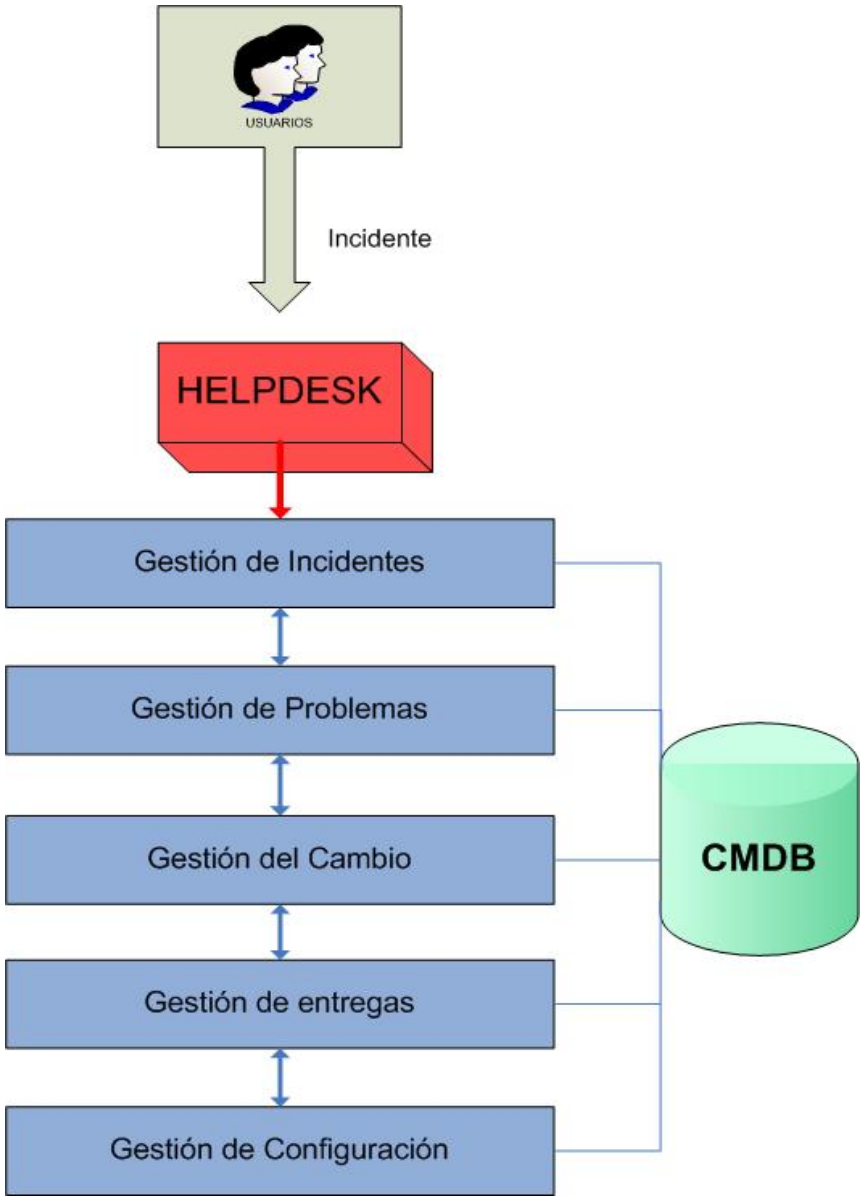


Figura 30.- **Interacción entre ITIL y la CMDB.**
(Fuente: Soporte de Servicio de la OGC)

En la figura 30 se observa cómo el *HelpDesk* es el único punto de atención al usuario, y cómo, todos los procesos se relacionan con la CMDB, que contendrá los datos de todos los CIs que componen la TI en la organización.

Para MISITILEON, una vez aplicada la seguridad a todo el proceso, y en un primer nivel de abstracción, el esquema anterior se vería completado como sigue:

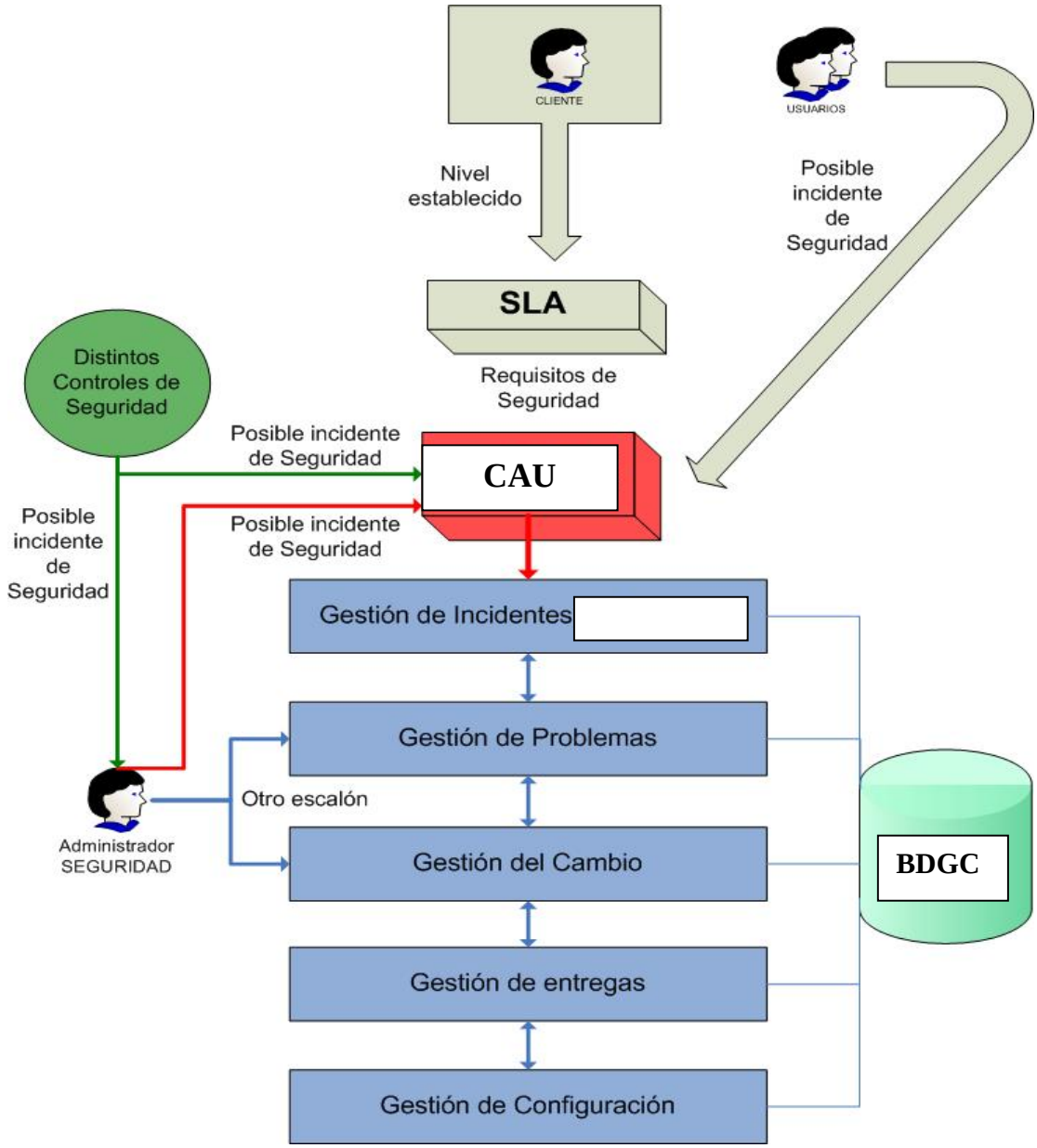


Figura 31.- **Seguridad en la interacción entre MISITILEON y la BDGC.**
(Fuente: propia)

El proceso de Seguridad en MISITILEON se superpone al resto de procesos.

Se puede observar cómo en el gráfico de la figura 31 se han introducido, respecto al gráfico anterior que representaba únicamente los procesos de ITIL, una serie de elementos

y las consiguientes relaciones entre ellos. Estos elementos van a aportar el servicio de seguridad de la información al organigrama de gestión de servicios de la organización y se describen más detalladamente en el siguiente capítulo, en forma de casos de uso.

En los siguientes apartados se describe cada uno de los componentes de MISITILEON.

5.1. CAU

Con la experiencia que la doctorando ha adquirido en estos años, se puede afirmar que, hoy en día, el *HelpDesk* de la TI es el pilar de cualquier negocio pequeño o grande, y la mayoría de los gestores de TI luchan por tener un *HelpDesk* productivo y eficiente.

En MISITILEON se forma a los analistas del CAU para que den el mayor soporte posible a los usuarios que piden nuevos servicios. Se hace comprender a los analistas, gracias a la formación, la importancia que tiene que graben las peticiones con detalles de urgencia y prioridad. Con MISITILEON se pretende que el equipo del CAU no sea un simple *call center* y busque nuevos planes de servicio e hitos.

En MISITILEON es muy importante la formación. Se debe entrenar al personal del CAU en: hacia dónde deberían mirar para responder a las FAQs.

5.2. Gestión del Nivel de Servicio

Los ANSs sirven para definir y comprobar que se mantiene un nivel del servicio acorde con las necesidades y posibilidades de la organización.

El proceso de la Gestión de Niveles de Servicio se encarga de definir, negociar y supervisar la calidad de los servicios TI ofrecidos, alineando tecnología con procesos de negocio y todo ello a unos costes asumidos y contrastados por la organización.

Lógicamente, uno de los servicios a definir y posteriormente mantener es el que se encarga de la Seguridad de la Información en la organización, entendiendo éste en su aspecto más amplio, es decir, aspecto que se irá desarrollando en función del resto de los servicios TI ofrecidos por dicha organización. En definitiva se trata de aportar un servicio más que permita ofrecer el resto con un cierto nivel de seguridad acordado.

El principal instrumento de la Gestión del Nivel de Servicio son los ANSs establecidos entre el cliente y el proveedor y donde realmente se decide el nivel de servicio a adoptar, es decir, la calidad que se espera de todos los servicios TI ofrecidos.

Parece evidente que, uno más de los servicios a “discutir” en el establecimiento de los ANSs es el servicio anteriormente mencionado de la Seguridad de la Información.

El ANS formaliza los requisitos del cliente para los niveles de servicio y define las responsabilidades de todas las partes participantes, para ello se establecen una serie de reuniones que van a determinar, los niveles de seguridad acordados, es decir, las medidas de seguridad a aplicar a la organización.

Estas reuniones, siempre que se considere necesario, contarán con el asesoramiento de personal experto en seguridad.

Para poder hacer efectivas las medidas de seguridad deducidas de los ANSs, será necesario establecer una serie de controles de seguridad.

El conjunto de todos los controles de seguridad de la organización van a constituir el Sistema de Gestión de la Seguridad de la Información.

Se establece aquí una fuerte relación entre la gestión de servicio según ITIL y toda la serie de la normativa ISO 27000, donde, entre otros conceptos, se detalla la definición de dichos SGSI y los controles de seguridad que los constituyen.

En el siguiente gráfico de la figura 32 se observa una representación del principal objetivo, en materia de seguridad, de las reuniones entre cliente y proveedor, constituir los ANSs de seguridad, de la organización:

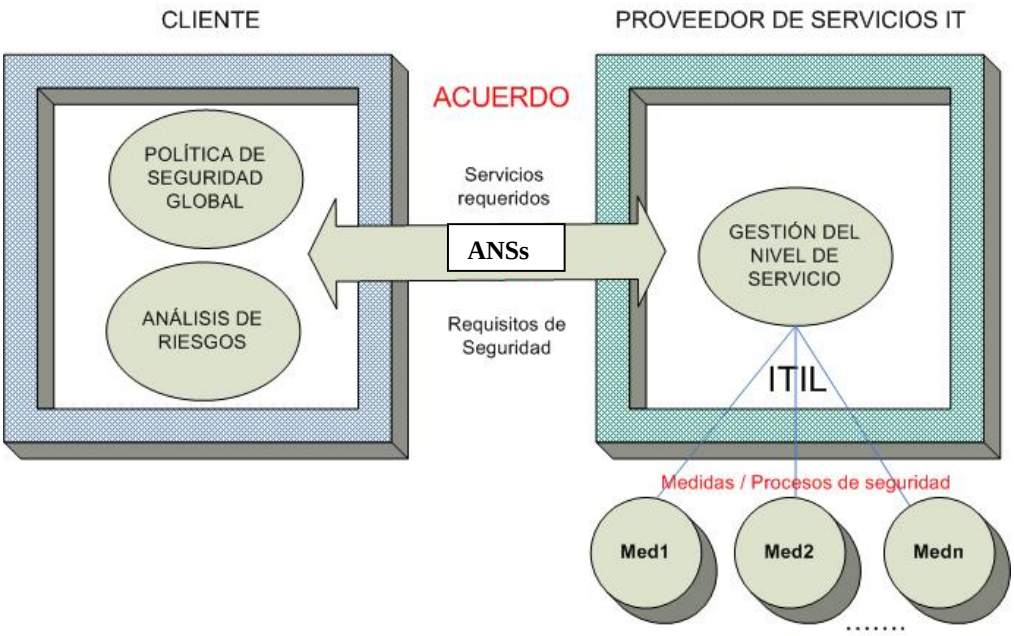


Figura 32.- **ANS: Acuerdo Cliente-Proveedor.**
(Fuente: propia)

Los controles de seguridad, derivados de las medidas de seguridad acordadas, van a necesitar de una serie de procesos que los definan, implementen, mantengan y evalúen, serán los llamados subprocesos o procedimientos de seguridad de la organización los que se encarguen de realizar estas tareas.

El conjunto de todos los subprocesos o procedimientos de seguridad constituirán el proceso general de seguridad.

Para la correcta y coherente definición y aplicación de los procedimientos de seguridad, será necesario disponer en la organización de una Política general de seguridad perfectamente establecida y asumida por todos los componentes de dicha organización.

De las reuniones entre cliente y proveedor se establecerá un nivel acordado de seguridad. Este nivel se podría denominar, en términos específicos de seguridad, Nivel Básico de Seguridad[78].

Evidentemente, la administración del nivel de servicio alcanzado requiere un ciclo continuo de acuerdo, supervisión y creación de informes sobre los logros del servicio de TI, así como tomar las decisiones adecuadas para equilibrar los niveles de servicio con las necesidades y los costos de la empresa, es decir, es posible que dichas necesidades cambien con el tiempo, y sea necesario modificar el nivel de seguridad.

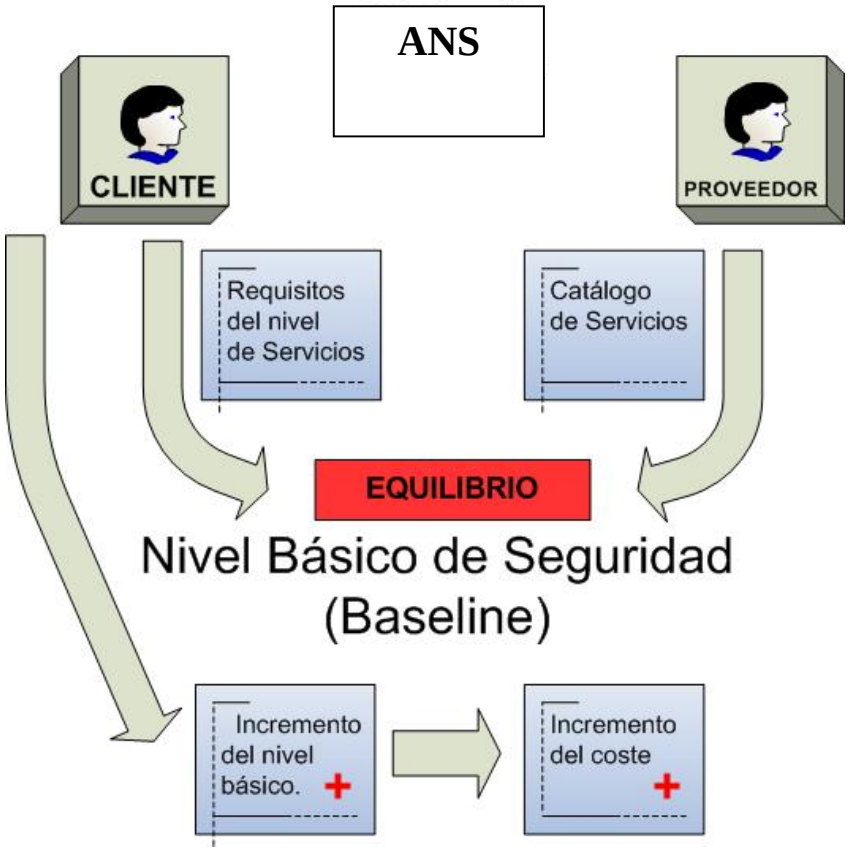


Figura 33.- **ANS: Nivel Básico de Seguridad.**
(Fuente: propia)

[78] En ocasiones denominado *baseline*.

El ANS, como acuerdo, debe quedar reflejado en un documento[79], con un formato predefinido y adaptado a la organización.

Un ejemplo de ANS de seguridad podría ser el que se muestra en la tabla 11:

ANS DE SEGURIDAD	
Identificador	**Nº Secuencial que identifica el documento ANS.**
Titulo	**Título del documento. Identifica el Servicio aportado.**
GENERAL	
Cliente	**Es el cliente, generalmente una organización, con el cual se establece el contrato del Servicio.**
Responsable	**Responsable por parte de la organización cliente del servicio.**
Inicio de Acuerdo	**Fecha de inicio de acuerdo de prestación del servicio. A partir de cuándo el contrato es vigente.**
Fin de Acuerdo	**Fecha de fin de acuerdo de prestación del servicio.**
Impacto	**Indica cómo repercute o impacta el servicio en la organización. Es el valor, por defecto, que tomarán los incidentes.**
Urgencia	**Indica la urgencia con que debe prestarse el servicio. Es el valor, por defecto, que tomarán los incidentes.**
Tiempo de Servicio	**Horario, por defecto, de resolución de los incidentes.**
Tiempo de Respuesta	**Tiempo máximo que puede tomarse el responsable para resolver los incidentes.**
EQUIPO DE TRABAJO	
Responsable del ANS	**Responsable del cumplimiento del servicio por parte de la empresa proveedora del servicio.**
Rol del Responsable	**Rol que ocupa el responsable en la empresa proveedora.**
Integrantes	**Todas las personas que integran los equipos de trabajo.**
Identificador	**Rol**
……	**…**
Identificador	**Rol**
Niveles de Resolución	**Distintos niveles de resolución de incidentes, así como los integrantes que forman los equipos asignados.**
Nivel	**Integrantes Líder**

[79] También podría tratarse de una aplicación informática.

…….	**……**		**…….**	
Nivel	**Integrantes**		**Líder**	
PRIORIDADES DEL INCIDENTE				
Distintas prioridades de incidentes por impacto y urgencia, así como tiempos y niveles de resolución asignados (por defecto).				
Impacto	**Urgencia**	**Prioridad**	**Tiempo**	**Nivel Resol**
……	……	……..	……	**……**
Impacto	**Urgencia**	**Prioridad**	**Tiempo**	**Nivel Resol**
ESCALAMIENTOS				
Funcional	**Posibles escalamientos, de resolución, por porcentaje.**			
Porcentaje	**Acción**		**Nivel a Escalar**	
……	……		**……**	
Porcentaje	**Acción**		**Nivel a Escalar**	
De Notificación	**Posibles escalamientos, de notificación, por porcentaje.**			
Porcentaje	**Notificaciones Fijas**		**Notificaciones Variables**	
…….	……		**……**	
Porcentaje	**Notificaciones Fijas**		**Notificaciones Variables**	
ANEXOS				
Documentos anexos: descripción de medidas y controles de seguridad necesarios, periodos de revisión de los ANS, etc…				

Tabla 11 .- ANS de seguridad.
(Fuente: propia)

La revisión del ANS es un punto de control de la administración clave, que ocurre a intervalos especificados en la propia ANS. Esta revisión tiene el propósito de asegurar que la empresa y la sección de TI tienen la oportunidad de evaluar el rendimiento de sus servicios en base a los objetivos del ANS.

La revisión del ANSs está diseñada para incluir a la administración de alto nivel en el proceso de revisión, asegurando así la implicación y las comunicaciones entre el proveedor de TI y la empresa, en todas las decisiones futuras relacionadas con la provisión del servicio.

5.3. Gestión del Incidente

Se ha tomado la misma definición de "incidente" de ITIL. Un incidente es una interrupción del servicio normal que afecta al usuario y al negocio. El objetivo del proceso Gestión del Incidente es reestablecer a su estado normal los servicios de TI tan pronto como sea posible, con soluciones temporales o definitivas, asegurándose de que ello no afecte al negocio.

Un incidente es un evento que no es parte de la operativa normal; es un evento que no se desea que ocurra, pero que en ocasiones sucede. En otras palabras, la Gestión del Incidente es un proceso para gestionar interrupciones en servicios críticos de TI y restablecerlos, como suele decirse, ASAP[80].

La Gestión del Incidente dice cómo implementar un CAU en la TI que entienda y trabaje según las prioridades del negocio.

La Gestión del Incidente en MISITILEON subraya la necesidad de tener un proceso de reestablecimiento del servicio. La función del CAU es el nexo que une los procesos en un Único Punto de Contacto con el usuario, asegurando así que los servicios de TI se centran en el negocio. A continuación se señalan los hechos principales que suceden a través de este CAU según lo plantea MISITILEON:

[80] ASAP = *As Soon As Possible*, lo antes posible.

Registrar Datos Básicos

Todas las incidencias deben quedar registradas con todos sus datos, incluyendo fecha y hora.

Informar al usuario

El usuario es informando de una interrupción o el usuario pregunta por un nuevo servicio.

- Si está preguntando por un nuevo servicio – Nueva Petición de Servicio.
- Si el usuario está notificando una interrupción o parada – Incidente.

Diagnosticar

Se debe determinar cuándo es un Incidente o no con un diagnóstico básico. Cuando un usuario comunica una incidencia al CAU, el agente del centro debe intentar registrar el mayor número posible de síntomas de la incidencia a modo de un primer diagnóstico.

BDC

Verificar cuándo se puede ayudar al usuario con una solución de la base de datos de conocimiento (BDC).

Asignar el Incidente al Grupo de Especialistas en Soporte

Si está claro que el CAU no puede resolver (con la rapidez suficiente) la incidencia, ésta debe ser escalada inmediatamente para recibir un nivel de soporte más alto. Si la organización tiene un grupo de segunda línea de soporte y el CAU cree que ese grupo puede resolver la incidencia, se envía la misma a la segunda línea (y así sucesivamente).

Ofrecer soluciones

Se debe trabajar cerca del Grupo de Especialistas de Soporte para ofrecer soluciones al usuario.

Cerrar el Incidente con la confirmación del usuario

Siempre debe ser el usuario el que dé la aprobación final y por tanto, hasta que éste no lo confirme al CAU por los canales establecidos, no se puede cerrar el incidente.

En la figura 34 se puede observar el flujo del proceso Gestión del Incidente.

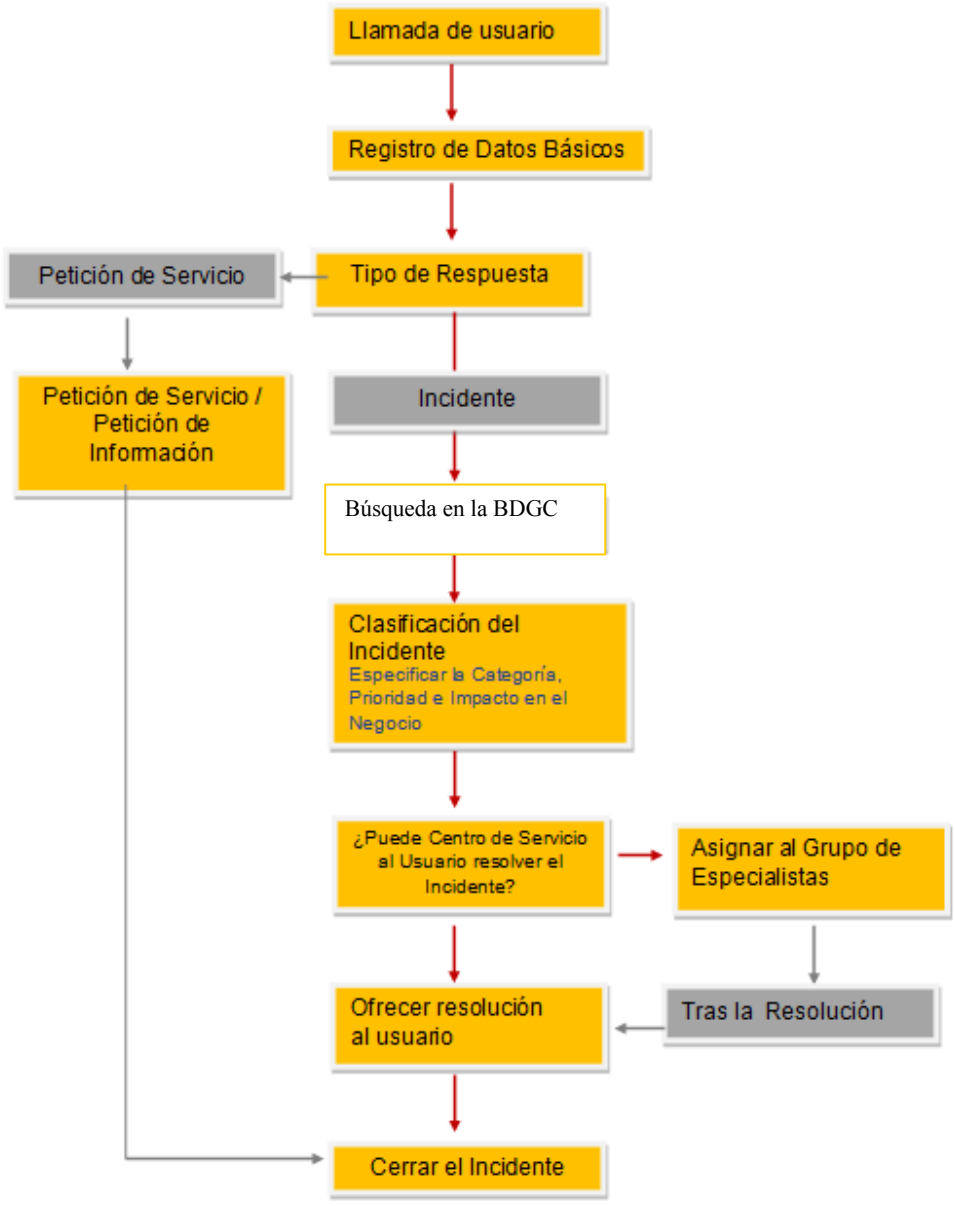


Figura 34.- **Flujograma del proceso Gestión del Incidente en MISITILEON.**
(Fuente: propia)

5.4. Gestión del Problema

El objetivo de Gestión del Problema en MISITILEON es encontrar la causa raíz de los incidentes y reducir el impacto en el negocio. Gestión del Problema es una aproximación proactiva que previene incidentes recurrentes.

Gestión del Problema ofrece una estrategia al CAU de cualquier organización; ayuda a evolucionar de la forma de trabajo en modo "apagafuegos" al modo proactivo. En otras palabras, las interrupciones con las que se encuentran los usuarios suelen ser instancias de un mismo problema. Cuando se encuentra y se elimina la causa raíz de todos los incidentes, también se está previniendo futuros incidentes.

Las tareas que se realizan desde Gestión del Problema de MISITILEON son las siguientes:

Registrar el Problema y cruzarlo con la Base de Datos de Errores Conocidos

Un problema puede surgir por sí solo o ser la combinación de uno o más incidentes. Una vez que el problema se registra, los técnicos de problemas chequearán si ya fue reportado con anterioridad y si se conoce una solución temporal o definitiva.

Problemas que tienen Solución Temporal/Solución Definitiva: Errores Conocidos

Si el problema reportado tiene una solución temporal o definitiva, es un Error Conocido. Los técnicos del CAU pueden darle al usuario una solución temporal o definitiva. Los técnicos deben anotar la ocurrencia del problema e incrementar el contador del mismo para poder evaluar la frecuencia con la que dicho problema aparece.

Clasificar el Problema para Determinar la Prioridad Correcta

En MISITILEON es importante clasificar el problema en Categoría, Subcategoría y Elemento y con los atributos de Impacto en el negocio y Urgencia. La clasificación correcta es vital ya que ayuda enormemente a los técnicos a determinar la prioridad del problema.

Analizar el problema para determinar la causa raíz

Cuando se clasifica un problema, los técnicos tienen una idea clara de por dónde empezar. Si por ejemplo el problema se encuentra en la máquina del usuario, en el servidor *proxy* o en el *firewall*, los técnicos usarán distintas herramientas para diagnosticar y resolver el problema. Los técnicos registran todos los síntomas y las causas raíz relacionadas con las soluciones temporales y definitivas.

Ofrecer una Solución o Iniciar una Petición de Cambio

Los técnicos se ponen en contacto con los usuarios si encuentran una solución disponible. Si el problema requiere algunos cambios en el sistema, pueden ofrecer soluciones temporales e iniciar una Petición de Cambio.

Por ejemplo: Un grupo de usuarios no pueden conectarse a Internet, la causa raíz de ello es el firewall. Los técnicos pueden ofrecer a los usuarios una solución temporal para acceder a Internet y, al mismo tiempo, iniciar una petición de cambio para sustituir el firewall y prevenir así indisponibilidades en el acceso a Internet en el futuro.

Cerrar el Problema

A pesar de que los técnicos de problemas resuelven el problema, es responsabilidad del personal de primera línea de soporte del CAU mantener a los usuarios informados sobre el progreso y las actividades. Cuando los usuarios tienen un único punto de contacto, como es el caso en MISITILEON, no deben ir explicando su situación a diferentes técnicos. Además, el personal de primera línea que ha registrado la llamada debe asegurarse de que la solución cumple exactamente con las necesidades del usuario. Y es en ese momento cuando se procede al cierre del problema.

En la figura 35 se puede observar el flujo del proceso Gestión del Problema.

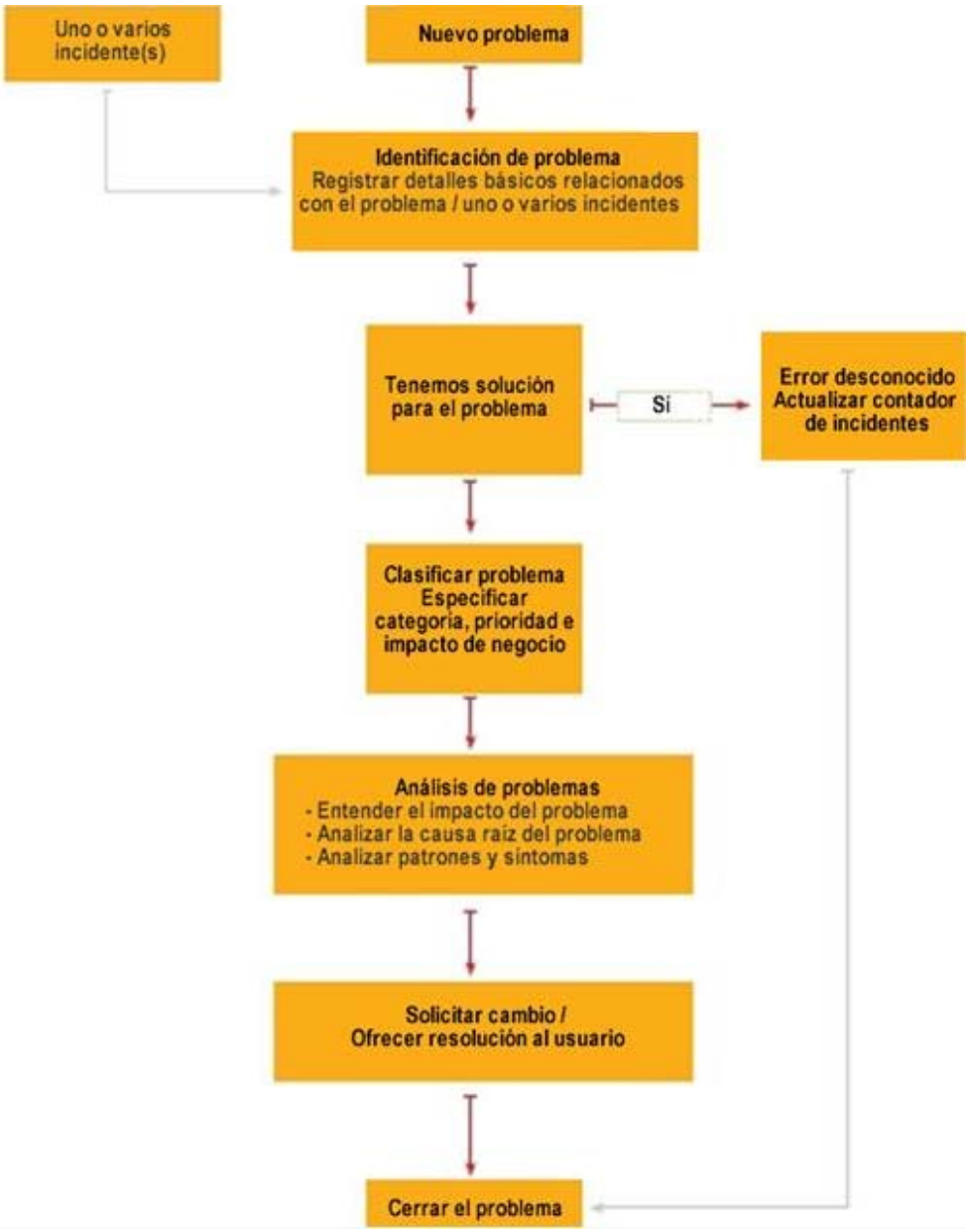


Figura 35.- **Flujograma del proceso Gestión del Problema en MISITILEON.**
(Fuente: propia)

5.5. Gestión del Cambio

El proceso de Gestión del Cambio en MISITILEON ayuda a coordinar los cambios para tener mínimas interrupciones y riesgos aceptables.

La mayoría de los pequeños negocios piensan que la Gestión del Cambio requiere demasiado control y que no es posible implementar un cambio rápidamente cuando se tiene un proceso tan largo. La Gestión del Cambio en MISITILEON no será complicada. Consiste en tener un plan sencillo y organizarse para no tener sorpresas fuera de tiempo.

Da igual qué marco de trabajo se emplee, toda organización, por mínima que sea, necesita la Gestión del Cambio. Ello ayuda a los gestores y al personal de la TI a mantener informados a los ejecutivos y a todos los interesados de los cambios importantes cuando éstos suceden. Cuando todo el mundo (desde los ejecutivos hasta el personal de la TI) está involucrado (desde la toma de decisiones hasta la implementación) no queda espacio para sorpresas no deseadas.

EL planteamiento de MISITILEON es implementar un proceso de Gestión del Cambio sin demasiadas complicaciones para así conseguir un sistema significativo que ayude a la gente y les facilite el trabajo.

Aquí se presenta dicho proceso de Gestión del Cambio sencillo y efectivo que mapea un plan con sentido común hacia ITIL. Las tareas que se realizan en el proceso de Gestión del Cambio son:

Formular un Plan

En primer lugar se debe formular un plan bien definido para minimizar la exposición a riesgos no controlados. Se debe hacer una planificación para minimizar también la gravedad del impacto y la interrupción del servicio. Y como objetivo principal de dicho plan está el implementar el cambio correctamente en el primer intento.

Definir el propósito

Se debe definir claramente cuál es el propósito del cambio, quién lo propone y por qué lo hace.

Clasificar el cambio

Se debe determinar la complejidad del cambio, en el caso de los cambios en MISITILEON la clasificación es: mayor / menor / regular.

Ubicar el cambio

Hay que tener muy claro cuándo y dónde está planeado llevar a cabo el cambio.

Alcance

En este momento hay que preguntarse ¿El negocio se verá afectado cuando se esté implementando este cambio? Para evitar sorpresas de última hora, hay que dimensionar el alcance del cambio.

Reestablecer el servicio

En caso de que fallen los planes de cambio ¿se reestablecerá el último servicio conocido que funcionaba?

Inventariar

Se debe hacer una lista de comprobación de las cosas que se supone que estarán disponibles.

Identificar y obtener aprobación

Es de vital importancia identificar y obtener aprobación de los interesados que podrían verse afectados por el cambio.

Priorizar y programar

Hay que establecer cuál debe ser la prioridad el cambio (en función de su importancia, urgencia y demás). Una vez determinada su prioridad, hay que programar el momento en el cual se llevará a cabo el cambio.

Probar

Antes de implementar el cambio, hay que probarlo en un entorno controlado.

Documentar

Tan importante como el resto de pasos es dejar constancia de lo que ha sucedido durante el proceso. Hay que preguntarse ¿Cómo ha ido el cambio? Y anotar todos los fallos.

Mejorar

Siempre se aprende algo en cada implementación, así que se debe tomar buena nota de las debilidades y fortalezas para mejorar el plan la próxima vez.

En la figura 36 se puede observar el flujo del proceso Gestión del Cambio.

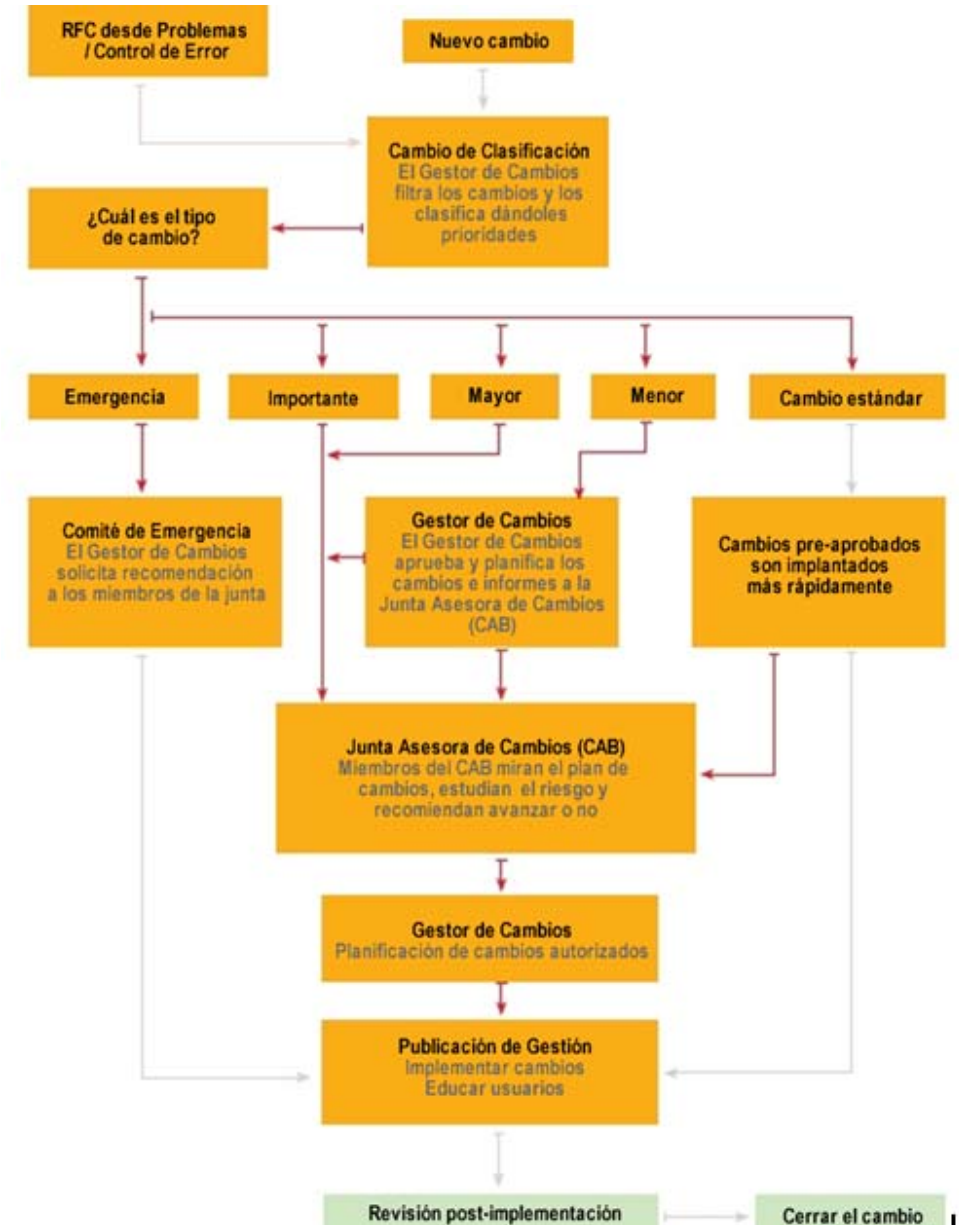


Figura 36.- **Flujograma del proceso Gestión del Cambio en MISITILEON.**
(Fuente: propia)

5.6. Gestión de la Versión

El proceso Gestión de la Versión trata de cómo se entrega el servicio.

La Gestión de la Versión en MISITILEON trabaja codo con codo con la Gestión del Cambio, lo cual es de suma importancia. La Gestión del Cambio es responsable de planificar y el objetivo de la Gestión de la Versión es ejecutar/implementar además de dar formación de los usuarios.

Véase un ejemplo de la vida cotidiana. Siempre que hay obras de reparación de tuberías importantes en una calle concurrida, el tráfico no puede interrumpirse de improviso. Las autoridades municipales informan a través de periódicos y TV a los que circulan por dicha calle, para que sepan que la calle va a ser cortada en un día concreto y les ofrecen rutas alternativas. Así los viajeros son capaces de planificar las cosas por adelantado de forma que se evitan decepciones y los cambios se hacen suavemente.

Desde la perspectiva de la TI, la Gestión de la Versión ayuda a desarrollar cambios en la TI suavemente sin ninguna interrupción. A continuación se presenta cómo realizar Gestión de la Versión con MISITILEON:

Planificar

Un plan de Gestión de la Versión con información relativa a qué desplegar, cómo hacerlo y especificaciones en las que se trabajará.

Probar

La estructura/cambio de lo desplegado se prueba a fondo es condiciones de test similares a las condiciones reales.

Línea Base

Se graban los valores de configuración de la línea base antes de aplicar los cambios.

Distribuir

Se lanza y distribuye según el plan.

Verificar

Se verifica y prueba si los cambios solicitados se han cumplido.

5.7. Gestión de la Configuración y la BDGC (Base de Datos de la Gestión de la Configuración)

Según Mike Glenn (FedEx) "La información sobre un paquete es tan importante como el propio paquete". Con esto se quiere subrayar que la BDGC reviste una importancia fundamental.

La BDGC en MISITILEON es equivalente a la CMDB de ITIL. Como MISITILEON es una metodología respetuosa con el castellano, una mejora respecto a ITIL es dejar sus siglas en dicho idioma[81].

El objetivo de la BDGC es construir y mantener una BD de activos: hardware, software, documentos y sus relaciones.

La idea principal que subyace a la BDGC es construir un repositorio de activos de forma que éstos puedan ser identificados, controlados y gestionados de manera única.

♦ *¿Qué contendrá la BDGC?*

La BDGC debería contener información de todos los componentes críticos del negocio, a saber:

• Las Personas: Nombres de usuario, departamento al que pertenecen, localidad, etc…

[81] Licencia de la autora.

• Los Activos: Todos los activos que son parte del negocio tales como estaciones de trabajo, escritorios, *routers*, impresoras, etc…

• El Software: Todo el software comercial con sus licencias que esté instalado en el entorno TI.

Los activos y componentes de la BDGC son conocidos y en MISITILEON se les llama Elementos de Configuración (ECs)[82].

♦ ***¿Por dónde se debería empezar?***

Lo primero que se necesita implementar para la BDGC de MISITILEON es el mapa de la estructura que va tener esa BD. Aquí se presentan algunas guías de proceso que pueden ayudar a esbozar un buen plan.

Hay que tener siempre presente que el objetivo de la BDGC es construir un repositorio de activos con toda la información de los mismos.

Un repositorio de activos puede ser lógico y distribuido, construir una BDGC no significa intentar tener todo en una BD física enorme. Es decir, la BDGC no tiene que contener toda la información físicamente, sino que lo que contiene esta BD son las referencias de todos los ECs existentes en la organización.

Por ejemplo: en MISITILEON es esencial que exista una Biblioteca de Software Definitivo (BSD). Con versiones de software cada poco tiempo y parches de seguridad

[82] En ITIL los elementos de configuración se llaman CI (*Configuration Item*).

semanales, es importante incluir las copias del software en un entorno vivo. Si uno de los servidores más importantes de una organización se cae y se dispone del número de versión del software, pero no la copia exacta de dicha versión, en esa organización podrían encontrarse con graves problemas. Según este sencillo ejemplo, en la BSD estaría la copia física de dicho software y en la BDGC estaría la referencia (el "puntero") a dicho software.

- ***Tener una Línea Base de Configuración***

Una línea base de configuración es una "foto" de un instante determinado de la BDGC.

En todo entorno de TI hay numerosos sistemas con diferentes configuraciones, software, memoria, procesadores, periféricos, etc... Cuando se tienen tantas variables, hay que asegurarse de que cualquier cambio que se haga soporte todas las versiones.

Los gestores de TI deben planificar y reducir el número de variables de tal forma que se tenga todo bajo control.

En una organización que aplica MISITILEON se podría establecer un sistema operativo y un navegador de versiones estándares, y asegurarse así de que todo el mundo usa la configuración de línea base óptima.

En MISITILEON se debe definir una línea base para asegurarse de que todas las aplicaciones del negocio funcionan con normalidad utilizando una serie de parámetros. A continuación se muestra un ejemplo muy sencillo:

• SO Estándar – Windows xp.

• RAM – 1 GB.

• Procesador - Intel Mobile Centrino.

• Navegador Soportado – IE 7.

6. Gestión de la Seguridad.

La desconfianza es la madre de la seguridad[83].

Este proceso es otro de los componentes de la metodología, pero como tiene gran importancia en esta tesis doctoral, requiere un apartado independiente del resto de componentes de MISITILEON.

En este apartado se desgrana la opción elegida[84]: La seguridad como un Servicio más gestionado por MISITILEON.

6.1. Introducción a la Seguridad como un Servicio más gestionado por MISITILEON.

Al igual que existen una serie de procesos que permiten gestionar servicios propios de las TI, existirá en MISITILEON otro proceso, formado a su vez por subprocesos, que va a permitir administrar o gestionar la seguridad en la organización, es decir, que va a proporcionar servicios de Seguridad de la Información.

Los pilares donde descansa cualquier sistema de Seguridad de la Información son los siguientes:

[83] Aristófanes (444-385 a. C.).
[84] De las dos planteadas en el apartado 1.4 de este capítulo (Dos Posibles Enfoques para la Seguridad).

- **Confidencialidad**: Proteger la información sensible de accesos no autorizados.
- **Integridad**: Asegurar que la información se mantiene completa y precisa.
- **Disponibilidad**: Mantener la información y los sistemas disponibles cuando éstos se requieran.

Para conseguir estos objetivos se necesitan una serie de funciones, implementadas por procesos, que van a formar parte del sistema de seguridad de la organización. Estas funciones, necesitan de una estructura y gestión para que puedan ser ofrecidas como servicio con los niveles de calidad acordados con el cliente o usuario de la TI.

Algunos ejemplos de funciones de seguridad en el sistema y que van a ser, por tanto, aportadas como servicios de seguridad, podrían ser:

- Gestión de la defensa perimetral en la organización.
- Gestión de los sistemas antivirus y otros códigos maliciosos.
- Gestión centralizada del registro de eventos.
- Etc.

Para poder llevar a cabo correctamente estas funciones, éstas se subdividen o apoyan en tareas, fundamentadas en la seguridad, como pueden ser:

- Identificación.
- Autenticación.

- Control de acceso.
- Confidencialidad.
- Integridad.
- No repudio.
- Auditorias.
- Análisis de vulnerabilidades.
- Etc.

Todas estas tareas o procesos que se "añaden" al sistema o estructura de Gestión de Servicios, y en los que se profundizará en el apartado siguiente, deben estar perfectamente integrados en el mismo, es decir, no se van a tratar como elementos aislados, sino que formarán parte activa en ejecución y relaciones con el esquema adoptado por la organización.

El propósito de una infraestructura TI es proporcionar a una determinada organización los sistemas necesarios para su buen funcionamiento, funcionamiento normalmente sustentado en el tratamiento y comunicación de la información.

La información mantenida en una organización (así como los sistemas donde se soporta) están sometidos a una serie de amenazas de las cuales es necesario protegerse, es decir, requieren de la aplicación y gestión de una seguridad.

Como el tema de la seguridad es muy amplio, este trabajo se centra en una serie de procesos, principalmente aquellos orientados a la gestión o administración de dicha seguridad. El resto de procesos se implementarían de forma análoga.

Es importante hacer una referencia al concepto de la imposibilidad de la seguridad absoluta. Este concepto expone cómo, una vez que se conectan los sistemas a redes, y con más razón, si esas redes son públicas (como Internet) lograr una seguridad absoluta, es decir, sin ningún tipo de riesgo para esos sistemas y la información que contienen, es prácticamente imposible. La gestión de la seguridad es el proceso de gestionar un nivel definido y acordado con la organización, según el nivel de seguridad al que quiera llegar [OCGSM99].

Los gestores o administradores de la seguridad son los responsables de tomar o mantener las medidas apropiadas para reducir los riesgos, de tal forma que se alcance, y se mantenga, el nivel de seguridad acordado con el cliente[85].

Es importante mencionar que una condición necesaria para el éxito en cuestiones de seguridad, es que todo el personal de la organización, en sus diferentes niveles (estratégico, táctico y operacional) debe estar implicado. Por lo tanto, la dirección de la organización deberá apoyar todas las fases de los procesos de seguridad.

[85] En el apartado 6.1.5 de este capítulo se explica en detalle cómo se establecen los niveles de seguridad (ANSs).

Los sucesos o incidentes de seguridad, que como más adelante se detallará, son elementos clave en la gestión de la seguridad, podrán afectar a los tres pilares donde descansa la información, esto es, la confidencialidad, la integridad y la disponibilidad, aunque indudablemente, dependiendo del tipo de organización y de la información que ésta maneje, dichas variables se verán más o menos afectadas. Así, por ejemplo, en un entorno de defensa primaría la confidencialidad, en un entorno financiero, la integridad y en un entorno de urgencias hospitalarias, la parte más importante sería la disponibilidad. Evidentemente, esto no quiere decir que no haya que tener en cuenta el resto de variables, que como se comentó, son pilares básicos de la seguridad.

Una vez claras las medidas de seguridad que se necesitan implantar y mantener en la organización, el siguiente paso es desplegar dichas medidas de seguridad, en forma de controles de seguridad, por los diferentes sistemas de la organización. Estos controles de seguridad van a necesitar de una serie de procesos que los planifiquen, implanten, mantengan, evalúen y mejoren de forma continua, es decir, que los gestionen. Estos procesos, encargados de gestionar el servicio de seguridad, serán los denominados procesos o subprocesos de seguridad, y el conjunto de todos ellos es lo que vendrá a formar el proceso de Gestión de la Seguridad MISITILEON.

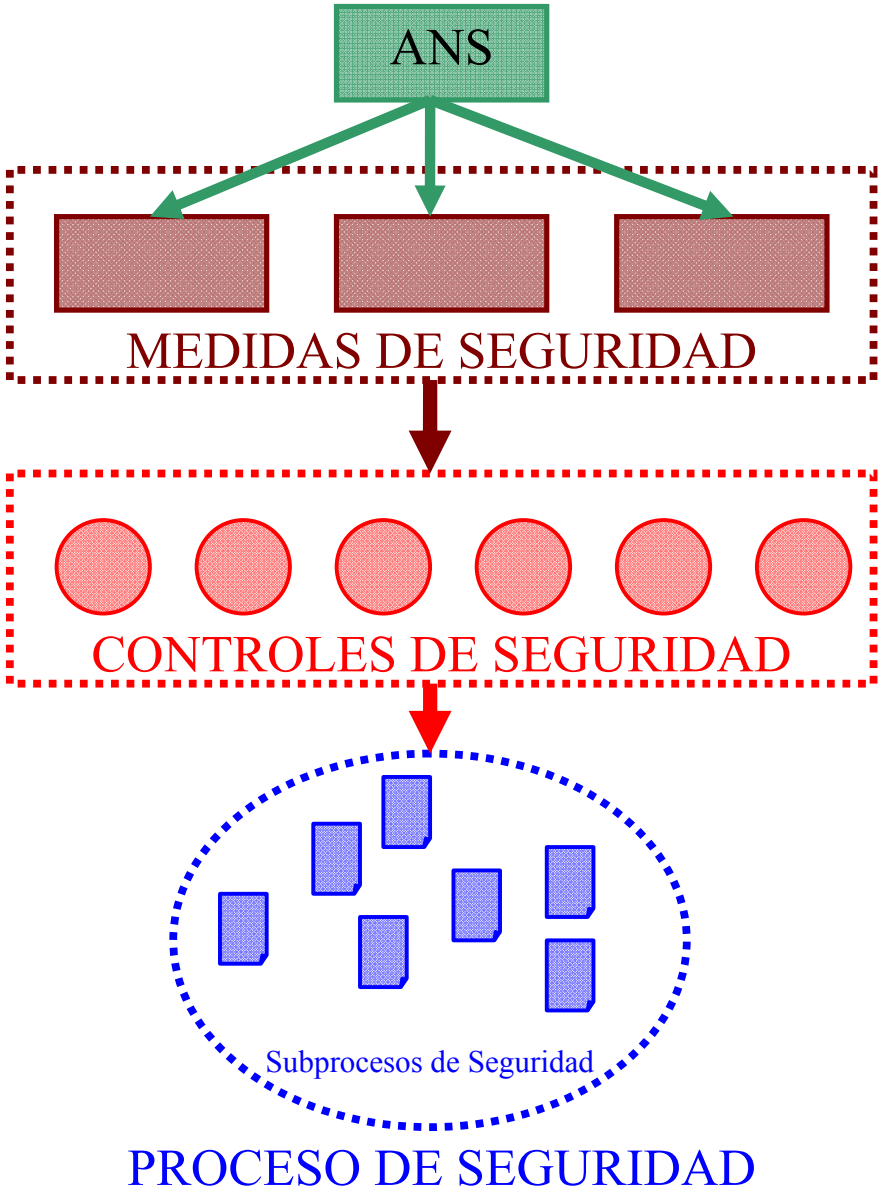


Figura 37.- **Proceso de Gestión de la Seguridad.**
(Fuente: propia)

Basándose en la norma ISO 17799[86], el proceso de Gestión de la Seguridad MISITILEON, y todos aquellos subprocesos que lo forman, tendrán una misma estructura, la cuál se compondrá de las siguientes fases:

[86] Y posteriormente, en la norma ISO 27002.

- **Control:** Organiza y dirige el proceso de Gestión de la Seguridad TI, define todos los subprocesos, funciones, roles y responsabilidades, estableciendo el marco de trabajo para cumplimentar el proceso concreto de forma que esté perfectamente coordinado con el resto de los procesos de gestión TI.

- **Planificación:** Especifica la forma de llevar a cabo las medidas de seguridad concretada en el ANS; su línea debe marcarse por la Política de Seguridad de la organización.

- **Implementación:** Desarrollo de las medidas de seguridad planeadas. Normalmente, se trata de poner en funcionamiento los controles de seguridad necesarios para satisfacer las medidas de seguridad. Estos controles pueden ser herramientas de seguridad, establecimiento de procedimientos, etc.

- **Evaluación:** Su objetivo es mantener la eficacia de los diferentes controles de seguridad, que son indispensables para cerrar el bucle. La consecuencia de esta evaluación puede ser la actualización o sustitución de medidas, controles, etc.

- **Mantenimiento:** Las posibles amenazas, así como la propia infraestructura de la organización, evolucionan con el tiempo, por lo tanto, las medidas de seguridad están sujetas a actualizaciones constantes. Es importante que las medidas de seguridad y los diferentes controles que las conforman estén documentados, por lo que es necesario que esa documentación también sea mantenida.

- **Informes:** En el proceso de la seguridad, el almacenamiento y la presentación de los distintos incidentes de seguridad son una parte muy importante en el desarrollo de los distintos procesos. Es una actividad interna, por lo que va a depender de otros procesos que la nutran.

  Debe existir una buena base de datos de incidentes de seguridad, entre otras cosas, para poder realizar un seguimiento de todos los incidentes de seguridad de la organización, así como disponer de argumentos necesarios para demostrar que se requieren medidas específicas.

En este punto, se encuentra una fuerte relación entre la definición de un proceso de seguridad MISITILEON y la implementación de un control de seguridad según la norma ISO 17799[87]. En el siguiente gráfico de la figura 38 se muestra cómo se ha realizado para MISITILEON la integración de un control de seguridad, según lo definiría la normativa ISO.

[87] Y posteriormente, en la norma ISO 27002.

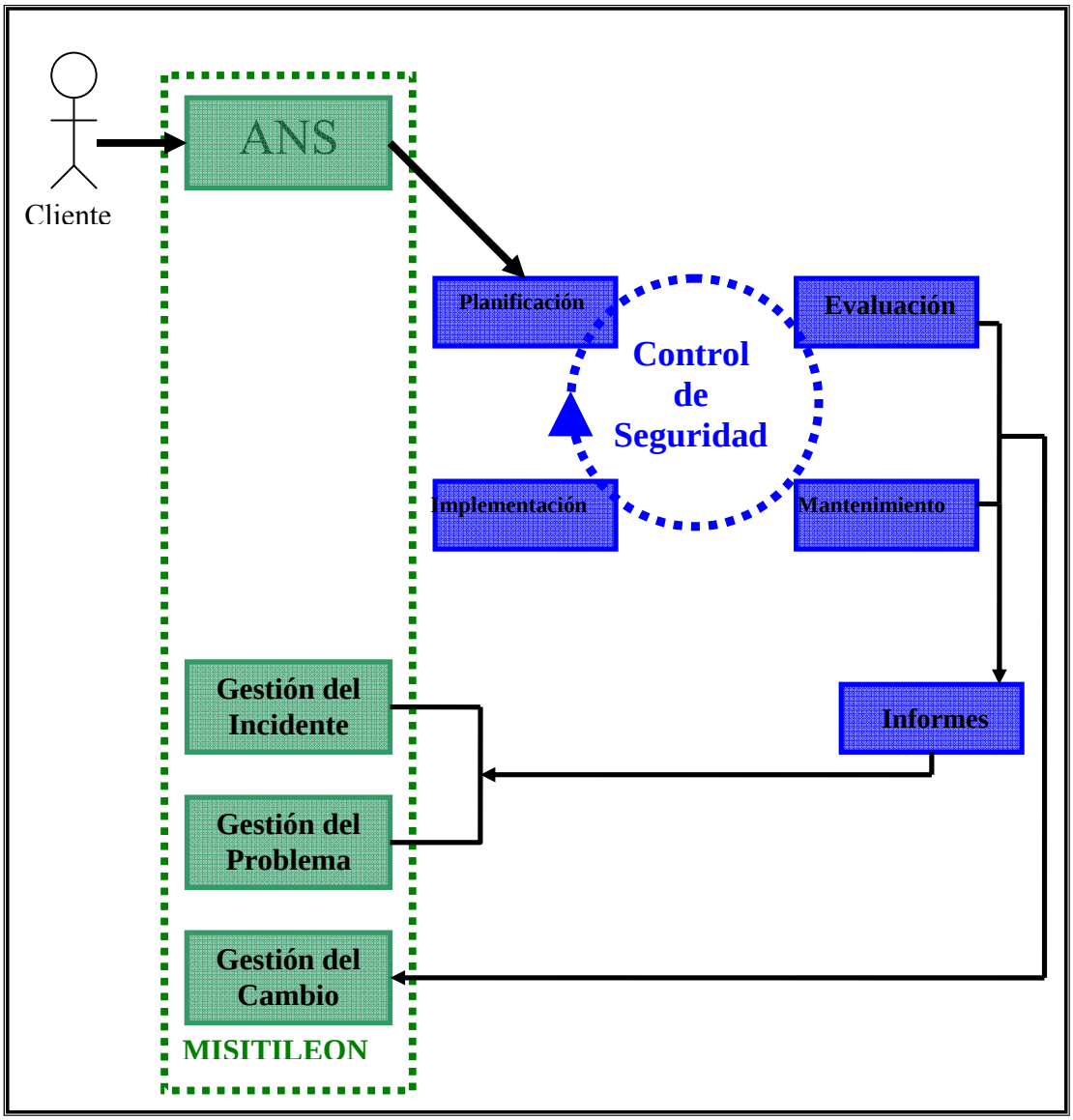


Figura 38.- **Control de Seguridad según MISITILEON.**
(Fuente: propia)

6.2. Rol y Responsabilidad del Gestor y del Administrador de Seguridad en el modelo MISITILEON.

Las dos figuras que van a representar estos procesos de gestión y administración de la seguridad son:

- Gestor de la Seguridad[88].
- Administrador de Seguridad[89].

6.2.1. Diferencias entre el Gestor y el Administrador de Seguridad.

A veces es difícil diferenciar las funciones del Gestor (también denominado Director de Seguridad) y el Administrador de Seguridad, de tal forma que en muchas organizaciones dichas funciones se concentran en una única figura.

Si embargo si se profundiza, estas diferencias se pueden encontrar a nivel organizacional. El Gestor de Seguridad tiene responsabilidades más estratégicas, centradas en la organización y la gestión; mientras que para el Administrador de Seguridad, la responsabilidad es más a niveles táctico y operativo.

Una descripción general de cada una de las figuras y de las actividades desarrolladas por éstas, sería: [MSM05]

Gestor de Seguridad:

Es el responsable de la valoración, resolución y mantenimiento de los requisitos de seguridad dentro de la organización.

Debe asegurar que en la organización se desarrollan estrategias efectivas para:

[88] *Security Manager*.
[89] *Security Administrator*.

- Identificar las necesidades más importantes para desarrollar un entorno seguro.
- Clasificar los distintos tipos de datos y el nivel de seguridad asociado a éstos.
- Identificar y documentar reglas de seguridad básicas para el negocio de la organización.
- Detectar los riesgos de seguridad.

Administrador de Seguridad:

Es el responsable de la gestión de la continuidad de la infraestructura de seguridad en la organización. Una vez que la política de la organización ha sido definida y los mecanismos de seguridad han sido identificados, el administrador realiza las siguientes tareas:

- Establece la configuración detallada de las soluciones de seguridad.
- Desarrolla las medidas de seguridad adoptadas.
- Mantiene el despliegue de los controles de seguridad.
- Monitoriza los distintos componentes o controles de seguridad.
- Evalúa los problemas de seguridad potenciales que puedan ocurrir en los sistemas.
- Prepara informes con las salidas de los controles de seguridad.
- Responder a los incidentes de seguridad escalados por el CAU.

6.2.2. El Gestor y el Administrador de Seguridad en MISITILEON

El Gestor de Seguridad estaría más encuadrado en la relación del proceso de seguridad con procesos propios de la Entrega del Servicio de ITIL, mientras que el Administrador de Seguridad encaja en la relación con el conjunto de Soporte del Servicio.

Figura 39.- **Gestión y Administración de Seguridad en MISITILEON.**
(Fuente: propia)

Seguidamente se representan una serie de diagramas de Casos de Uso en lenguaje UML[90], y la posterior explicación, con las diferentes acciones de los dos roles, Gestor y Administrador de Seguridad, dentro de los procesos MISITILEON.

[90] *Unified Modelling Language*, Lenguaje Unificado de Modelado.

El Gestor de Seguridad y MISITILEON:

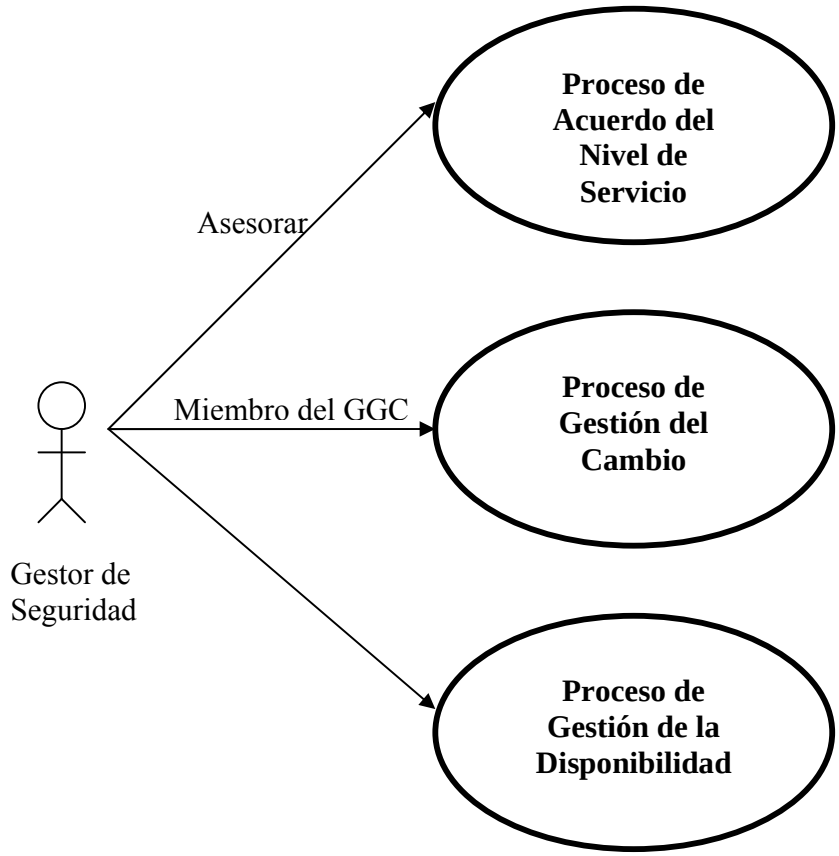


Figura 40.- **El Gestor de Seguridad y MISITILEON.**
(Fuente: propia)

- **Proceso de Acuerdo de Nivel de Servicio**: El Gestor de Seguridad puede participar en funciones de asesoramiento en el proceso de Acuerdo del Nivel de Servicio. Como parte de las necesidades del cliente es necesario definir un acuerdo del nivel de los requisitos de seguridad incluidos en el ANS. El Gestor de Seguridad puede

participar en esos acuerdos identificando las necesidades y riesgos más importantes para desarrollar un entorno lo suficientemente seguro.

- **Proceso de Gestión del Cambio**: Bien porque se hayan detectado vulnerabilidades en algunos sistemas, bien porque se necesite cambiar un sistema por cualquier otro motivo, en la Gestión del Cambio es necesario tener en cuenta que dicho sistema debe mantener el valor de seguridad acordado en el ANS. Es por tanto recomendable, sobre todo en el primero de los casos, que el Gestor de la Seguridad sea miembro activo del GGC para ese cambio.

- **Proceso de Gestión de la Disponibilidad**: Una de las principales funciones del Gestor de Seguridad es participar en la definición y ejecución de los planes de contingencia, piezas clave en el proceso de Gestión de la Disponibilidad.

El Administrador de Seguridad y MISITILEON:

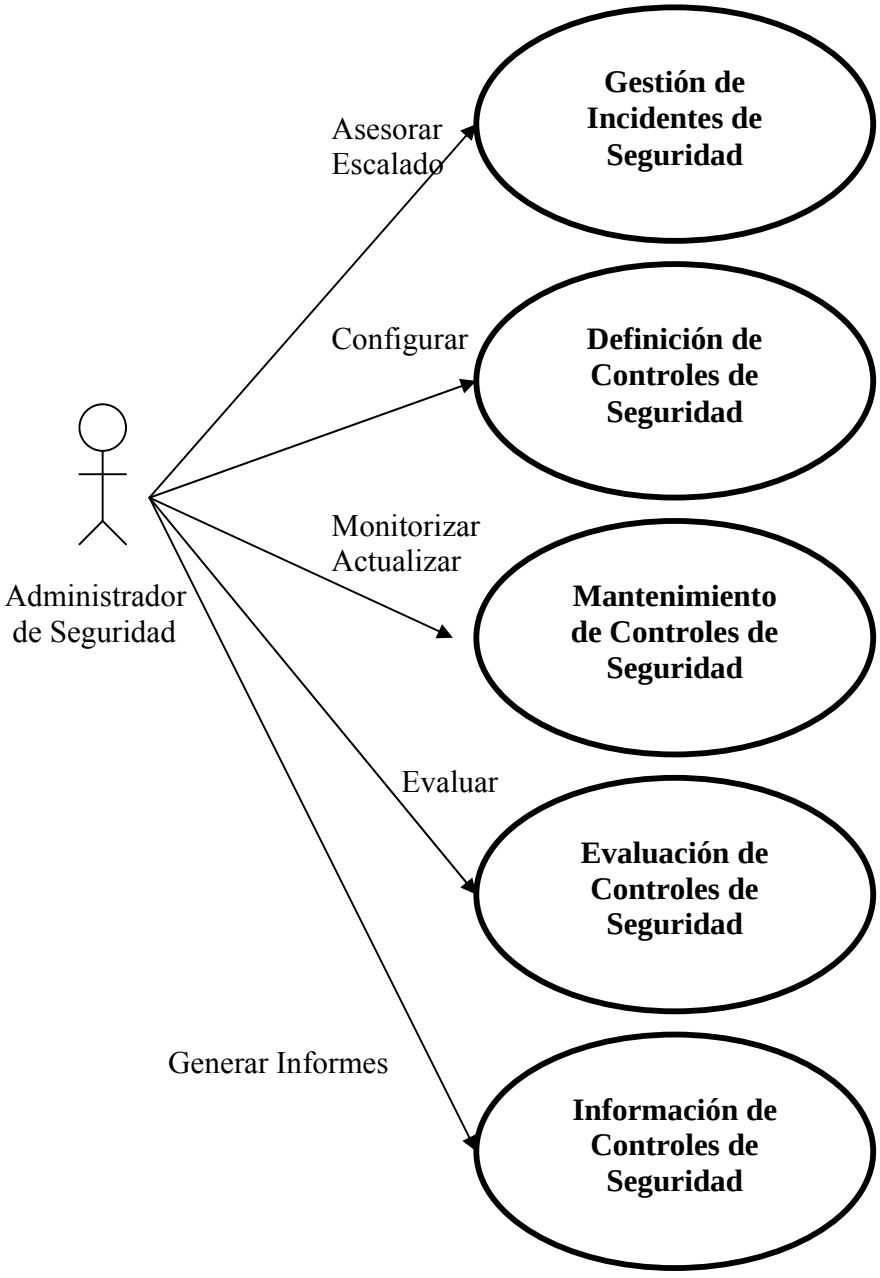


Figura 41.- **El Administrador de Seguridad y MISITILEON.**
(Fuente: propia)

- **Proceso de recogida de incidentes**: El Administrador de Seguridad realizará tareas de monitorización de los controles de seguridad, parece evidente que sean una de las principales fuentes de comunicación de incidentes al CAU .

- **Gestión de incidentes de seguridad**: Los incidentes de seguridad necesitan un tratamiento especial, normalmente no son competencia del CAU. Una vez registrado y catalogado el incidente, éste es escalado a personal técnico especializado en seguridad. Parte de este personal puede ser (o bien contar con su asesoramiento) el Administrador de Seguridad.

- **Definición de controles de seguridad**: Una de las principales funciones de los Administradores de Seguridad es la configuración detallada de las soluciones de seguridad, es por tanto un componente esencial en el desarrollo y definición de los controles de seguridad. El Administrador de Seguridad es el que implementa la configuración definida en el ANS, de forma que se alcance el nivel de seguridad acordado.

- **Mantenimiento de controles de seguridad**: Además de alcanzar dicho nivel de seguridad, ese nivel debe ser mantenido durante todo el ciclo de vida del sistema. El Administrador de Seguridad realiza estas funciones de mantenimiento en los diferentes controles de seguridad desplegados por la organización. Tareas como la actualización de los sistemas son fundamentales para mantener dicho nivel.

- **Información de los controles de seguridad**: Dentro del ciclo de vida de un control de seguridad, una de las etapas más importantes es la realización de informes con las salidas de dicho control. Estos informes se utilizarán posteriormente para detectar y facilitar la resolución de los incidentes de seguridad.

- **Evaluación de los controles de seguridad**: Los informes anteriormente descritos van a servir también para valorar la eficacia del propio control de seguridad. En función del resultado de los informes, el Administrador de Seguridad será el más indicado para evaluar los problemas de seguridad, es decir, detectar las diferentes vulnerabilidades que puedan presentar los servicios TI de la organización.

En el siguiente capítulo se presenta la experimentación que demuestra la viabilidad de todo lo expuesto en este capítulo.

6.3. Gestión de Incidentes de Seguridad. Integración con el CAU (HelpDesk).

El CAU[91] es el único punto de contacto entre el proveedor del servicio y el propio usuario del sistema. Esta unicidad hace que todos los incidentes detectados por los usuarios, incluidos los incidentes de seguridad, deban comunicarse al proceso de Gestión del Incidente por medio del referido *HelpDesk*.

En cuanto a la consideración de incidente, como incidente de seguridad, es interesante particularizar un par de aspectos:

[91] También denominado Centro de Servicio al Usuario.

- **1º.-** El tratamiento de **Confidencialidad** de los incidentes de seguridad:

  Es importante conocer qué personas están implicadas, o tienen conocimiento del incidente, con el fin de minimizar ese número de personas. Un incidente de seguridad, muchas veces se produce por una vulnerabilidad en un sistema, por consiguiente cuantas menos personas conozcan esa vulnerabilidad, menos inseguro es el sistema.

- **2º.-** El tratamiento de **Actuación Inmediata** de los incidentes de seguridad:

  El principal objetivo de la función *HelpDesk* es dar continuidad de servicio al cliente. En el caso de los incidentes de seguridad, esta continuidad se ve seriamente condicionada por una respuesta inmediata ante el incidente acaecido.

Un incidente de seguridad normalmente conlleva la pérdida de alguna de las variables que fundamentan la seguridad: confidencialidad, integridad o disponibilidad, si el incidente no es inmediatamente solucionado es muy probable que la acción de dicha variable se vea más afectada, o bien, se sufra la pérdida del resto de las variables.

Así, por ejemplo, un atacante que penetra en un sistema de la organización, puede limitarse al hecho de haber burlado la protección de dicho sistema, pero si no es rápidamente neutralizado, puede ocasionar graves pérdidas de información (pérdida de la confidencialidad), modificar esa información (pérdida de integridad) e incluso afectar a la funcionalidad (pérdida de disponibilidad).

En el sentido procesal, para el *HelpDesk*, los incidentes de seguridad no son diferentes de otros incidentes, es decir, son registrados y catalogados como los demás. El *HelpDesk* es el propietario de todos los incidentes [OGCSM99].

Sin embargo es evidente, por las características anteriormente comentadas de la confidencialidad y la necesidad de acción inmediata (implícitas en los incidentes) que habrá determinados incidentes de seguridad que llevarán asociados procedimientos de mayor prioridad que el resto de los incidentes.

Es fundamental, por tanto, que el primer nivel de recogida de incidentes, sea capaz de catalogar la importancia del incidente de seguridad y si éste va a necesitar un tratamiento especial.

¿Cómo se determina que un incidente de seguridad necesita un tratamiento especial?

Una propuesta de solución pasa por que el CAU disponga de una serie de incidentes "tipo" sobre los que debe actuar directamente, es decir que sigan el procedimiento normal, y otra serie de incidentes que requieran un escalado y por tanto tengan asociado una clasificación y un tratamiento especial.

Véase el gráfico de la figura 42 que muestra esta alternativa:

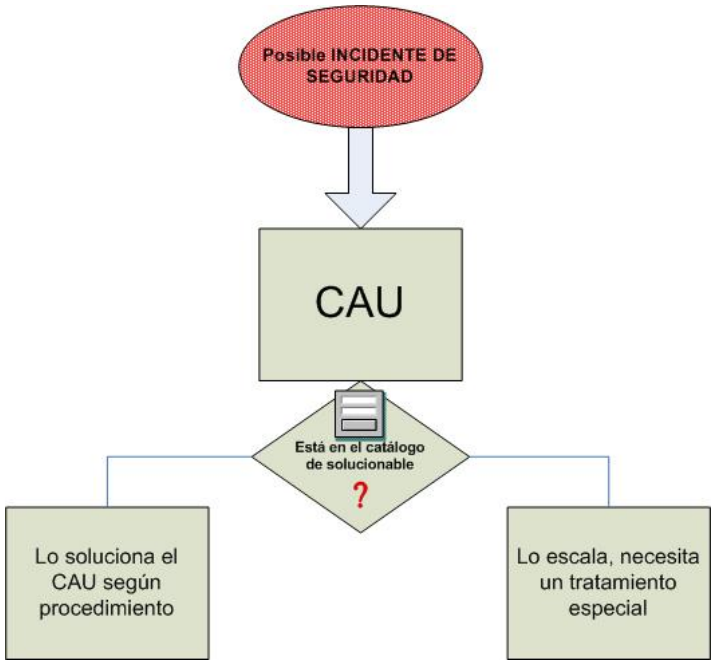


Figura 42.- **Gestión de Incidentes de Seguridad en MISITILEON.**
(Fuente: propia)

Ejemplos:

- Si una cuenta se bloquea porque un usuario ha introducido mal una clave, el CAU dispone de un procedimiento "normal" de solución ante este incidente.

- Si una cuenta se bloquea sin la acción consciente del usuario, o se bloquea muchas veces en una hora, se está produciendo un incidente o un problema de seguridad, que el CAU deberá escalar, es decir, necesita un tratamiento especial.

El tratamiento especial del incidente, clasificado como incidente de seguridad, llevará consigo las siguientes premisas:

- Su gestión se separará del resto de los incidentes, esto quiere decir que sólo será accesible para un determinado grupo de personas.[92]

- La Base de Datos donde resida será distinta de la del resto de incidentes.

- Las notificaciones serán restringidas, y estarán perfectamente predeterminadas, pudiendo implicar escalado a otros organismos.

Independientemente de este tratamiento especial, no debe olvidarse, que el incidente de seguridad siempre será notificado y registrado por *HelpDesk*.

Para poder llevar a cabo una correcta gestión de los incidentes de seguridad es fundamental que *HelpDesk* reconozca éstos como tales.

Algunos incidentes típicos de seguridad son: [OGCSM99]

Incidentes típicos de Seguridad	
Infracción de la Confidencialidad	• **Posible acceso no autorizado a la información.** • **Pérdida de datos.** • **Pérdida o robo de portátil.** • **Intento de adquirir autorizaciones más elevadas que las adjudicadas por la organización.** • **Intento de acceder (desde el exterior o desde la propia organización) a sistemas no autorizados.**
Infracción de la	• **Pérdida de datos o transacciones incompletas.** • **Virus, Troyanos, etc[93].**

[92] Administradores de Seguridad, Oficial de Seguridad, Responsables del sistema afectado,…
[93] En general, los denominados software malicioso.

Incidentes típicos de Seguridad	
Integridad	• **Discos con pistas defectuosas, errores de paridad de memoria.** • **Fallo de chequeos o valores *hash*.**
Infracción de la Disponibilidad	• **Interrupción del servicio un periodo de tiempo inaceptable (superior al acordado en la ANS).** • **Software malicioso.** • **Robo de portátiles, componentes o datos.**

Tabla 12 .- Incidentes típicos de seguridad.
(Fuente: propia)

Por último, un correcto registro de los incidentes de seguridad permitirá una mejor gestión de los problemas ocasionados por los propios incidentes, a la vez que posibilitará analizar la efectividad de las medidas de seguridad y los posibles riesgos a los que está sometida la organización.

Un posible registro de un incidente de seguridad estaría formado por los siguientes campos: [OGCSM99]

Registro de Incidente de Seguridad	
Fecha y hora (informe)	**Prioridad (urgencia)**
Fecha y hora (incidente)	**Unidad Organizacional**
Detalles del informador	**Sistema afectado**
Título	**Punto de Contacto**
Detalle Descriptivo	**Estado de Escalado**
Daño estimado (si procede)	**Solución**

Tabla 13 .- Registro de incidente de seguridad.
(Fuente: propia)

6.3.1. Procedimiento de Recogida de Incidentes

Un incidente se puede recoger por tres vías:

- A través de la vía acordada en el ANS (llamada telefónica, correo electrónico, etc…) el usuario comunica al CAU la existencia de un incidente, problema o necesidad de ayuda.

- Alguno de los controles de seguridad (desplegados por el sistema TIC) envían una alerta al CAU.

- El administrador se pone en contacto con el CAU para notificar cualquier incidente detectado por cualquiera de los medios a su alcance (como por ejemplo los controles de seguridad anteriormente referidos).

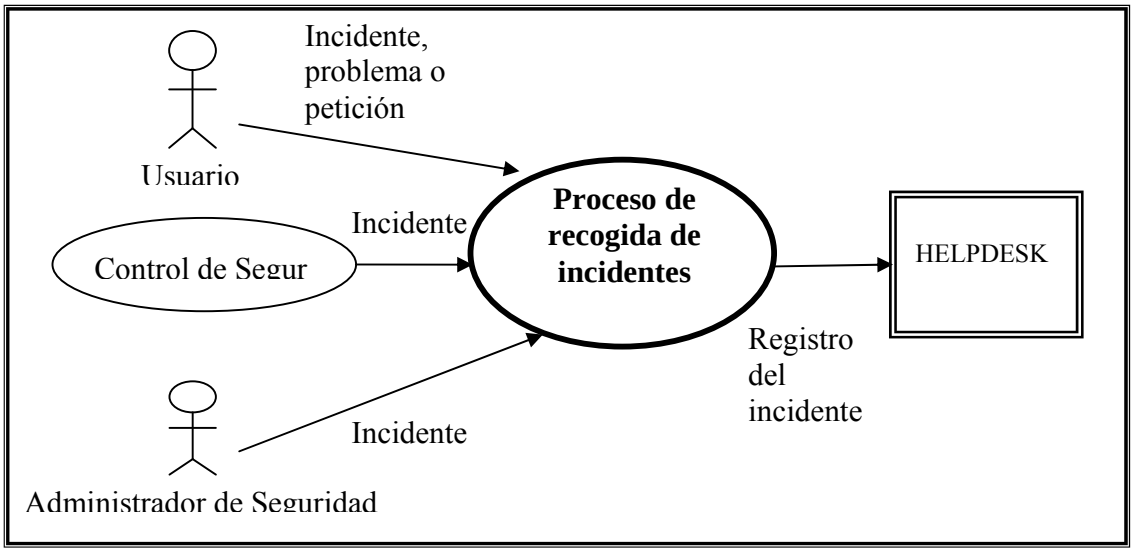


Figura 43.- **Caso de Uso del proceso de recogida de llamadas por el CAU.**
(Fuente: propia)

6.3.2. Proceso de Gestión de Incidentes de Seguridad.

El operador una vez recogida la notificación (por cualquiera de las vías referidas en el apartado anterior) y en base a una serie de procedimientos establecidos, determinará si el incidente o problema es de seguridad, en cuyo caso se registrará en el repositorio especial, dedicado al tratamiento de incidentes de seguridad, siempre según el procedimiento establecido.

Es importante que aquellas personas que recojan estas notificaciones o peticiones tengan muy claro los procedimientos de actuación y clasificación de éstas, con el fin de iniciar correctamente el tratamiento de cada tipo.

Se puede decir que, una buena Gestión del Incidente depende de que las definiciones de los distintos criterios de clasificación de las llamadas de servicio sean claras y concisas, de forma que los operadores puedan tratarlas sin ningún género de duda.

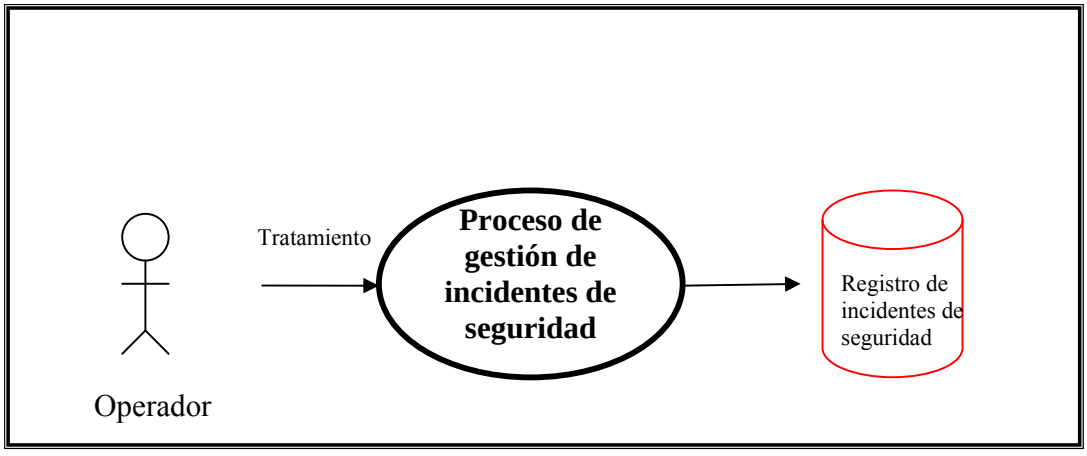


Figura 44.- **Caso de Uso del proceso de Gestión de Incidentes de Seguridad en MISITILEON.**
(Fuente: propia)

6.3.3. Gestión de los Administradores de Seguridad.

Cuando el CAU escala un incidente (porque no ha podido resolverlo) entra en juego el Administrador de Seguridad, como otro eslabón en la Gestión de la Seguridad.

El administrador de seguridad, podrá intervenir en los procesos de Gestión del Problema y Gestión del Cambio como personal experto en seguridad, teniéndose en cuenta su opinión para toda aquella toma de decisiones que afecten al sistema de seguridad de la organización.

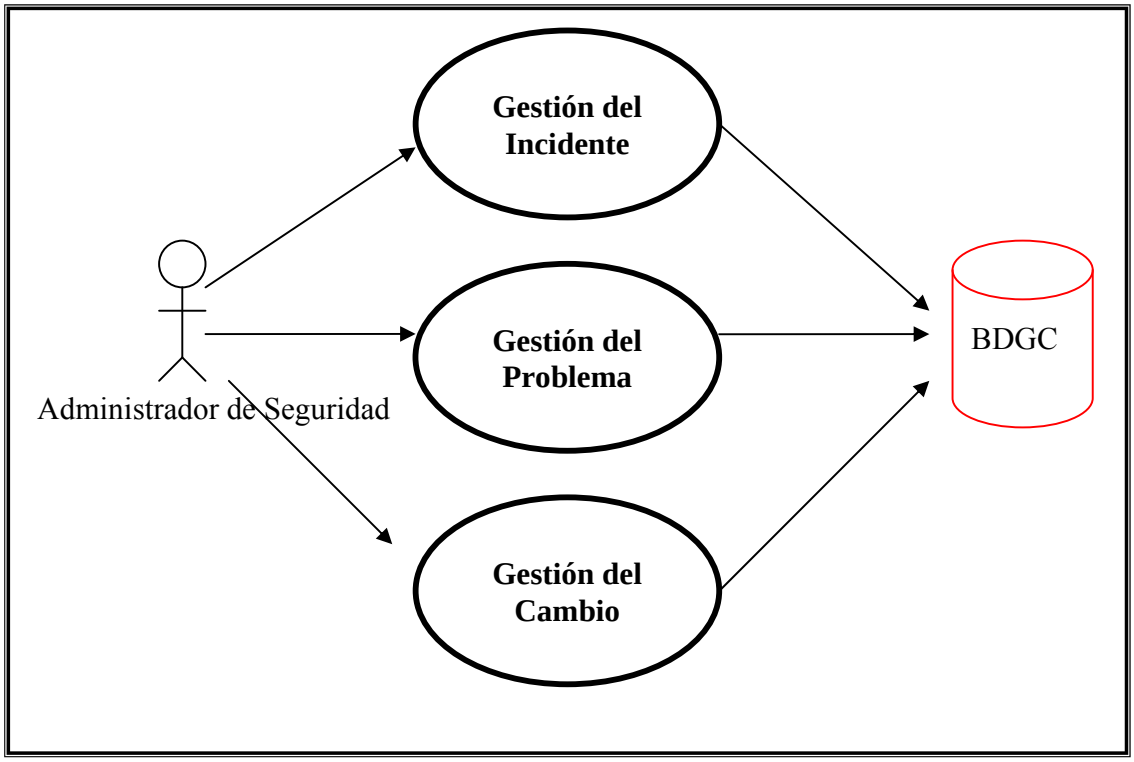


Figura 45.- **Caso de Uso del proceso de gestión de administradores de seguridad.**
(Fuente: propia)

6.4. Gestión de Problemas ocasionados por incidentes de seguridad. Reiteración de incidentes.

El proceso de Gestión del Problema pretende descubrir la conexión entre incidentes, de forma que las causas de dichos incidentes sean rastreadas y relacionadas, y puedan adoptarse, si procede, las medidas que los eviten.

El proceso de Gestión del Problema exige un exacto y completo registro de incidentes [OGCSOP06].

La gestión de problemas ocasionados por incidentes de seguridad sigue el mismo patrón. La reiteración de incidentes de seguridad relacionados, deriva en un problema de seguridad, que normalmente es escalado por *HelpDesk* hacia expertos en seguridad y que puede ocasionar una solicitud de cambio.

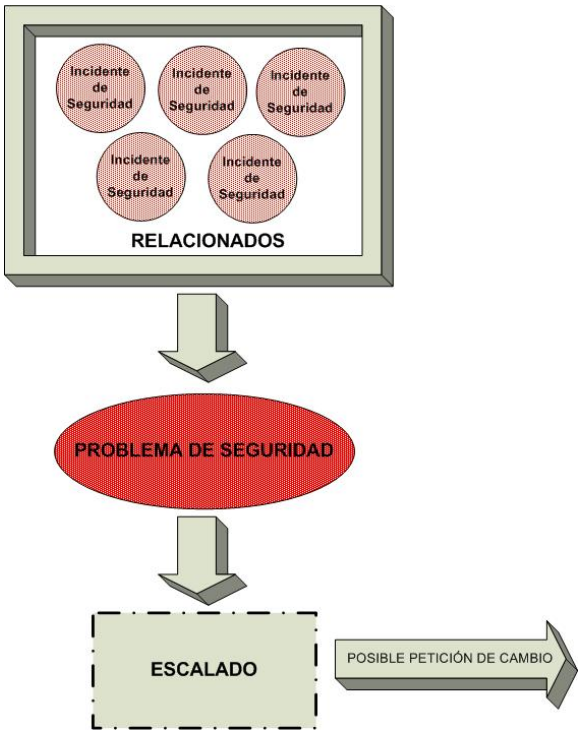


Figura 46.- **Proceso de gestión de problemas de seguridad en MISITILEON.**
(Fuente: propia)

En seguridad la reiteración de incidentes suele ser síntoma claro de un ataque o intento de ataque informático a la organización.

Este ataque puede ser debido (o su resultado puede ser agravado) por una vulnerabilidad en alguno de los sistemas TI de la organización, lo cual deriva en un problema de seguridad para dicha organización.

Ejemplos:

- Si el sistema antivirus en una estación de trabajo detecta un virus, esto es un incidente de seguridad.

- Si el virus es detectado en un número suficiente de estaciones de trabajo, el incidente se convierte en un problema de seguridad, que además implica una acción inmediata.

- Si el virus explota una vulnerabilidad existente en el sistema, el problema de seguridad puede ocasionar un mayor impacto en la seguridad de la organización.

La importancia y clasificación del problema están predeterminadas por aquellas que tenga la información contenida en el sistema afectado, y atendiendo a ellas debe ser tratado el problema.

Así, no será tratado con la misma celeridad, un problema de seguridad en un sistema que contiene información vital para el funcionamiento de la organización, que un problema donde la información no tenga relevancia.

Como se comentó anteriormente, uno de los fines de la Gestión de Problemas de Seguridad en MISITILEON, además de reestablecer el servicio al usuario, es descubrir agujeros de seguridad, vulnerabilidades en la organización, de forma que un problema de seguridad deberá estudiar aspectos enfocados a detectar dichas vulnerabilidades.

Ejemplos:

- ¿Cómo entró el virus en el sistema? ¿Cuál es el foco? -> *Posible vulnerabilidad.*
- ¿Cómo se propagó el virus por la organización? -> *Posible vulnerabilidad.*

- ¿En qué puede afectar el virus a la organización? -> *Posible vulnerabilidad.*

Otro tipo de problemas de seguridad, que conviene referenciar, son aquellos que son detectados o asociados a incidentes que en principio no son de seguridad.

Ejemplos:

- La caída de un sistema (un servidor de aplicaciones) es un incidente, pero no tiene por qué ser catalogado como incidente de seguridad.
- La caída continua del mismo sistema, puede ser un problema de seguridad ocasionado por un ataque de denegación de servicio contra dicho sistema, aprovechando una vulnerabilidad del mismo.

Así, el problema de seguridad deberá estudiar aspectos como:

- ¿Por qué se está produciendo la caída del sistema?
    - Acción de un virus residente en el sistema -> *Posible vulnerabilidad.*
    - Acción de un atacante que penetró en el sistema -> *Posible vulnerabilidad.*
    - Reacción del sistema ante cualquiera de los casos anteriores -> *Posible vulnerabilidad.*
- ¿Qué otras posibles consecuencias puede tener el ataque? -> *Otras posibles vulnerabilidades.*

6.5. Relación entre Gestión de la Configuración, Gestión del Cambio y Gestión de la Seguridad.

La Gestión de la Configuración y la Gestión del Cambio son procesos muy relacionados (incluso se podría decir, gestión del cambio de esa configuración), que lógicamente también guardan una estrecha relación con la Gestión de la Seguridad.

La Gestión de la Configuración es el proceso responsable de mantener la información de los componentes de la infraestructura TI, de su estado y de la relación con otros componentes.

La Gestión del Cambio es el proceso responsable del control del ciclo de vida de los cambios de los componentes TI.

Todo cambio deber ser registrado por la Gestión de la Configuración [OGCSOP06].

En este apartado se va a desgranar la relación existente entre estos dos procesos y la Gestión del Problema, y cómo esa relación y el desarrollo de cada uno de los procesos, se ven afectados por el proceso de seguridad.

Se verá la importancia del nivel de clasificación de los sistemas en todo su ciclo de vida, y cómo ese nivel de seguridad debe mantenerse según lo estipulado en el ANS.

La salida o resolución del proceso de Gestión de Problemas de Seguridad puede ocasionar una solicitud de cambio[94], el cuál una vez ejecutado deberá ser registrado por la Gestión de la Configuración.

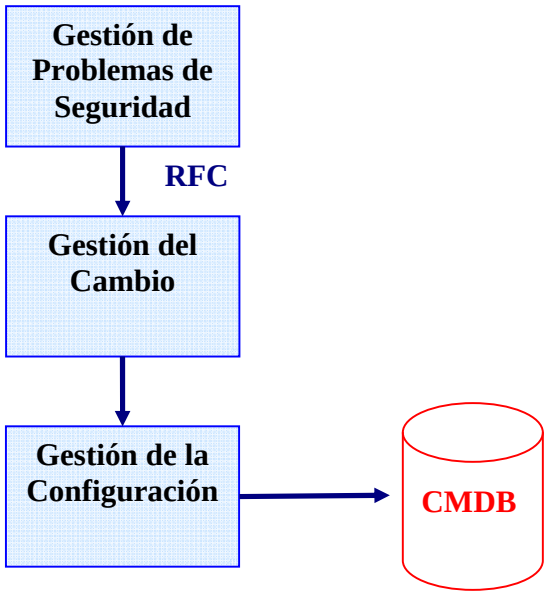


Figura 47.- **Proceso de solicitud de cambio.**
(Fuente: OGC.- Soporte)

Estos dos procesos van a trabajar fundamentalmente con dos conceptos:

- **EC**: Unidad más pequeña de trabajo.
- **BDGC**: Es la vista total de la infraestructura TI, ya que contiene todos los ECs de la organización (software, hardware, documentación, procedimientos,...).

[94] En inglés "*Request for Change*" (RFC).

La CMDB proporciona un punto de integración de todos los procesos que forman la gestión de los servicios TI, integración que es esencial para una implementación ITIL satisfactoria [VPCMDB06].

Según MISITILEON se considera a la Gestión de la Seguridad como un proceso más, por tanto se deduce que la BDGC va a ser utilizada por dicho proceso para su relación con otros procesos propios de ITIL.

Cada EC, dentro de la BDGC, dispondrá de un identificador que hará referencia de forma unívoca a una serie de atributos. Dentro de esos atributos contenidos en el EC, se encuentra uno muy importante y que indicará el nivel de clasificación de seguridad correspondiente a ese EC. De esta forma se enlazará el propio EC con una serie de medidas o procedimientos de seguridad, asociados a dicho nivel de clasificación.

La asignación del nivel de seguridad de cada CI debe ser determinada por el cliente, ya que es la única entidad capaz de determinar la importante de la información o del sistema que lo contiene. Esta clasificación se deriva, por tanto, de los requerimientos de seguridad acordados en el SLA [OGCSM99].

El nivel de clasificación de seguridad de cada EC se determinará en función de las tres variables que identifican los paradigmas de la seguridad:

- Confidencialidad
- Integridad
- Disponibilidad

A cada una de estas variables se le asignará un valor en función de la clasificación de la información adoptada por la organización. La Administración en España generalmente clasifica como:

- Secreto
- Confidencial
- Reservado
- Sin clasificar

A nivel OTAN[95], la clasificación similar, sería:

- *Cosmic Top Secret*
- *NATO Secret*
- *NATO Confidential*
- *NATO Restricted*
- *NATO Unclassified*

La clasificación del EC enlaza a éste con un juego de medidas de seguridad, a veces recopiladas en procedimientos, que forman una serie de actividades que deben ser debidamente documentadas.

Como se ha comentado anteriormente, un problema de seguridad, ocasionado por una vulnerabilidad en el sistema, suele ir precedido de un cambio en los ECs afectados por dicha vulnerabilidad, con el fin de reducirla o eliminarla, si es posible. Por ejemplo:

[95] Organización del Tratado Atlántico Norte.

Vulnerabilidad: Un sistema de actualización de parches de sistema operativo, necesita conectarse a Internet y recibe constantes ataques desde el exterior.

↓

Cambio: Separar el sistema de Internet por medio de una pasarela.

Por otra parte, cuando cualquier sistema es sometido a un cambio (no tiene por qué ser por un problema de seguridad) será necesario que dicho sistema mantenga el nivel de seguridad que tenía previamente asignado.

Será misión de la Gestión del Cambio asegurar que todos los ECs afectados por el cambio mantienen el nivel de seguridad acordado en los ANSs.

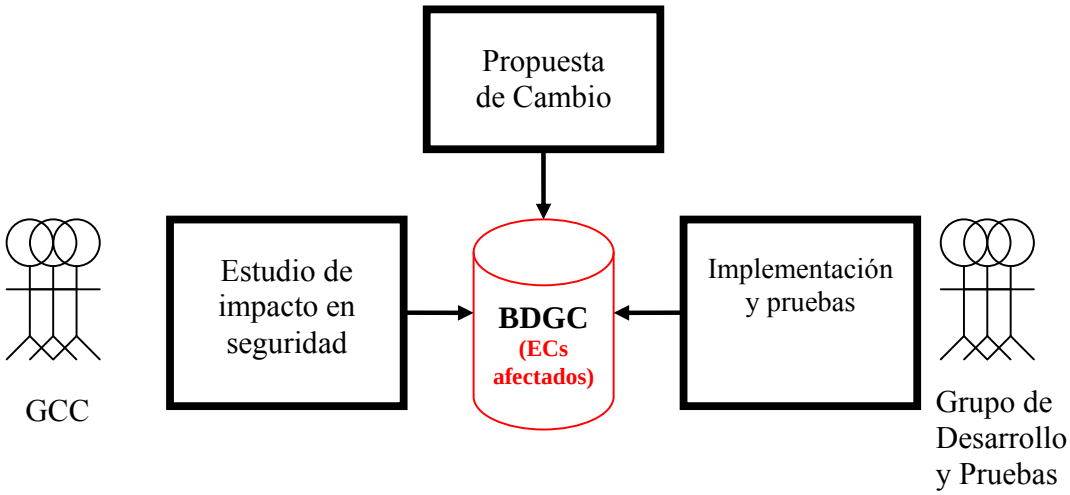


Figura 48.- **Gestión de impacto de seguridad de los cambios.**
(Fuente: propia)

No es necesario que el administrador de seguridad esté implicado en cada cambio, la composición del grupo GGC[96] (Grupo de Gestión del Cambio) será decisión del gestor del cambio, dentro de una política de normalización de seguridad en el ciclo de vida de los cambios.

6.5.1. Proceso de Gestión del Cambio.

Una vez definidos los requerimientos o nivel de seguridad que pretende la organización, será necesario implementar una serie de sistemas o modificar otros, de forma que sea factible alcanzar dicho nivel de seguridad, esta función se realiza en el proceso de gestión de cambio.

Los gestores de seguridad formarán, de forma habitual, parte de los equipos dedicados a los cambios que afecten al sistema de seguridad de la organización, siendo por tanto parte activa del proceso de Gestión del Cambio de MISITILEON.

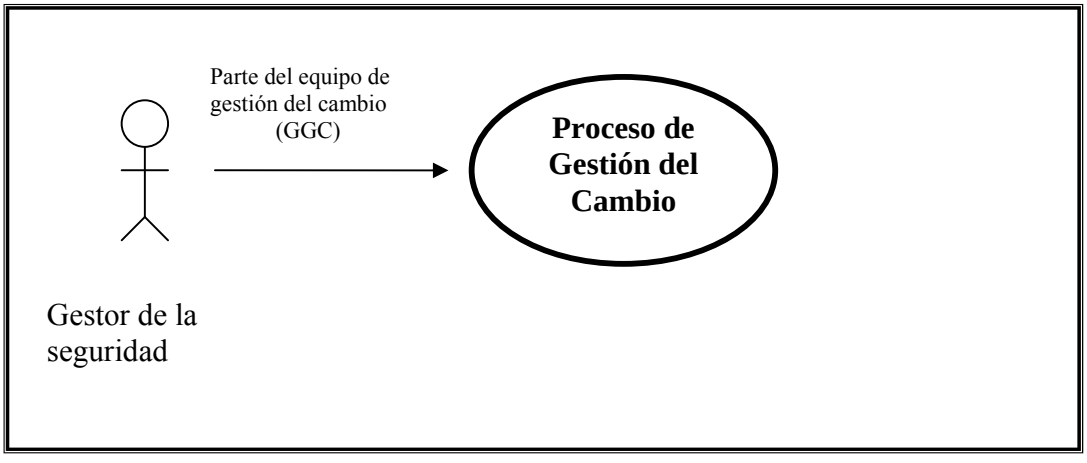


Figura 49.- **Caso de Uso del proceso de Gestión del Cambio en MISITILEON.**
(Fuente: propia)

[96] Análogo al CAB (*Change Advisory Board*) de ITIL.

CAPÍTULO V. CASO PRÁCTICO: SERVICIO DE SEGURIDAD MISITILEON. SISTEMA ANTIVIRUS.

A continuación se detallan los procesos, actividades y tareas creados para proporcionar a una organización un servicio de seguridad antivirus:

PROCESOS RELACIONADOS CON EL NIVEL DE SERVICIO (A)

- **Gestión del nivel del servicio Antivirus. (A.1)**
  - Definición del nivel del servicio Antivirus. (A.1.1)
    - Reuniones (Cliente-Proveedor para definir ANSs). (A.1.1.1)
    - Formulario ANS del Servicio Antivirus. (A.1.1.2)
- **Medidas/Controles de Seguridad. (A.2)**
  - Definición de Controles de Seguridad. (A.2.1)
    - Antivirus nivel protocolo de red. (A.2.1.1)
    - Antivirus nivel servidor. (A.2.1.2)
    - Antivirus nivel cliente. (A.2.1.3)
  - Configuración de los controles de seguridad. (A.2.2)
    - Nivel de protección aplicado. (A.2.2.1)
    - Archivos de registros de detecciones. (A.2.2.2)
    - Sistemas de Alarmas. (A.2.2.3)
  - Mantenimiento de los controles de seguridad. (A.2.3)

        - Procedimiento de actualización del antivirus. (A.2.3.1)
        - Procedimiento de modificación de la configuración. (A.2.3.2)

- **Modificación del nivel de seguridad. (A.3)**
    - Incremento o decremento del nivel del antivirus. (A.3.1)
- **Procedimientos de contingencia y recuperación. (A.4)**
    - Procedimientos de actuación generales ante un virus. (A.4.1)

PROCESOS QUE OFRECEN EL SERVICIO (B)

- **Proceso de Recogida de incidentes de seguridad. (B.1)**
    - Procedimiento de comunicación de posible virus, a nivel usuario. (B.1.1)
    - Procedimiento de discriminación de llamadas de servicio, a nivel operador. (B.1.2)
    - Procedimiento de comunicación de posible virus, a nivel Administrador de Seguridad. (B.1.3)
    - Procedimiento de comunicación de posible virus, a nivel Control de seguridad. (B.1.4)
- **Proceso de gestión de incidentes de seguridad ocasionados por virus. (B.2)**
    - Procedimiento de actuación, a nivel operador, ante un posible virus. (B.2.1)
    - Procedimiento de actuación, a nivel Administrador de seguridad, ante un posible virus. (B.2.2)
- **Proceso de gestión de problemas de seguridad ocasionados por virus. (B.3)**

- Procedimiento de actuación, a nivel Administrador de Seguridad, ante un posible problema ocasionado por un virus. (B.3.1)

- **Proceso de Gestión de la Configuración y Gestión del Cambio ocasionados por virus. (B.4)**
  - Procedimiento de colaboración del administrador de seguridad ante un cambio. Pertenencia a GGC. (B.4.1).

En el proceso anteriormente descrito, los subprocesos y procedimientos se identifican de forma numeral para una mejor y más rápida referencia.

Una representación gráfica de todo este proceso, que a continuación se irá desarrollando, sería:

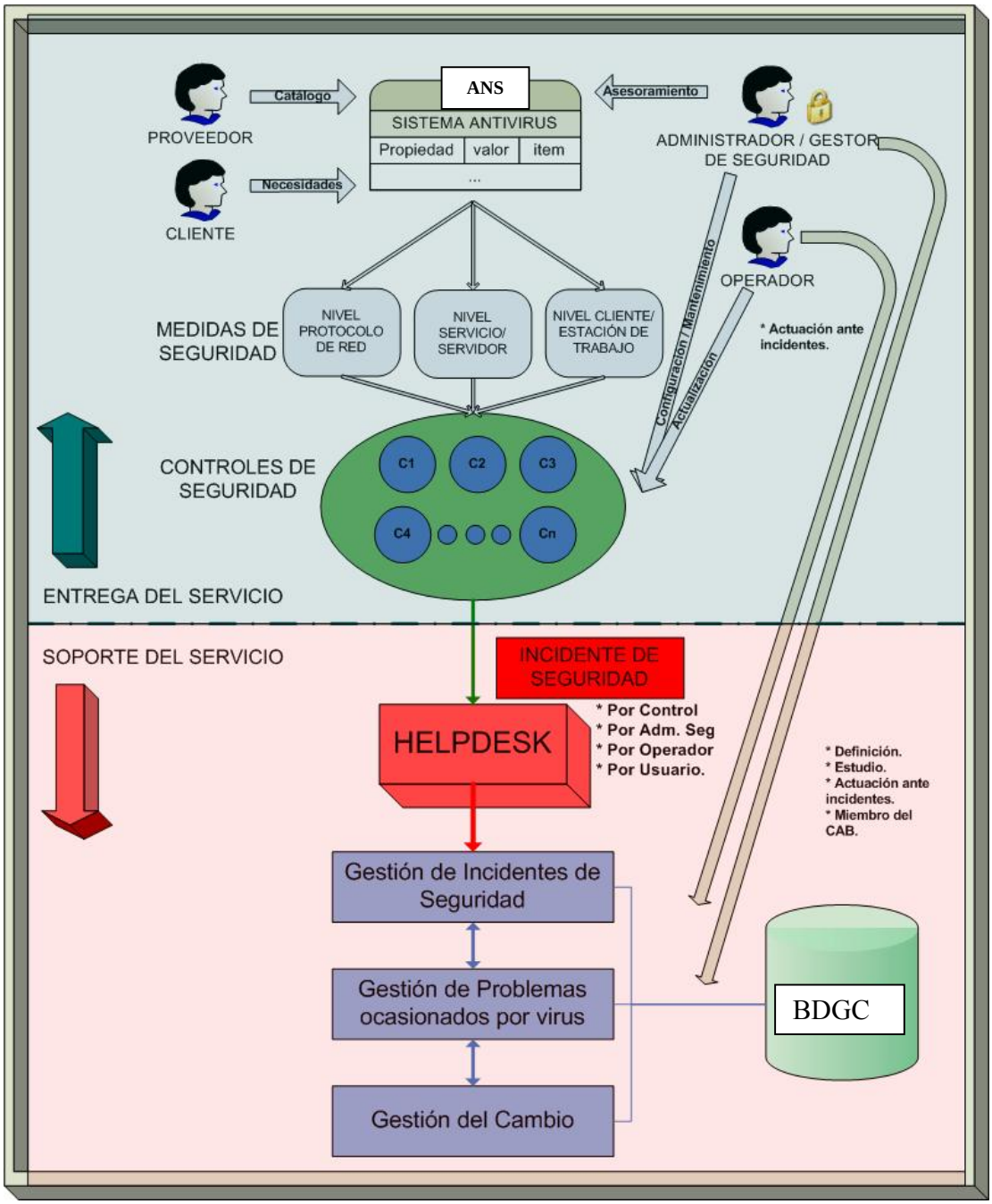


Figura 50.- **Proceso de gestión del servicio de seguridad en MISITILEON.**
(Fuente: propia)

Es muy importante que estos procesos y los procedimientos que se derivan de ellos, se definan y realicen correctamente, ya que van a marcar el éxito o el fracaso del sistema antivirus en la organización, sobre todo cuando el caso de fracaso puede derivar en graves

desastres para la organización, como puede ser la pérdida de información fundamental o la denegación de un servicio vital para el funcionamiento de la organización.

Se verá que los agentes o actores que intervienen de una u otra forma en estos procesos son: el propio cliente, el proveedor del servicio y el gestor/administrador de la seguridad:

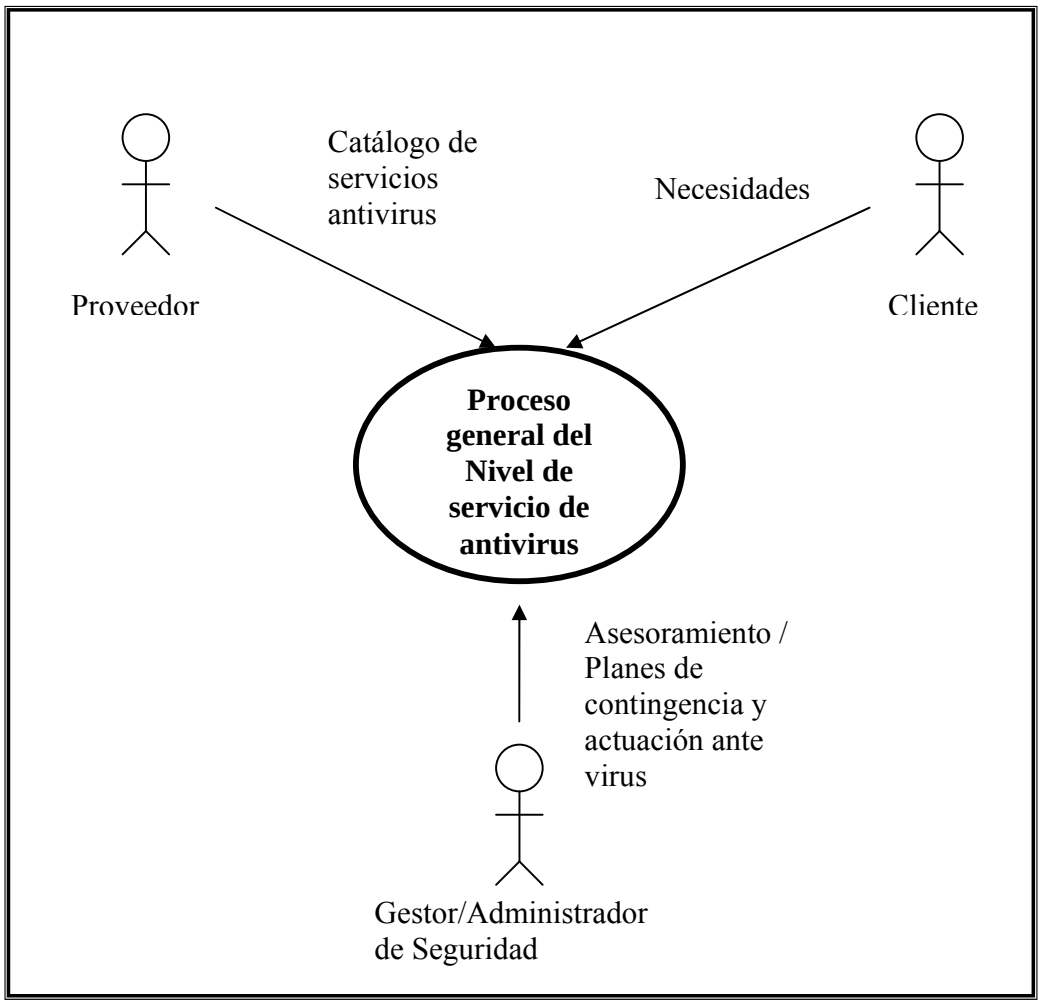


Figura 51.- **Caso de Uso: proceso general del Nivel de Servicio antivirus.**
(Fuente: propia)

Las funciones del cliente y proveedor están más relacionadas con la definición del sistema y el nivel de seguridad a aportar, es decir, estarán en las fases iniciales de la implantación del sistema, o en caso de que haya que modificar dicho nivel de seguridad.

El Administrador de Seguridad, formará parte activa del sistema, realizando funciones de mantenimiento de la disponibilidad del sistema, ante posibles infecciones de virus.

1. Procesos y Procedimientos relacionados con el Nivel de Servicio (A)

Este primer grupo de procesos son los encargados de definir el nivel del servicio, así como de asegurarse de que dicho nivel se mantiene en el tiempo.

El constante crecimiento de la base de datos que contiene los posibles virus[97], genera unos procesos continuos de actualización del sistema, que en esta fase habrá que definir en forma de procedimientos.

1.1. Gestión del nivel del servicio Antivirus (A.1)

(A.1.1) Definición del nivel del servicio Antivirus

[97] Denominada patrón de virus o catálogo de virus.

El primer paso consiste en la definición del nivel del servicio antivirus que se quiere aportar a la organización. Básicamente, consiste en una serie de reuniones entre el proveedor del servicio y el cliente (en representación de la organización) donde se van a definir, con asesoramiento del Gestor de Seguridad, qué posibilidades se van a desplegar dentro del catálogo de servicios antivirus soportados por el proveedor.

De estas reuniones, cliente-proveedor, surgirá el ANS, que deberá ser respetado por ambas partes.

Así, la definición del nivel del servicio antivirus se compone de:

- Programación de reuniones (Cliente-Proveedor) para definir y mantener las ANSs.
- Establecimiento de formularios ANSs para servicio antivirus.

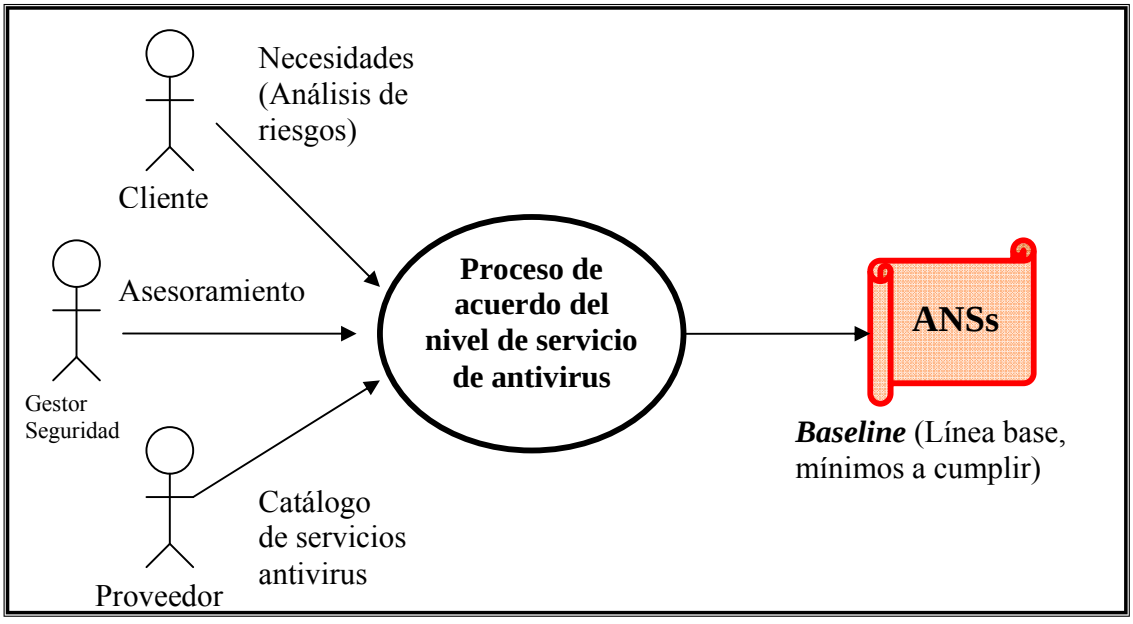


Figura 52.- **Caso de Uso: proceso de acuerdo del nivel de servicio antivirus.**
(Fuente: propia)

(A.1.1.1) Reuniones (Cliente-Proveedor) para definir y mantener los ANSs.

Profundizando más en el proceso de gestión de los niveles del servicio antivirus, y considerando éste como un servicio más a gestionar por MISITILEON, éste se compondrá de una serie de actividades que habrá que realizar de forma ordenada.

Algunas de estas actividades implican una serie de reuniones entre proveedores y clientes. A continuación se detallan las principales actividades de la Gestión de Niveles de Servicio y las reuniones pertinentes.

- **Planificación**:
    - Análisis e identificación de las necesidades del cliente.
    - Elaboración de un catálogo de servicios de seguridad.
    - Desarrollo del ANSs de seguridad particular.
    - Asignación de recursos de seguridad.
    - Herramientas para la monitorización de la calidad del servicio de seguridad.
    - Elaboración de los siguientes documentos:
        - Requisitos de Nivel de servicio (RNS[98]).
        - Hojas de Especificación del Servicio.
        - Plan de Calidad del Servicio (PCS[99]).
        - Propuesta de ANS para el cliente.

[98] Análogo al SLR *(Service Level Requirements)*.
[99] Análogo al SQP *(Service Quality Plan)*.

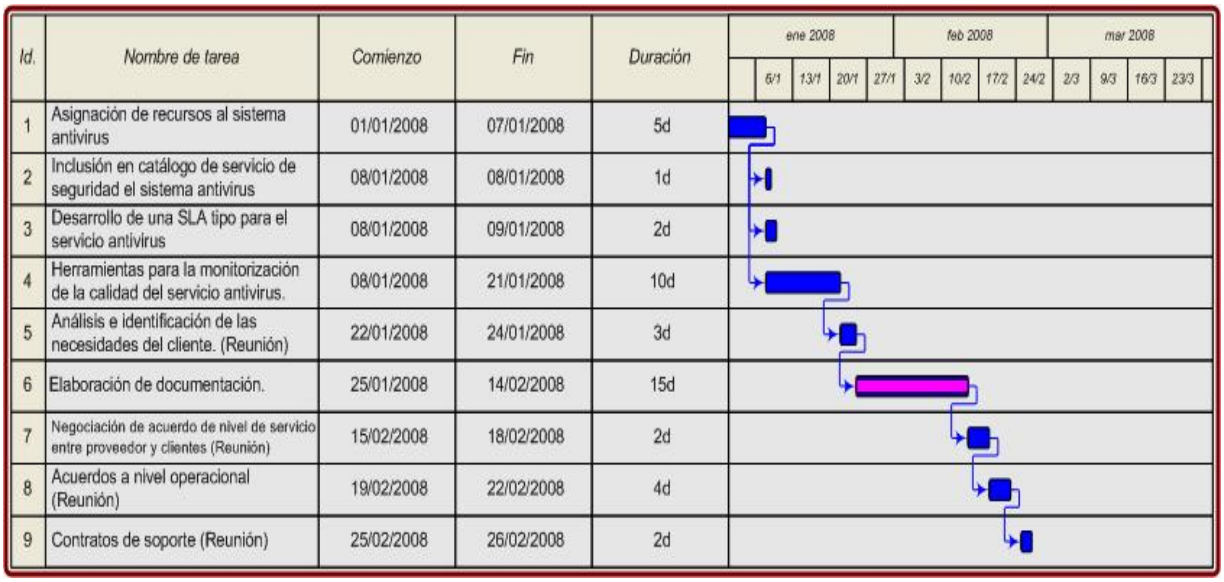
- **Implementación de los Acuerdos de Nivel del Servicio:**
    - Negociación de aprobación del ANS propuesto.
    - Acuerdos de Nivel de Servicio.
    - Firma de Contratos de Soporte.

- **Supervisión y revisión de los ANSs:**
    - Elaboración de informes de rendimiento.
    - Control de los proveedores externos.
    - Elaboración de Programas de Mejora del Servicio (PMS[100]).

Será necesario establecer una programación de las reuniones a realizar, con objeto de establecer los acuerdos y contratos necesarios para una correcta gestión del nivel de servicio.

Una herramienta de programación de actividades o tareas muy útil son los diagramas de Gantt. Pero también se pueden usar otras técnicas como el PSP[101], etc. Un ejemplo de Gestión de los niveles del servicio antivirus, utilizando Gantt para representarlo, podría ser:

[100] Análogo al SIP *(Service Improvement Programs).*
[101] Proceso Software Personal, en inglés *Personal Software Process*.



Id.	Nombre de tarea	Comienzo	Fin	Duración
1	Asignación de recursos al sistema antivirus	01/01/2008	07/01/2008	5d
2	Inclusión en catálogo de servicio de seguridad el sistema antivirus	08/01/2008	08/01/2008	1d
3	Desarrollo de una SLA tipo para el servicio antivirus	08/01/2008	09/01/2008	2d
4	Herramientas para la monitorización de la calidad del servicio antivirus.	08/01/2008	21/01/2008	10d
5	Análisis e identificación de las necesidades del cliente. (Reunión)	22/01/2008	24/01/2008	3d
6	Elaboración de documentación.	25/01/2008	14/02/2008	15d
7	Negociación de acuerdo de nivel de servicio entre proveedor y clientes (Reunión)	15/02/2008	18/02/2008	2d
8	Acuerdos a nivel operacional (Reunión)	19/02/2008	22/02/2008	4d
9	Contratos de soporte (Reunión)	25/02/2008	26/02/2008	2d

Figura 53.- **Diagrama Gantt: Gestión de los niveles del servicio antivirus.**
(Fuente: propia)

Es importante tener en cuenta que para la creación del diagrama anterior se han estimado los tiempos de las tareas para una organización de una entidad media. Lógicamente, estos tiempos cambiarán cuándo se lleve a un caso real, no siendo importantes, sino más bien una referencia para mostrar un posible ejemplo de representación de las tareas necesarias para gestionar el nivel de calidad del servicio antivirus.

(A.1.1.2) Formulario ANS del Servicio Antivirus.

Este formulario contiene toda la información relevante extraída de las diversas reuniones mantenidas con el cliente. Un formulario ANS tipo, diseñado por la doctorando para MISITILEON, donde queda reflejado el nivel de calidad a alcanzar por el servicio antivirus podría ser:

ANS DE SEGURIDAD - Servicio Antivirus		
Identificador	**10001**	
Título	**Sistema de Seguridad Antivirus.**	
GENERAL		
Cliente	**Es el cliente con el cual se establece el contrato del Servicio.**	
Responsable	**Responsable por parte de la organización cliente.**	
Inicio de Acuerdo	**dd/mm/aa**	
Fin de Acuerdo	**dd/mm/aa**	
Impacto	**Crítico**	
Urgencia	**3**	
Tiempo de Servicio	**7x24**	
Tiempo de Respuesta	**dd:hh:mm**	
EQUIPO DE TRABAJO		
Responsable del ANS	**Responsable del cumplimiento del servicio por parte de la empresa proveedora del servicio.**	
Rol del Responsable	**Administrador de Seguridad.**	
Integrantes	**Todas las personas posibles a integrar los equipos de trabajo.**	
Admin1	**Responsable de Seguridad Antivirus.**	
……	**…**	
Admin4	**Responsable de Sistemas.**	
Niveles de Resolución	**Distintos niveles de resolución de incidentes por virus, así como los integrantes que forman los equipos asignados.**	
Nivel 1	Admin1/Admin2	**Admin1**
…….	……	**…….**
Nivel 4	Admin1/Admin2/Admin3	**Admin1**

PRIORIDADES DEL INCIDENTE				
Distintas prioridades de incidentes por impacto y urgencia, así como tiempos y niveles de resolución asignados (por defecto).				
Prioridad 1	Bajo	1	1 día	**Nivel 1**
……	……	……..	……	**……**
Prioridad 4	Critico	3	1 hora	**Nivel 4**
ESCALAMIENTOS				
Funcional	**Posibles escalamientos, de resolución, por porcentaje**			
Porcentaje 10%	Escalamiento		**Nivel 2**	
……	……		**……**	
Porcentaje 70%	Escalamiento y Notificación		**Nivel 4**	
De Notificación	**Posibles escalamientos, de notificación, por porcentaje.**			
Porcentaje 10 %	Admin1		**Admin2,**	
…….	……		**……**	
Porcentaje	Admin1, Admin2		**Admin3, Gestor1, Super2**	
ANEXOS				
Documentos anexos, referencias: descripción de medidas y controles de seguridad necesarios para cumplir con el acuerdo de nivel del servicio Antivirus.				

Tabla 14 .- ANS de Seguridad.- Servicio Antivirus.

Independientemente del formato del ANS, la información contenida debería ser la que se ofrece en la tabla 14, pero desde luego puede modificarse para adaptarse mejor en cada caso particular.

1.2. Medidas/Controles de Seguridad (A.2)

Tras un acuerdo Cliente-Proveedor (ANS), el siguiente paso consiste en definir los Requisitos del Servicio antivirus a implantar en la organización, lo que se traduce en el establecimiento de una serie de medidas de seguridad que concreten el grado de seguridad acordado.

A su vez, las medidas de seguridad se van a materializar con la creación de una serie de controles de seguridad. Estos controles de seguridad van a constituir la definición del SGSI a implantar en la organización, teniendo en cuenta la relación entre MISITILEON e ISO 27002 (que se ocupa del desarrollo, implantación y mantenimiento de un SGSI).

En la normativa ISO/IEC 27002:2005, se detalla una lista de objetivos de control y controles recomendables en un sistema de seguridad de la información. Esta lista contiene 39 objetivos de control y 133 controles de seguridad, agrupados en 11 dominios[102]. En esta lista de controles se encuentra el servicio antivirus, o control equivalente, definido en esta memoria:

- **Dominio**: 10.- Gestión de comunicaciones y operaciones.
    - **Objetivo**: 10.4.- Protección contra código malicioso y descargable.
        - **Control**: 10.4.1.- Controles contra código malicioso.

Los controles de seguridad, como parte de un proceso de gestión de un servicio MISITILEON (y en la línea de integración de ITIL y los SGSI) siguen una estructura marcada por la norma ISO 27001, el PDCA (*Plan-Do-Check-Act*)[103].

(A.2.1) Selección de Controles de Seguridad.

En un sistema antivirus los controles de seguridad van a estar formados por elementos software y/o hardware, organizados en forma de barrera para los posibles virus.

[102] Véase Anexo 4.
[103] Véase el apartado 5.2.2. del capítulo 2 de esta memoria.

El objetivo de estos controles es detectar, lo antes posible, dicho software malicioso y, dependiendo de la política instaurada, eliminarlos o tratarlos de alguna manera.

Un sistema antivirus se puede estructurar en distintos niveles o capas, de hecho es muy recomendable que se realice de esta forma, de forma que el virus tenga que atravesar todas estas capas para poder afectar a la organización; lógicamente, cuanto más le cueste llegar, más seguro será el sistema.

Las distintas capas o niveles de antivirus son las siguientes:

- Antivirus nivel protocolo de red.
- Antivirus nivel servicio/servidor.
- Antivirus nivel estación de trabajo.

Estas capas constituirán la definición del sistema antivirus, adaptado a la definición de los ANSs acordados entre proveedor y cliente, con el asesoramiento del experto en seguridad.

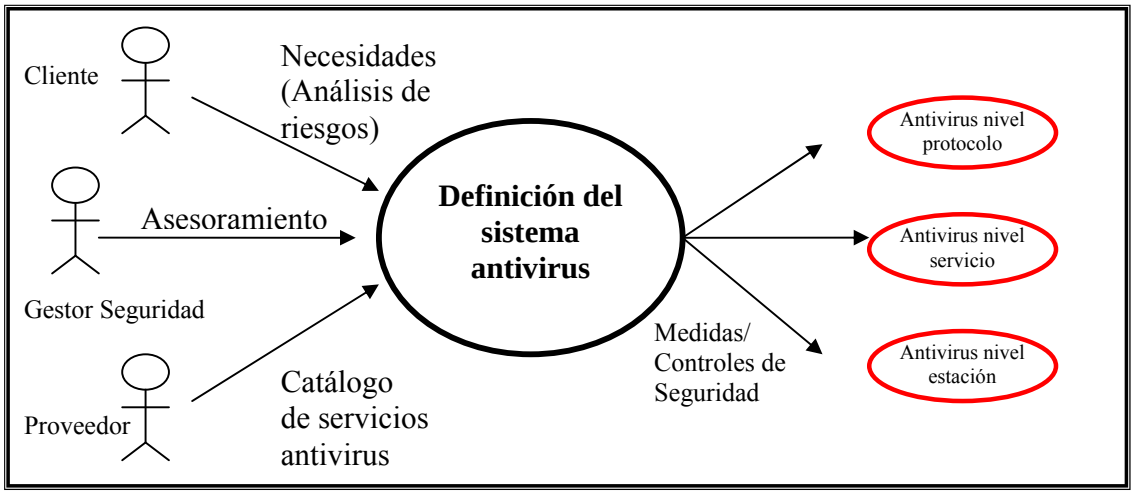


Figura 54.- **Caso de Uso: proceso de definición del sistema antivirus.**
(Fuente: propia)

(A.2.1.1) Antivirus nivel protocolo de red:

Los ataques que tienen lugar a través de la red representan el mayor número de incidencias ocasionadas por software malintencionado. Normalmente, los ataques de este tipo de software se inician aprovechando los puntos débiles en las defensas del perímetro de la red, a fin de tener acceso a los dispositivos dentro de la infraestructura de TI de la organización. Estos dispositivos podrían ser clientes, servidores, enrutadores o incluso equipos dedicados a la seguridad.

La primera capa o nivel de antivirus a implantar es la de protocolo de red, también denominado antivirus de perímetro de red.

Un antivirus en el perímetro de la red debe ser capaz de revisar la existencia de virus en los protocolos más utilizados por los distintos servicios aportados en la organización (HTTP[104], FTP[105], POP3[106], POP4[107], SMTP[108], IMAP[109], entre otros).

La mayor ventaja de utilizar este tipo de herramientas de seguridad antivirus es evitar el acceso de virus informáticos a una red, es decir, se detecta y se actúa frente al virus antes de que éste haya penetrado en los sistemas. Evidentemente, aporta un grado más de seguridad al sistema antivirus, aunque las distintas capas dentro de la red detecten el virus, el localizarlo y frenarlo antes de que penetre siempre es aconsejable.

Una solución óptima para implementar antivirus de perímetro de red son los denominados *appliance antivirus*, que son unos equipos de protección perimetral antivirus de alto rendimiento, compuestos de hardware y software, y que normalmente cubren las necesidades de protección ante muchos de los posibles tipos de software malicioso que puedan afectar a la organización, esto es, además de virus, *spyware*[110], *spam*[111], etc.

(A.2.1.2) Antivirus nivel servidor:

La defensa de los servidores de la organización tiene mucho en común con las defensas a nivel cliente: ambas intentan proteger el mismo entorno del equipo básico. Sin

[104] *Hypertext Transfer Protocol*: Protocolo utilizado para la navegación Web. [RefWeb-25]
[105] *File Transfer Protocol*: Protocolo de transferencia de ficheros. [RefWeb-26]
[106] *Post Office Protocol 3*: Protocolo utilizado para recibir correo. [RefWeb-27]
[107] *Post Office Protocol 4*: Protocolo avanzado para recibir correo. [RefWeb-28]
[108] *Simple Mail Transfer Protocol*: Protocolo utilizado para intercambio de mensajes de correo. [RefWeb-29]
[109] *Internet Message Access Protocol*: Protocolo de acceso a mensajes almacenados en servidores. [RefWeb-30]
[110] Software oculto que recopila información de los sistemas donde reside.
[111] Correo no deseado.

embargo, existen diferencias intrínsecas a la propia funcionalidad entre un antivirus de nivel cliente y un antivirus de nivel servidor. Los servidores tienen unas expectativas mayores de confiabilidad y rendimiento y por lo general son más importantes para el funcionamiento de la organización. Dichas diferencias están basadas fundamentalmente en los siguientes aspectos:

- **Utilización de la CPU durante la comprobación.** El uso de la CPU es un componente crítico en los servidores.
- **Confiabilidad de la aplicación.** Es necesario comprobar la confiabilidad del sistema antivirus.
- **Carga de la administración.** Es recomendable utilizar antivirus con capacidad para administrarse.
- **Interoperabilidad de la aplicación.** Con los servicios propios del servidor.

Las funciones dedicadas que muchos servidores realizan en la infraestructura de una organización a menudo conducirán a una solución de defensa especializada, es decir, existen productos antivirus dedicados a proteger una serie de servicios concretos.

Las soluciones antivirus que son específicas de aplicación, ofrecen mayor protección y rendimiento, puesto que han sido diseñadas para integrarse con un servicio concreto.

Las principales soluciones específicas soportan los siguientes servicios:

- ***Servidores Web.***

Los servidores Web de cualquier tipo, sitos en las organizaciones, son objetivo de ataques de seguridad continuos. Entre estos ataques, muchos provienen de software malintencionado, por lo que resulta imprescindible que la configuración de seguridad en los servidores Web se haga de forma que maximice las defensas contra dichos ataques.

- ***Servidores de mensajería.***

El servicio antivirus específico para mensajería, pretende impedir que cualquier software malintencionado se introduzca por medio del sistema de correo electrónico en los buzones de los usuarios de la organización.

En términos generales, las soluciones antivirus de comprobación de archivos no pueden evitar que un servidor de correo envíe software malintencionado a los clientes en forma de archivo adjunto. Hasta los servicios de correo electrónico más sencillos almacenan los mensajes en una base de datos de algún tipo[112]. Una solución antivirus de comprobación de archivos habitual no puede obtener acceso al contenido de dicha base de datos, por lo tanto será fundamental contar con una aplicación de antivirus integrada en el servicio de mensajería del servidor (o servidores) que se esté utilizando para realizar esta función en la organización.

[112] lo que se conoce algunas veces como el almacén de mensajes.

- ***Servidores de Bases de Datos.***

Otro de los servicios específicos de antivirus son los dedicados a proteger las bases de datos. Al considerar las defensas antivirus de un servidor de bases de datos hay cuatro elementos principales que se deben proteger:

- El propio servidor que contiene las bases de datos.
- Las distintas aplicaciones que proporcionan el servicio.
- El almacén de datos.
- Las comunicaciones entre los distintos elementos.

(A.2.1.3) Antivirus nivel cliente:

Es el antivirus que se instala en la estación de trabajo. Es la última barrera que tiene que traspasar el virus para afectar directamente a los equipos en la organización, y a la información contenida en ellos, por lo tanto, es tan importante como los anteriores en su configuración y mantenimiento.

Dicha configuración está basada en las aplicaciones o servicios que pueda ejecutar el cliente en su estación de trabajo y por tanto, se debe definir de forma que se proteja la propia estación de trabajo, de las posibles acciones a realizar por dichas aplicaciones y servicios.

Los principales servicios afectados en las estaciones de trabajo son:

- **Clientes de correo electrónico.** Si el software malintencionado consigue traspasar las defensas antivirus en la red y el servidor de correo electrónico, debe existir una configuración que ofrezca protección a nivel cliente de correo electrónico.

- **Aplicaciones de escritorio.** Los virus llamados "de macro" utilizan los archivos creados en el procesador de texto, hoja de cálculo u otra aplicación habilitada por macros para replicarse.

- **Aplicaciones de mensajería instantánea.** Aquellas aplicaciones que permiten transferencia de ficheros presentan, ante los posibles ataques por software malintencionado, una ruta directa a la red de la organización.

- **Exploradores Web.** Permiten descargar o ejecutar código de Internet, lo que supone un nuevo riesgo de contagio.

- **Aplicaciones P2P[113].** Estas aplicaciones favorecen el encontrar e intercambiar archivos con otros individuos. Diversos ataques de software malintencionado han utilizado dichas aplicaciones para replicar archivos en los equipos de otros usuarios.

Es interesante, por tanto, definir un sistema antivirus basado en una estructura de tres niveles, de forma que para que un virus que se sitúa en el exterior de una organización consiga infectar una estación de trabajo, deba atravesar tres capas:

[113] *Peer to peer* (red de pares).

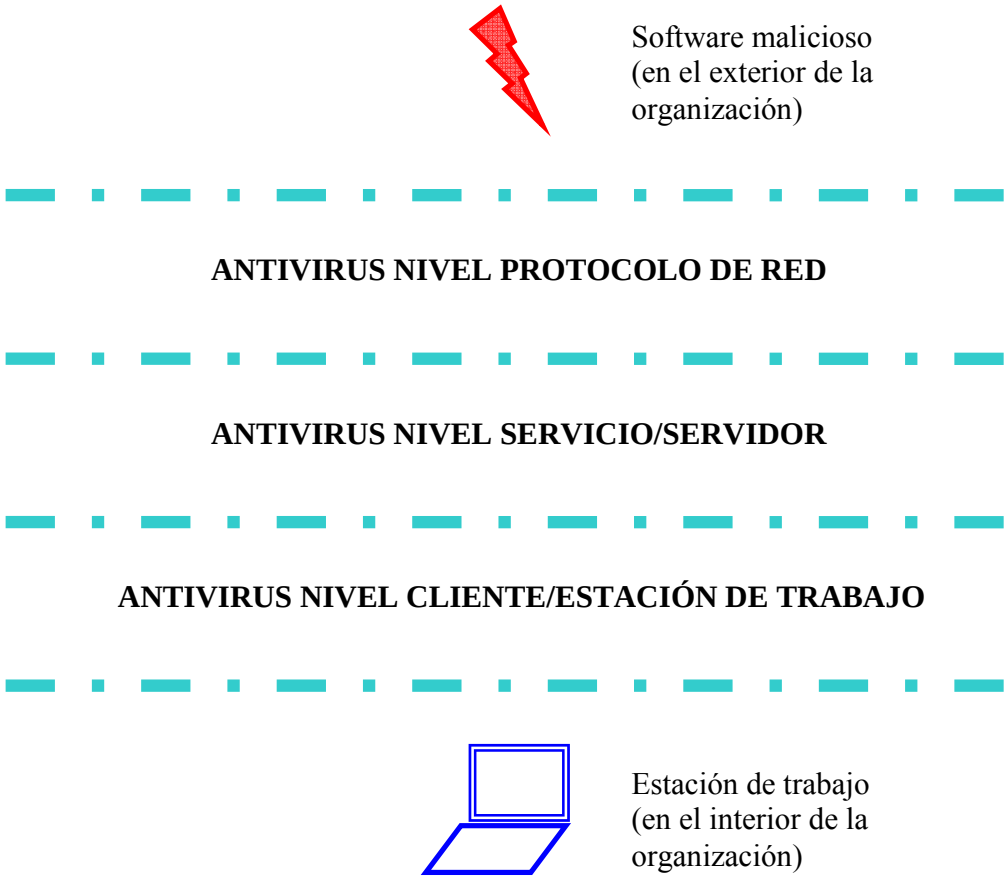


Figura 55.- **Diferentes niveles de la estructura de un sistema antivirus.**
(Fuente: propia)

Lógicamente, no siempre tiene por qué darse este escenario, y de hecho en esto reside la importancia de las tres capas, y la integración del sistema antivirus con otros controles de seguridad dentro de la política de la organización.

Así, por ejemplo, si un usuario introduce un disquete con software malicioso directamente en su estación de trabajo, las dos capas anteriores no actuarán, por lo tanto es fundamental que el antivirus a nivel cliente esté correctamente actualizado.

El gestor de seguridad, en función de lo acordado en el ANS y del caso concreto al que se enfrente, seleccionará los controles adecuados.

- **(A.2.1.4) Nivel de protección aplicado.**

Básicamente consiste en definir qué se quiere que el antivirus revise. Naturalmente, cuánto más alto sea el nivel de protección, más segura estará la organización, pero más afectará dicha protección al rendimiento de los sistemas.

El software antivirus es un software bastante costoso para el rendimiento de los sistemas, por lo tanto será necesario buscar un equilibrio entre seguridad-rendimiento que sea soportado por la organización y mantenga la calidad del servicio acordada en el ANS.

Es importante tener en cuenta que determinadas funcionalidades de los sistemas se ven muy afectadas por el software antivirus, por poner un ejemplo, la replicación del directorio activo de los controladores de Windows, aconseja la exclusión en el chequeo de una serie de directorios del propio controlador de dominio.

(A.2.2) Configuración de los controles de seguridad.

Una vez adoptada una estructura concreta para el sistema antivirus, y definidos los diferentes controles de seguridad que van a soportar dicha estructura, esto es, por ejemplo:

1º.-*Appliance Antivirus* que van a constituir la capa de perímetro de red.

2º.-Distintos servidores donde se aplicará software específico para servicios concretos.

3º.-Software de antivirus que se aplicará en las estaciones de trabajo.

Será necesario configurar cada uno de ellos, con el fin de implementar el nivel de protección, o el sistema de registro de detecciones y de alarmas, que se ha concretado en anteriores reuniones con el cliente, es decir, en los ANSs.

- **(A.2.2.1) Opciones de configuración.**

Seguidamente se presenta una tabla con algunas opciones de configuración para cada una de las capas, no están todas ya que pueden variar según el software antivirus elegido:

OPCIONES DE CONFIGURACIÓN DEL SISTEMA ANTIVIRUS	
CAPA O NIVEL	**OPCIONES**
Perímetro de red **Consiste, básicamente, en la elección de los protocolos que se van a chequear por el antivirus, así como los puertos que tienen asociados.**	**Protocolo — Puerto (por defecto)** • **HTTP — 80** • **FTP — 22** • **SMTP — 25** • **POP3 — 110…** **resto de protocolos que se quiere chequear y el Antivirus lo permita.**
Servicio/Servidor **Dependerá del servicio al que se especifica el software antivirus.** **El más extendido es para el servidor de mensajería.**	• **Almacenes protegidos.** • **Nivel de Filtrado.** • **Tipos de Filtros:** **SNMP** **VSAPI** • **Nivel de contenedores a escanear (p. e. 32)** • **Escanear rutas en correo.** • **Protección de correo no deseado[114].**

[114] En inglés "*AntiSpam*".

OPCIONES DE CONFIGURACIÓN DEL SISTEMA ANTIVIRUS	
Cliente/Puesto de Trabajo **Es el nivel que más posibilidades de configuración tiene. Y va a depender de las aplicaciones y servicios que corren en cada estación de trabajo.**	• **Analizar sectores de arranque.** • **Analizar disquetes al apagar.** • **Analizar archivos al escribir/leer en disco.** • **Analizar archivos en unidades de red.** • **Qué archivos analizar, todos, por extensión, exclusiones.** • **Activar análisis por heurística.** • **Analizar archivos comprimidos (p. e. ZIP).** • **Activar análisis en tiempo real al iniciar.** • **Definir un tiempo de análisis máximo.** • **Activar análisis de comandos Java.** • **Acciones a realizar al detectar un virus. Normalmente se define una acción alternativa.** • **Sitio de migración de ficheros infectados. (cuarentena)** • **Opciones para analizar correos electrónicos durante su recepción, como puede ser, analizar el cuerpo de los mensajes.**

Tabla 15 .- Opciones de configuración del sistema antivirus.

A continuación, se exponen algunos ejemplos, que muestran cómo se llevaría a la práctica la configuración de un software antivirus.

En las siguientes pantallas se define el analizador en tiempo real de un software antivirus instalado en una máquina cliente.

- En esta primera opción se eligen parámetros generales, como pueden ser:
  - ¿Qué analizar?
  - Si el análisis se activa al iniciar el sistema, o debería hacerse de forma manual.

- La carpeta de cuarentena, donde se depositarán los ficheros con virus detectados.
- Los tiempos máximos de análisis de los distintos tipos de archivos.

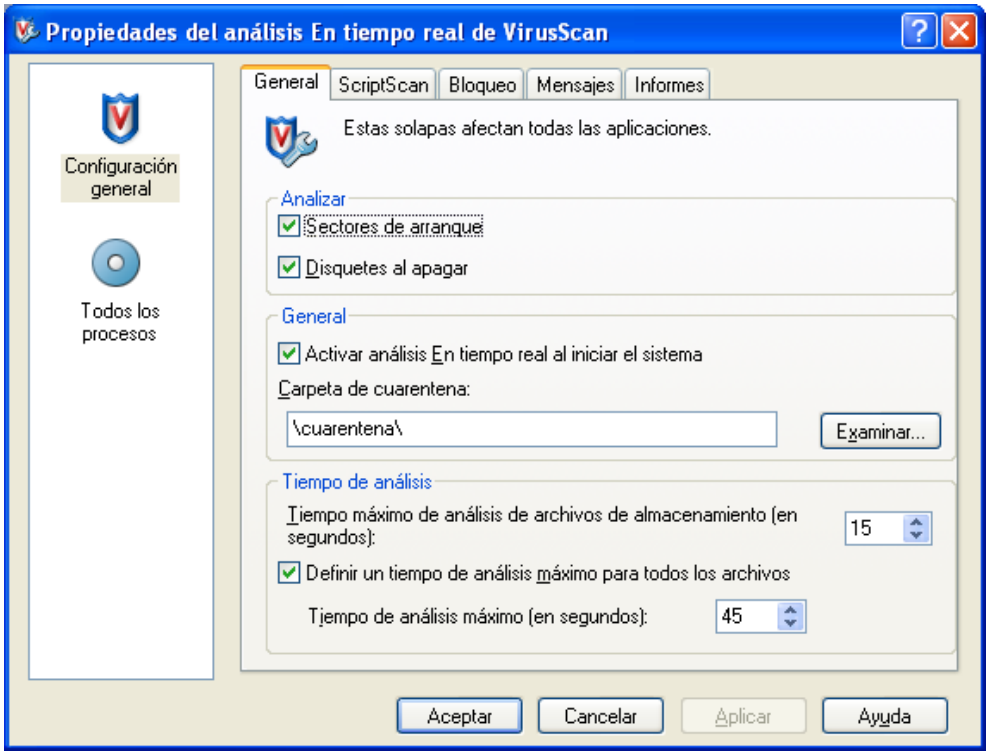


Figura 56.- **Propiedades Generales de análisis en tiempo real de VirusScan.**
(Fuente: VirusScan 8.0i de McAfee)

- En esta otra opción se eligen parámetros utilizados en la detección del software malicioso:
  - ¿Cuándo analizar los archivos?[115]
  - ¿Qué archivos analizar?
  - Exclusiones en el análisis[116].

[115] Si se marca la opción de unidades de red habrá que tener en cuenta que consume bastantes recursos.

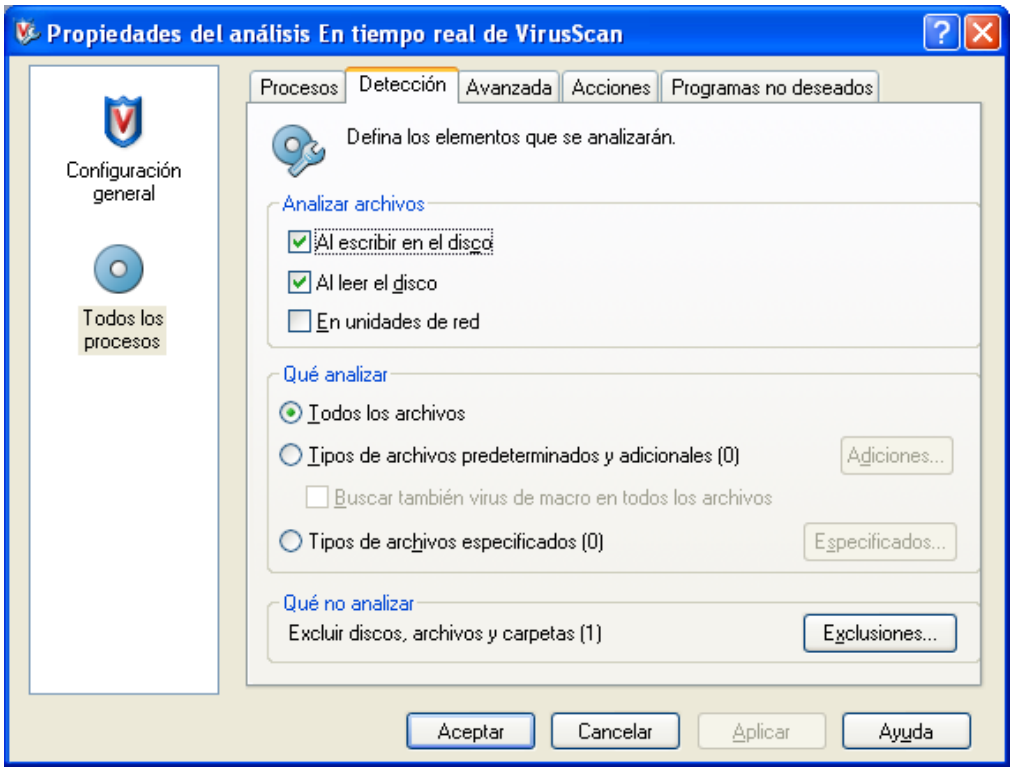


Figura 57.- **Propiedades de detección en el análisis en tiempo real de VirusScan.**
(Fuente: VirusScan 8.0i de McAfee)

- En esta pestaña se definen características avanzadas de la detección de software malicioso, presentando las siguientes opciones:
    - Búsqueda heurística para programas desconocidos.
    - Búsqueda heurística para macros desconocidos.
    - Analizar archivos comprimidos[117].
    - Analizar archivos codificados con MIME[118].

[116] Aquí es donde se relacionarían aquellos ficheros o carpetas que no se quiere que el antivirus analice por problemas de rendimiento, como por ejemplo, algunos ficheros de los controladores de dominio de Windows implicados en la replicación del directorio activo.
[117] Muy recomendable de activar, aunque hay que tener en cuenta que aquellos ficheros comprimidos utilizando clave no se analizarían.
[118] *Multiporpouse Internet Mail Extensions*.

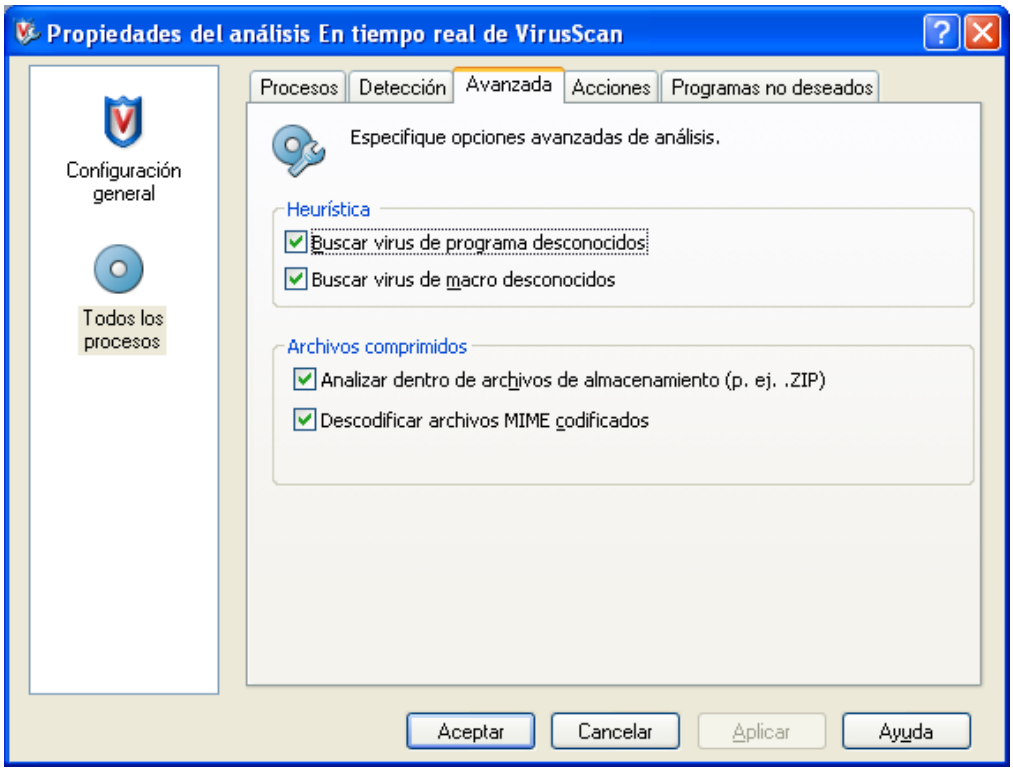


Figura 58.- **Propiedades avanzadas de detección en el análisis en tiempo real de VirusScan.**
(Fuente: VirusScan 8.0i de McAfee)

- Esta otra pestaña es de las más importantes, ya que en ella se van a configurar las acciones a realizar al detectar un virus:

  La acción principal, es la que se realizará en primera instancia, en caso de fallo, (que suele suceder cuando se elige la opción limpiar y ésta no se puede producir[119]) se pasará a realizar la acción secundaria.

  - Las posibles acciones, suelen ser:
    - Limpiar los archivos.[120]
    - Negar el acceso a los archivos.
    - Migrar los archivos.[121]

[119] Generalmente, porque el archivo se encuentra en uso.
[120] Esta opción suele presentarse únicamente en la acción principal.

- Borrar los archivos de forma definitiva.

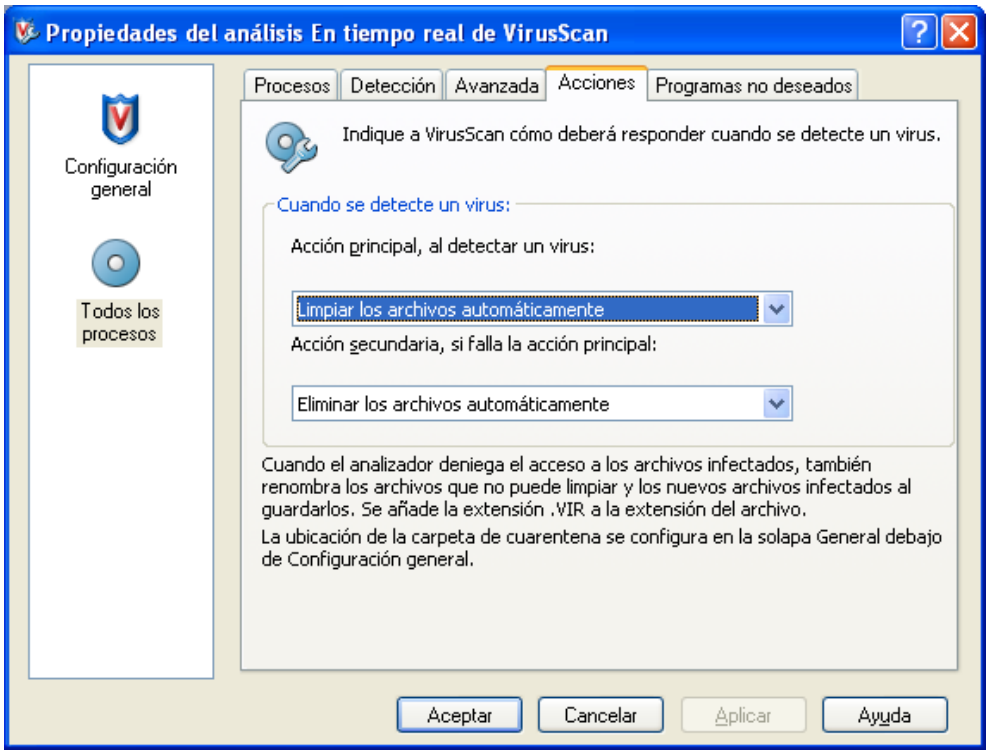


Figura 59.- **Propiedades de acción en el análisis en tiempo real de VirusScan.**
(Fuente: VirusScan 8.0i de McAfee)

- **(A.2.2.2) Archivos de registro de detecciones.**

Una de las partes más importantes en el sistema de antivirus es el registro de las detecciones ocurridas.

Normalmente se presenta como una opción más en la configuración del software antivirus, y es importante tener en cuenta que debe de estar de acuerdo con la política de registro de *logs* definida en la organización.

[121] Los archivos serán migrados a la carpeta configurada como cuarentena.

Será necesario definir, por tanto, las características, presentadas en la siguiente tabla:

CARACTERÍSTICAS DEL REGISTRO DE DETECCIONES DEL SISTEMA ANTIVIRUS	
Nombre del archivo donde se registrarán los incidentes.	**Nombre y ubicación inicial del registro. Puede encontrarse en el propio equipo donde se ejecuta el antivirus, o ya dirigirla a un sitio de red, con la consiguiente posibilidad de copias de seguridad.**
Tamaño y formato del archivo.	**En base al tamaño se establecerá una política de almacenamiento y rotación de logs.**
Qué se registrará	• **Actividades víricas.** • **Inicio de sesión.** • **Usuario que inicia sesión.** • **Fallo en la exploración.**
Política de almacenamiento y copias de seguridad	**Tiempo de duración mínimo del almacenamiento del registro.**

Tabla 16 .- Características del registro de detecciones del sistema antivirus.

Como ejemplo en la definición del archivo de registro de detecciones, se presenta una pantalla de configuración de un software antivirus a nivel cliente:

- Se pueden observar las siguientes posibilidades de configuración:
  - Nombre y ubicación del archivo de registro de las detecciones[122].
  - Tamaño máximo del archivo de registro, en caso de que se decida limitar dicho tamaño.
  - Formato del archivo, suele posibilitar:
    - ANSI (*American Nacional Standards Institute*).
    - Unicode[123].

[122] Se utiliza una variable del sistema para definir la ubicación de los archivos.
[123] Suele haber dos posibilidades: UTF8 (8-bit *Unicode Transformation Format*) y UTF16.

- Los elementos que desean registrarse en la detección, es decir, de qué campos estará formado el registro de detección de actividades víricas.

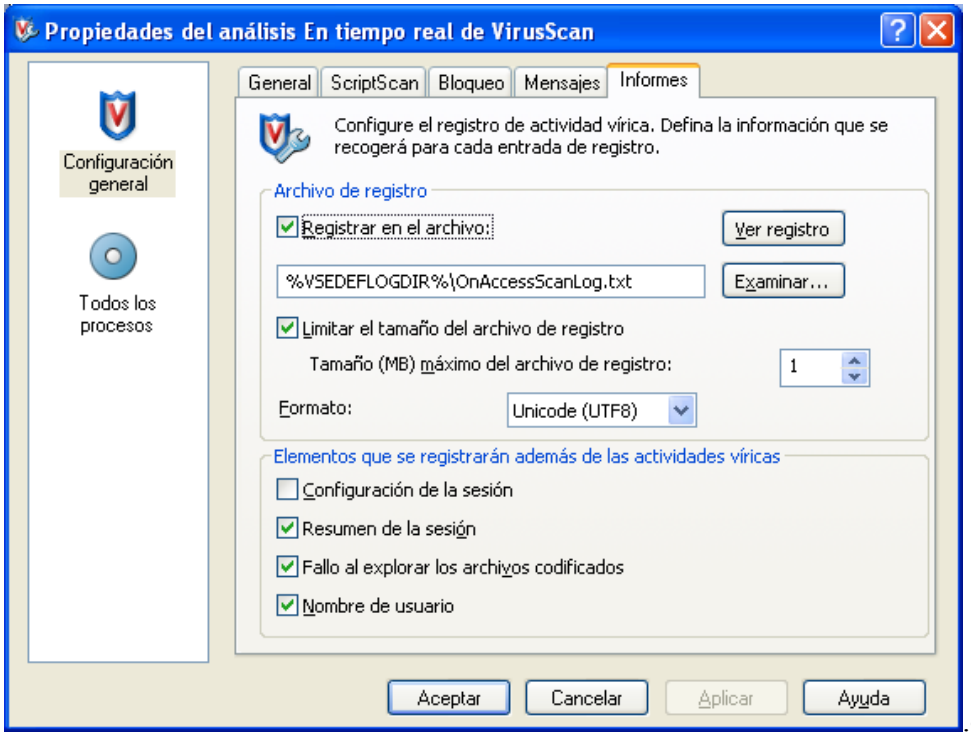


Figura 60.- **Propiedades del informe en el análisis en tiempo real de VirusScan. (Fuente: VirusScan 8.0i de McAfee)**

- **(A.2.2.3) Sistema de alarmas.**

Tan importante como registrar los eventos producidos por la detección de un virus, es configurar un correcto sistema de alarmas, de forma que cuando éste se detecte, el incidente se comunique lo antes posible a las personas o sistemas adecuados.

Esta parte de la definición del sistema antivirus está altamente relacionada con fases posteriores de la gestión del servicio ITIL, más concretamente, con la comunicación de incidentes de seguridad. Se puede decir que será el primer paso del engranaje de todo el

proceso de la gestión de un incidente de seguridad ocasionado por un virus en la organización.

Normalmente, los sistemas antivirus a nivel organización constan de un módulo aparte para gestionar el sistema de alarmas. Estas alarmas serán gestionadas por un servidor antivirus, que además de registrarlas, las lanza a aquellos usuarios, normalmente administradores u operadores de seguridad, así como a los sistemas de recepción de alarmas, mediante un correo o incidencia al CAU.

Otra posibilidad de definición, ésta ya a un nivel más local, es el mensaje que se reflejará en el puesto donde se ha detectado el virus. La redacción del mensaje que le aparecerá al usuario tiene mucha importancia, sin ser extremadamente alarmista, sí debe de dejar claro que el incidente requiere de toda su atención, y que se debe cumplir el procedimiento establecido para estos casos.

Existen configuraciones que en la presentación de este mensaje, dejan opción al usuario de actuar frente al virus, intentar limpiarlo, eliminarlo o mandarlo a cuarentena, aunque suele ser más recomendable, para evitar inconsistencias, que estas acciones vengan ya predefinidas por el sistema.

Se presenta un ejemplo de dichas posibilidades de configuración, en un software antivirus a nivel cliente:

- La primera opción a configurar es si se desea mostrar una alerta al detectar el virus[124].
- Seguidamente se configura el mensaje que se presentará al usuario, una vez detectado el virus[125].
- Por último, se elegirán las acciones permitidas al usuario, que dependerán de la política de cada organización[126].

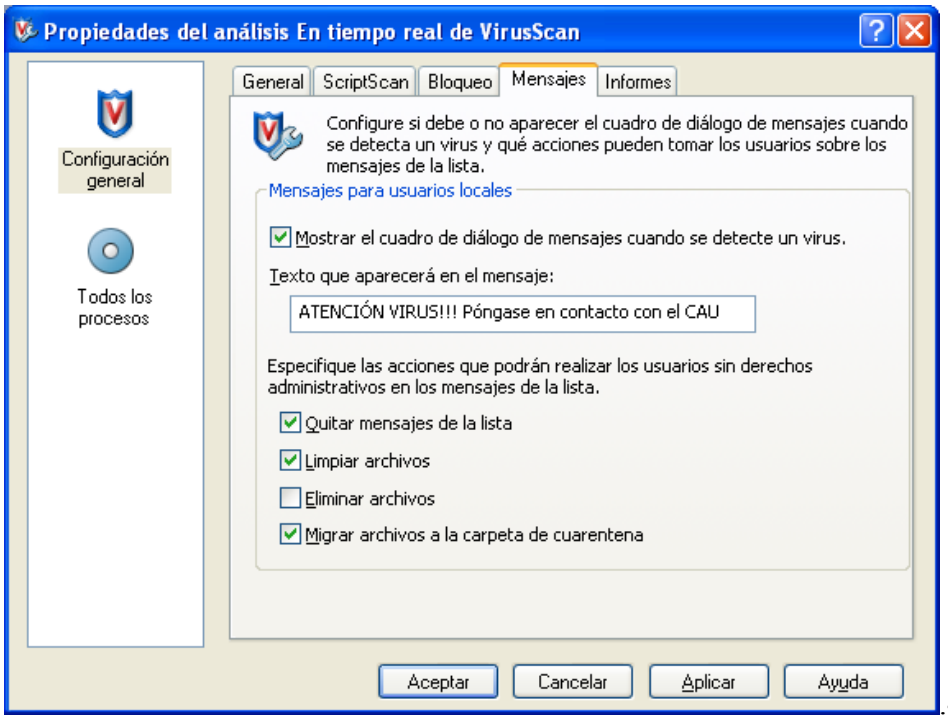


Figura 61.- **Propiedades de los mensajes en el análisis en tiempo real de VirusScan.**
(Fuente: VirusScan 8.0i de McAfee)

[124] Esta opción siempre debe estar configurada afirmativamente.
[125] Es importante hacer una referencia en este mensaje al punto de contacto del usuario con el sistema, para comunicar el incidente, en el caso de ITIL, obligatoriamente, el CAU.
[126] En ningún caso, se elegirá la primera opción de Quitar mensajes de la lista, y en muy raras ocasiones la opción de Eliminar archivos.

(A.2.3) Mantenimiento de los controles de seguridad.

- **(A.2.3.1) Procedimiento de actualización del antivirus.**

El antivirus es un programa, que trabaja analizando los archivos, en los que busca la existencia de códigos virales, que son cadenas particulares para cada virus y que el programa reconoce por comparación con su lista, o con la base de datos de definiciones, también llamada patrón de virus.

Se entiende que es fundamental que dicha lista de patrones de virus esté lo más actualizada posible. Como de todos es sabido, cada día aparecen numerosos virus, es por lo tanto fundamental intentar definir un sistema de actualización lo más automatizado posible. El objetivo es una actualización del sistema que dependa en el menor grado posible de la acción humana.

Normalmente las nuevas bases de datos, que consisten en una serie de ficheros, son descargadas de Internet. Los propios antivirus tienen, dentro de su configuración, la opción de actualizar los patrones de virus directamente desde Internet. Sin embargo, es importante tener en cuenta, que en la organización pueden existir sistemas que no puedan, por la propia política de seguridad de dicha organización, estar conectados a Internet, por lo tanto será necesario definir una serie de pasos para actualizar dichos sistemas "aislados" de la Red.

Existen varias posibilidades para superar este problema, dos de las más extendidas son:

1º.- Procedimiento de actualización basado en la interacción humana: un operador se descarga la nueva base de datos de los patrones de virus y la introduce en la red aislada.

2º.- Procedimiento de actualización basado en pasarelas: Se interpone una pasarela, que rompa el protocolo de red, entre el sistema aislado e Internet, opción que posibilita mucho más la automatización.

Procedimiento de actualización basado en la interacción humana.

El diagrama de casos de uso UML de este proceso, en el que intervienen como agentes, el operador y el administrador de seguridad, sería:

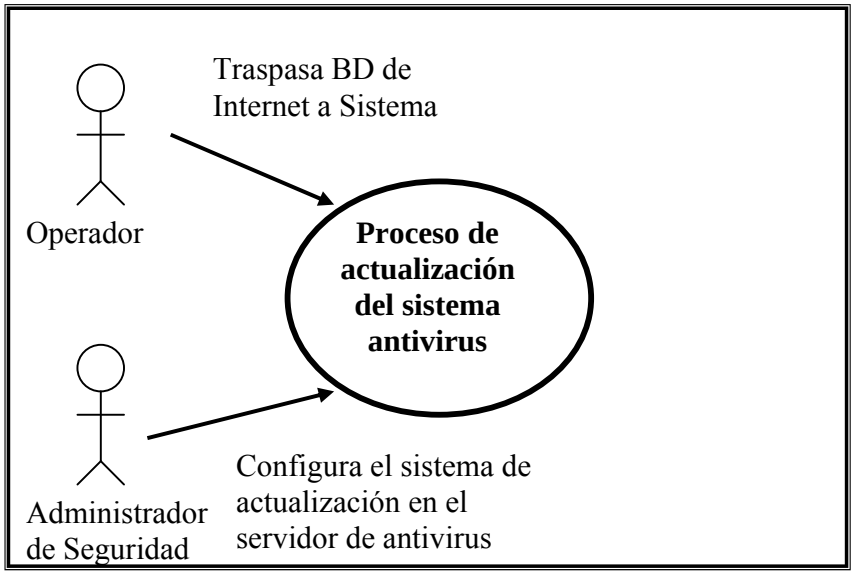


Figura 62.- **Caso de Uso: proceso de actualización del sistema antivirus.**
(Fuente: propia)

El operador realiza la función (últimamente de necesidad de frecuencia diaria) de traspasar la actualización del patrón de virus desde Internet hasta el sistema que se encuentra aislado. Esta función y su cumplimento exhaustivo es fundamental, ya que de ella depende en gran parte el éxito del sistema antivirus.

El Administrador de Seguridad configura el servidor de antivirus, de forma que distribuya la actualización del patrón de virus por todos los sistemas antivirus controlados por dicho servidor.

Aumentando un nivel, el sistema podría quedar definido de la siguiente forma:

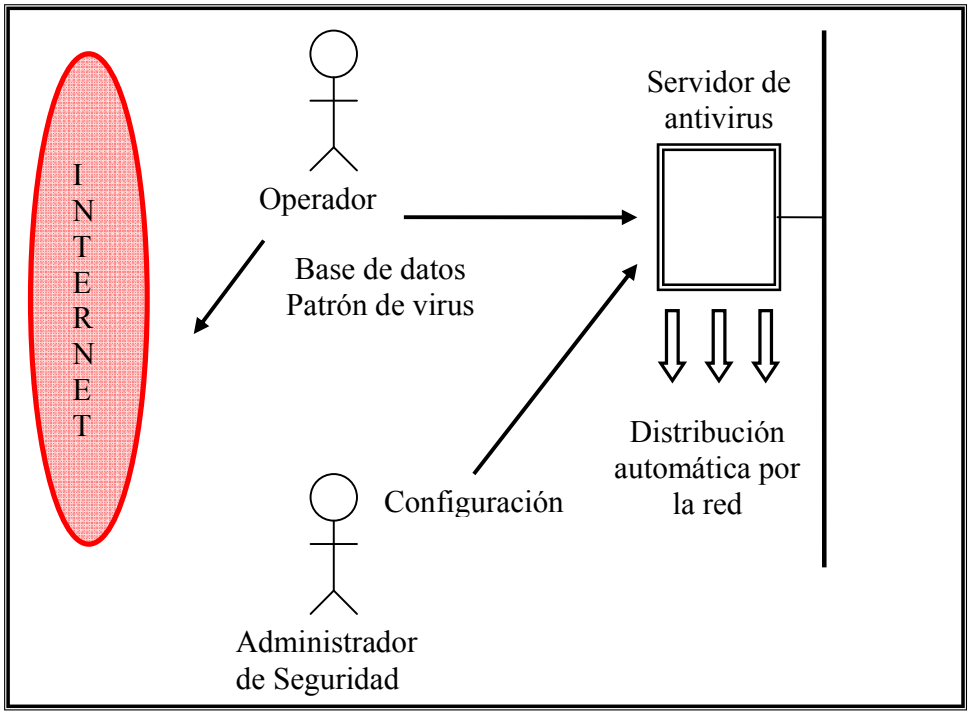


Figura 63.- **Caso de Uso: proceso de actualización del sistema antivirus.**
(Fuente: propia)

Procedimiento de actualización basado en pasarelas.

El diagrama de uso de este proceso, mucho más automatizado que el anterior, y donde sólo interviene como agente el administrador de seguridad, sería:

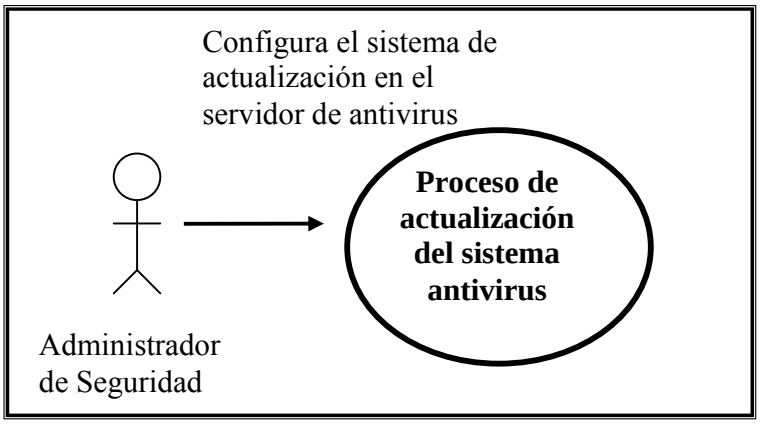


Figura 64.- **Caso de Uso: proceso de actualización del servicio antivirus basado en pasarelas.**
(Fuente: propia)

Aumentando un nivel, el sistema podría quedar definido de la siguiente forma:

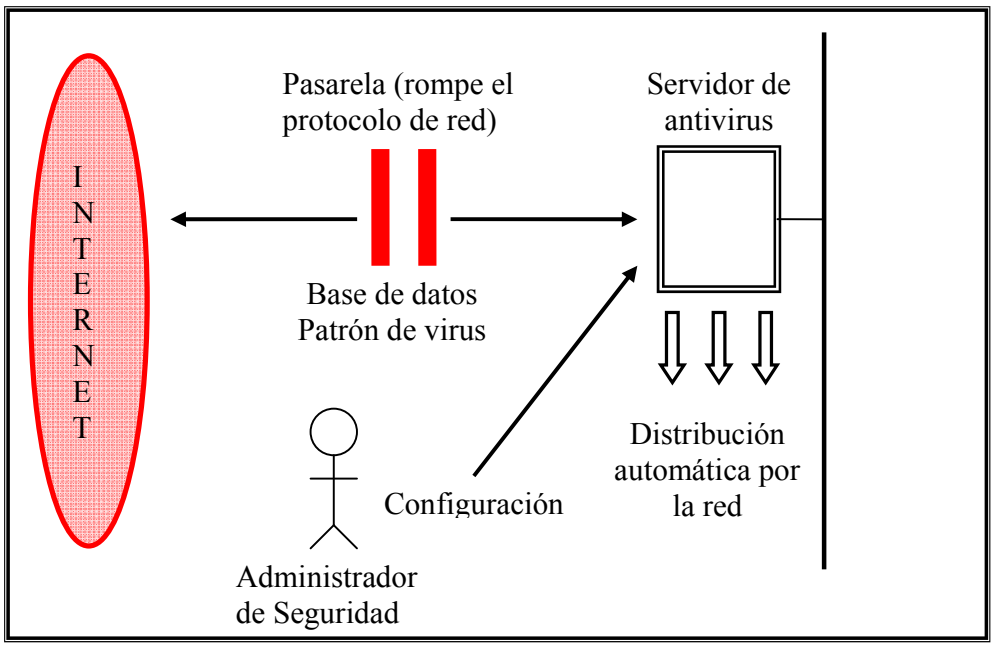


Figura 65.- **Caso de Uso: proceso de actualización del servicio antivirus basado en pasarelas.**
(Fuente: propia)

En este sistema, una vez configurado correctamente, no será necesaria la intervención de persona alguna, lo cuál aparte de ser más cómodo y disminuir costes, reduce en gran medida el riesgo de fallo.

Requiere un esfuerzo de monitorización del funcionamiento de la pasarela, aunque este funcionamiento puede corroborarse con la correcta actualización diaria del antivirus en la organización.

El sistema que define la pasarela puede estar basado en diversas técnicas, como por ejemplo la conexión de dos discos duros SCSI (*Small Computer System Interface*).

- **(A.2.3.2) Procedimiento de modificación de la configuración.**

La configuración del antivirus, y por tanto, el nivel de protección que aporta, puede requerir modificarse, según las necesidades de la organización.

Como ya se ha explicado anteriormente, la definición del nivel de protección a configurar en el antivirus, debe estar en equilibrio con el rendimiento de los sistemas que se ven afectados por dicho software. Es posible que, sobre todo en la capa de nivel servidor, las aplicaciones que soportan el negocio de la organización se vean afectadas por el análisis continuado de los ficheros. Por lo tanto, en determinados escenarios, se puede decidir excluir el análisis de ciertos ficheros o directorios completos, incluso el de desactivar ciertas funcionalidades del antivirus.

Lógicamente, según el impacto de estas modificaciones, éstas van a requerir la aprobación de las personas responsables de la Política de Seguridad de la organización.

Debe de existir un procedimiento que refleje el proceso completo de modificación. Un ejemplo podría ser este:

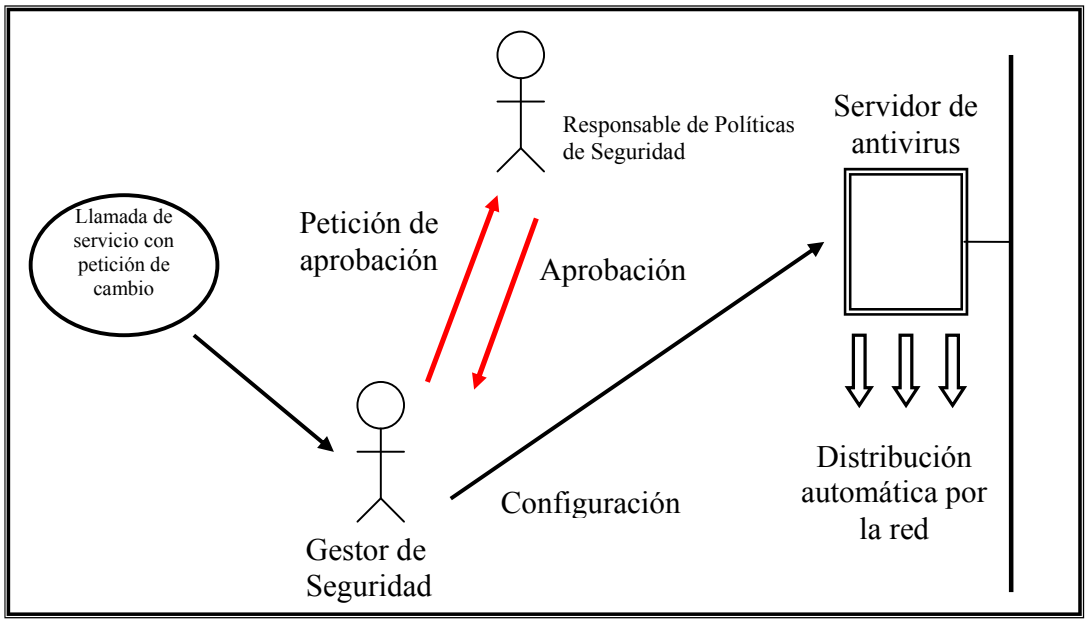


Figura 66.- **Proceso de modificación de la configuración del servicio antivirus.**
(Fuente: propia)

1.3. Modificación del nivel de seguridad (A.3)

Es posible que en determinadas circunstancias, normalmente por cambios en la Política de Seguridad de la organización, sea necesario modificar el sistema antivirus, de forma que corresponda con lo acordado en los ANSs. Se establecerá un procedimiento que sistematice estos cambios en los acuerdos.

- **(A.3.1) Procedimiento de cambio del nivel del antivirus.**

En este procedimiento, y debido a que necesita un nuevo acuerdo, van a intervenir el cliente, el proveedor y el experto en seguridad. Una vez decidido el nuevo ANS

(teniendo en cuenta el proceso de la gestión financiera) este acuerdo se traducirá en cambios que una vez aprobados repercutirán en las acciones correspondientes. Para la Gestión del Cambio es importante que un experto en Seguridad esté presente como un miembro más del GGC.

Una representación, en diagrama de casos de uso, de este procedimiento, sería:

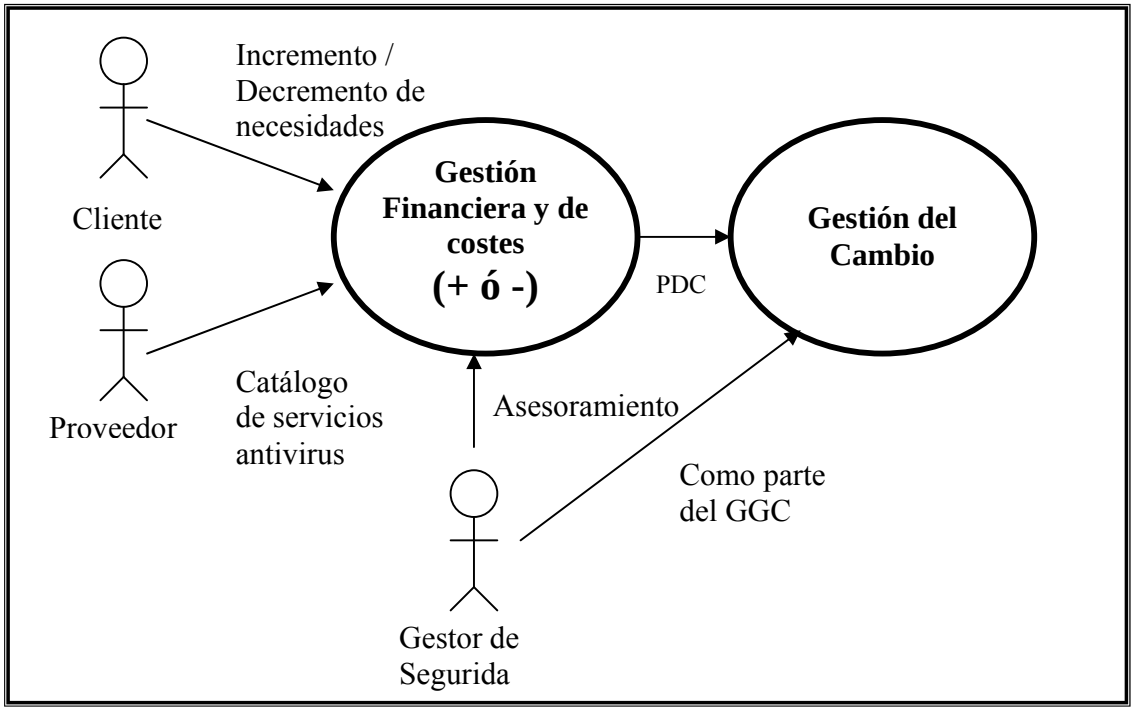


Figura 67.- **Caso de Uso: proceso de cambio de nivel del servicio de antivirus.**
(Fuente: propia)

1.4. Procedimientos de contingencia y recuperación (A.4)

Dentro del proceso general ITIL existe un proceso denominado de Gestión de la Disponibilidad que está estrechamente relacionado con la seguridad, y por ende, con el sistema antivirus, en tanto en cuanto que, precisamente uno de los principales efectos del

software malicioso es precisamente ocasionar la pérdida de la disponibilidad de los sistemas infectados.

(A.4.1) Procedimientos de actuación.

Será necesaria la definición de unos procedimientos de recuperación de los sistemas afectados por virus. Estos procedimientos deben de estar incluidos en el proceso de Gestión de la Disponibilidad de la organización (como otros muchos) con la salvedad de que en la concreción de ellos, el administrador de seguridad es pieza clave, ya que debe de realizar un estudio completo de los efectos del virus, y según éste, definir la actuación del resto de los agentes implicados:

- Procedimiento de actuación a nivel usuario.
- Procedimiento de actuación a nivel operador.
- Procedimiento de actuación a nivel Administrador de Seguridad.

El diagrama de casos de uso de la Gestión de la Disponibilidad sería:

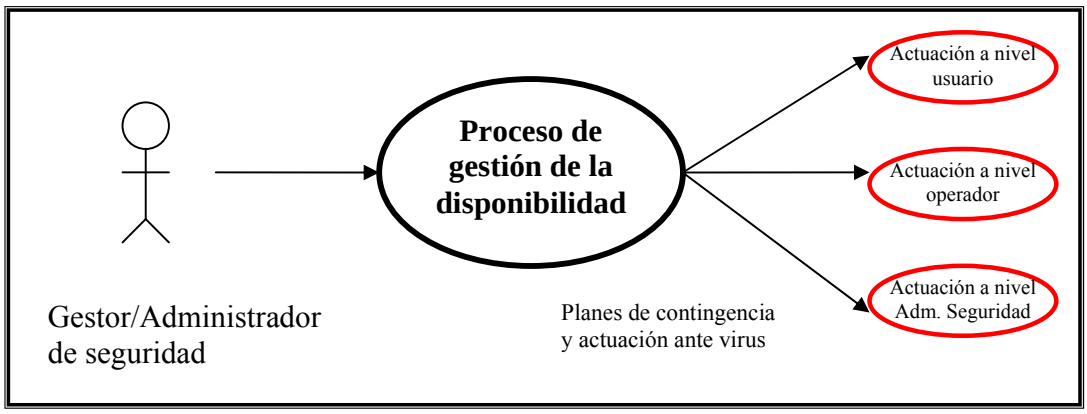


Figura 68.- **Caso de Uso del proceso de gestión de la disponibilidad del servicio antivirus.**
(Fuente: propia)

2. Procesos que ofrecen el Servicio (B)

En MISITILEON, los procesos pertenecientes a este grupo se encargan de ofrecer de forma controlada y eficaz los servicios TI a la organización. En el escenario de un sistema antivirus, los procesos de este grupo B se van a encargar, precisamente, de ofrecer y mantener dicho servicio, es decir, de gestionar e intentar solucionar todas las incidencias, problemas y cambios que pueda ocasionar el software malicioso que intente penetrar en un sistema, así como controlar que se está actuando correctamente para que esto no ocurra.

Los agentes que intervienen directamente en los procesos que ofrecen el servicio antivirus se pueden ver en el siguiente diagrama de casos de uso:

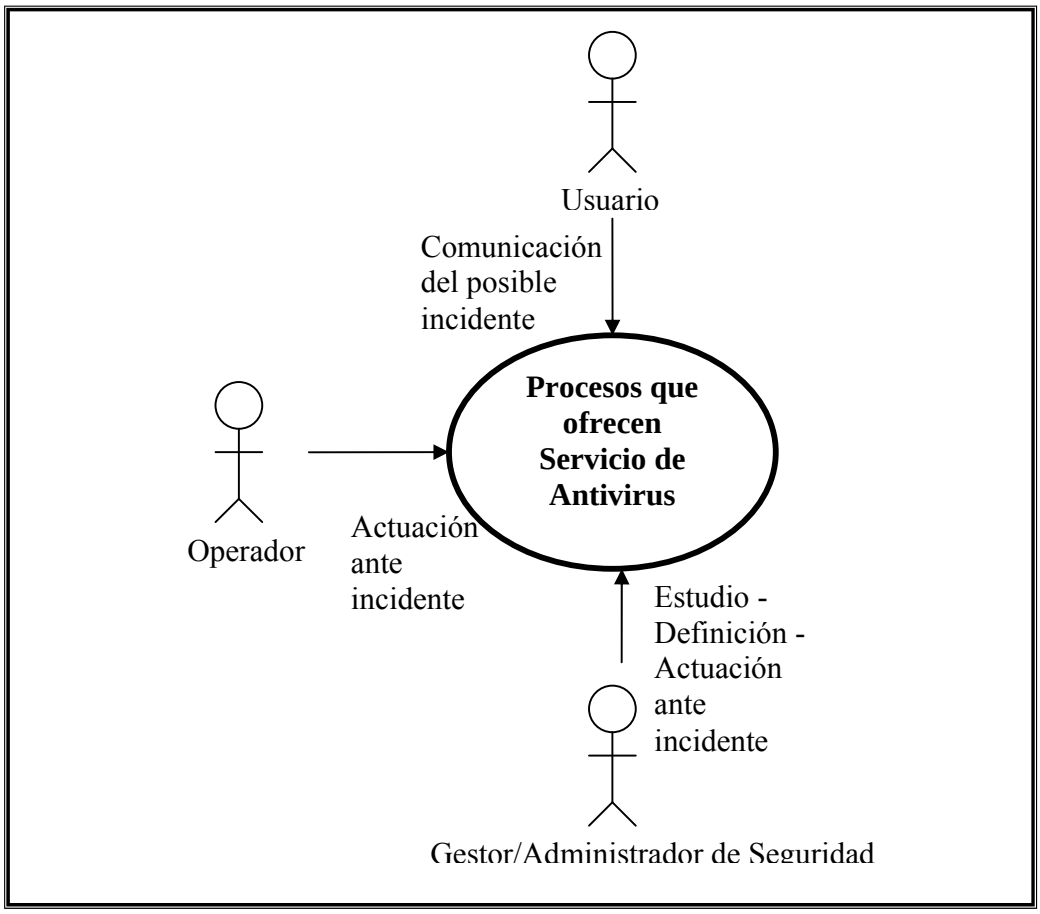


Figura 69.- **Caso de Uso: procesos que ofrecen Servicio de antivirus.**
(Fuente: propia)

2.1. Proceso de Recogida de incidentes de seguridad (B.1)

Uno de los aspectos clave para el buen funcionamiento de esta metodología consiste en que el punto de recogida de todos los incidentes de seguridad sea único, en concreto, sea exclusivamente el CAU.

Los incidentes provocados por posibles virus deben ser recogidos en dicho CAU, teniendo en cuenta que, como todos los incidentes de seguridad, éstos pueden ser comunicados por diferentes vías.

Se presenta el caso de uso de todas las posibilidades:

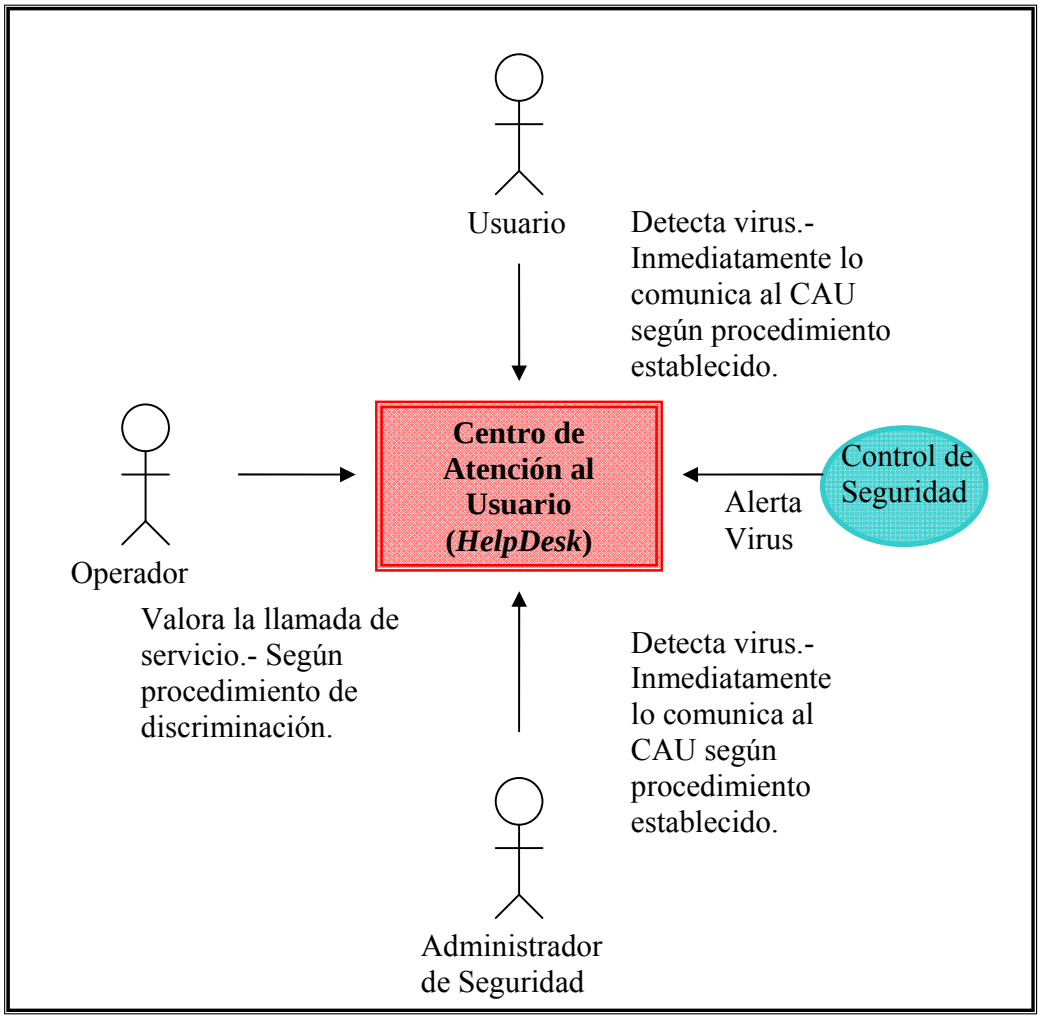


Figura 70.- **Caso de Uso: proceso de recogida de incidentes de seguridad.**
(Fuente: propia)

Procedimientos de recogida de incidentes de seguridad como posible virus.

Esta multiplicidad en la comunicación de los incidentes requiere de una precisa descripción de los procedimientos que se llevarán a cabo para comunicar y recoger dichos incidentes.

- **(B.1.1) Procedimiento de comunicación de posible virus, a nivel usuario.**

Es fundamental que la organización al completo tenga una concienciación plena de la importancia que representa su papel para mantener un nivel de seguridad adecuado. El usuario será la pieza clave dentro de todo el proceso de Gestión de la Seguridad, y cómo no, dentro del sistema creado para controlar los virus que puedan atacar a la organización.

De su actitud y rápida actuación ante un aviso de virus puede depender el impacto de éste. A continuación se presentan una serie de pasos, que habrá que comunicar al usuario, de cómo debe actuar ante la aparición de un posible virus en el sistema:

- El usuario recibe una alarma desde el sistema antivirus (a nivel cliente) instalado en su estación de trabajo.

  (Según configuración de sistema antivirus a nivel cliente -> enlace con A.2.2.3).
- El usuario se limita a anotar la información emitida por la alarma, pero NO actúa sobre el sistema.
- El usuario comunica, lo antes posible, el incidente al CAU. La forma de comunicación depende de la configuración de *HelpDesk*, pero dos son las vías habituales:
  - Llamada telefónica.

- Correo electrónico, con formato predefinido.

(B.1.2) Procedimiento de discriminación de llamadas de servicio, a nivel operador.

El CAU es el único punto de recepción y registro de incidentes en la organización, por lo tanto, todos lo avisos de posible virus deberán pasar por dicho Centro.

Los virus, como incidentes de seguridad, normalmente van a tener asignado un procedimiento especial debido a la necesidad de tratamiento de confidencialidad y actuación inmediata que requieren.

Es por tanto fundamental que el CAU sea capaz de discriminar aquellos incidentes ocasionados por virus, en el plazo de tiempo más breve posible, para poder darle el tratamiento antes comentado.

Para poder realizar este proceso de discriminación es necesario que dispongan de un catálogo perfectamente actualizado, donde figuren las acciones a realizar ante un aviso de virus.

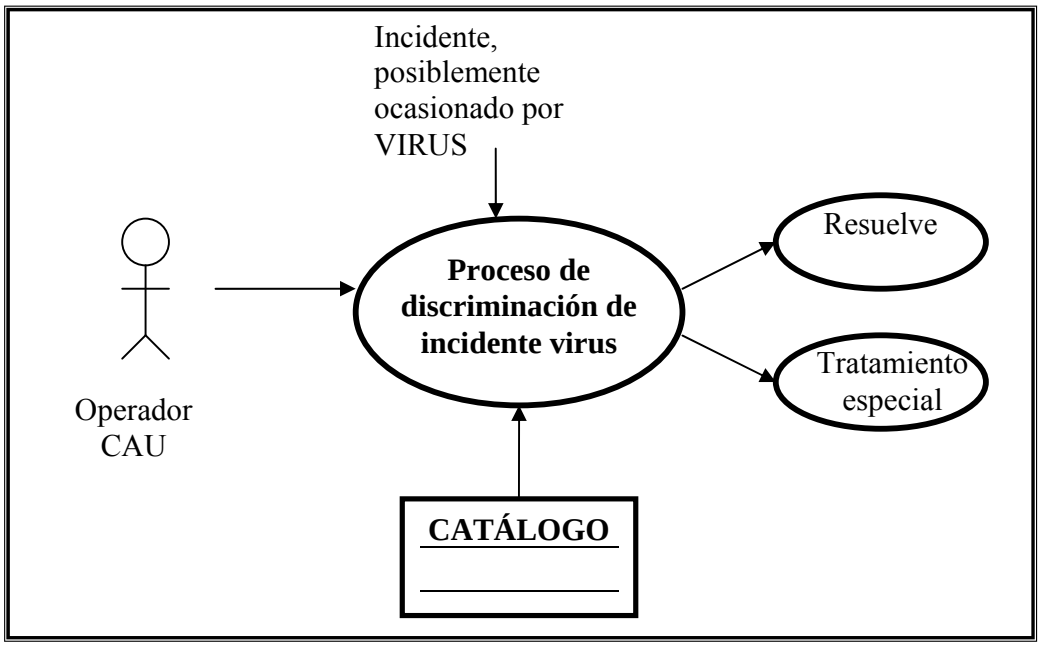


Figura 71.- **Caso de Uso: proceso de discriminación de incidente ocasionado por VIRUS.**
(Fuente: propia)

- **(B.1.3) Procedimiento de comunicación de posible virus, a nivel Administrador de Seguridad.**

Una de las funciones del Administrador de Seguridad es la monitorización de los diferentes controles de seguridad desplegados por la organización.

En el caso del sistema antivirus, por lo general, el Administrador de Seguridad será el encargado de gestionar los servidores de antivirus, además será una de las personas que figurarán en la configuración como receptores de las alarmas que puede ocasionar un virus al entrar en el sistema.

El Administrador de Seguridad será entonces otra de las fuentes de detección, y por tanto de comunicación al CAU de incidentes ocasionados por virus:

- El Administrador recibe una alarma de aviso de virus desde alguno de los controles.
- El Administrador notifica al CAU el aviso por cualquiera de las siguientes vías:
    - Llamada telefónica.
    - Correo electrónico, con formato predefinido.

(B.1.4) Procedimiento de comunicación de posible virus, a nivel Control de Seguridad.

Los controles de seguridad, en este caso los distintos programas antivirus de cualquiera de los tres niveles, deben de estar correctamente configurados para que emitan las alarmas a las personas correspondientes.

Esta función de configuración se realiza en el apartado A.2.2. *(Según configuración de controles de seguridad -> enlace con A.2.2)* y es un proceso fundamental para que se realice de forma correcta la comunicación de incidentes, y por tanto, el Proceso de Recogida de Incidentes.

Será función del proceso de definición de los controles *(Según definición de controles de seguridad -> enlace con A.2.1)* decidir qué personas (o sistemas) van a recibir los avisos de posible virus, en función del control de seguridad que detecte la alarma.

Así, no tiene la misma importancia (ni afectará de igual forma al sistema) un virus detectado por el control de antivirus a nivel de red[127], que un virus detectado a nivel cliente[128].

2.2. Proceso de Gestión de Incidentes de Seguridad (B.2)

Una vez que el incidente ocasionado por el posible virus es comunicado por alguna de las posibles vías, éste debe ser tratado.

Los incidentes ocasionados por virus, como incidentes de seguridad, tienen dos características especiales:

- El tratamiento de Confidencialidad.
- La necesidad de Actuación Inmediata.

El diagrama de casos de uso que genera un proceso de Gestión de Incidentes de Seguridad ocasionados por un virus es el siguiente:

[127] El virus no ha entrado aún en la organización.
[128] El virus ya se encuentra dentro de la organización.

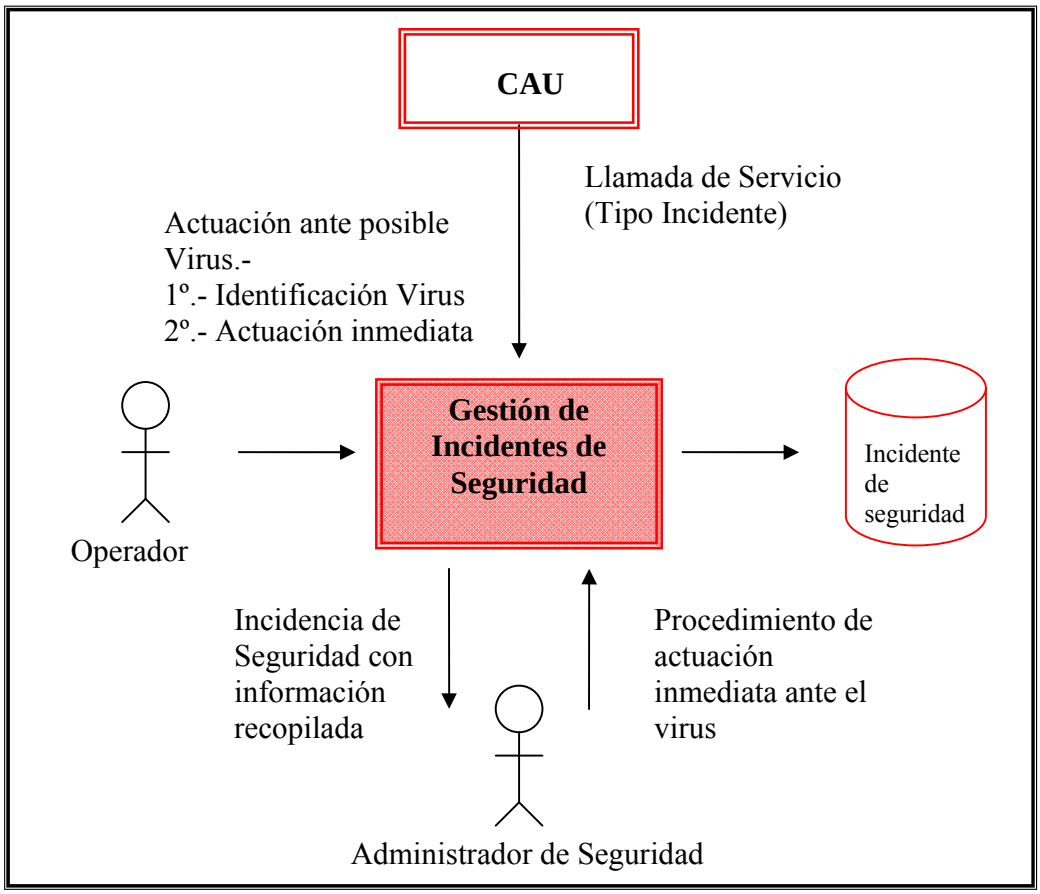


Figura 72.- **Caso de Uso: proceso de gestión de incidentes de seguridad.**
(Fuente: propia)

Procedimiento de Gestión de Incidentes de Seguridad ocasionados por virus

Una vez comunicado, el incidente debe ser registrado en el CAU. Será necesario intentar resolverlo o (si procede) escalarlo a las personas adecuadas[129]. Estas personas deberán definir el procedimiento para resolver el incidente en el menor tiempo posible.

Todas estas acciones deberán definirse en los siguientes procedimientos:

[129] Normalmente expertos en seguridad, a veces incluso en software malicioso.

- **(B.2.1) Procedimiento de actuación, a nivel operador, ante un posible virus.**

El operador perteneciente al CAU deberá realizar el siguiente procedimiento ante un incidente catalogado como "virus".

- Recibe el incidente, lo registra y en su caso lo cataloga como virus.

(Según procedimiento de llamadas de servicio a nivel operador -> enlace con B.1.2)

- Se pone en contacto con el usuario para recuperar la máxima información:
  - ¿Cómo detectó el usuario el virus?
  - ¿Cómo ha actuado ante el virus?
  - ¿Ha notado en qué puede estar afectada la máquina?
  - ¿Conoce otros posibles usuarios afectados?
- En este momento el operador debe ser capaz de decidir si puede actuar ante este incidente o debe escalarlo según instrucciones recibidas.
  - **Resuelve**, porque es un virus conocido[130] y está en disposición del procedimiento de actuación ante el virus.
  - **Escala**, porque no tiene instrucciones de actuación ante ese virus.

- **(B.2.2) Procedimiento de actuación, a nivel Administrador de Seguridad, ante un posible virus (Definición de actuación inmediata).**

El Administrador de Seguridad, como experto en sistemas de seguridad (y en este caso en sistemas antivirus) será la figura más indicada para resolver los problemas ocasionados por un virus.

[130] Es decir, está en el catálogo de virus.

El procedimiento a seguir será el siguiente:

- Recibe el incidente de seguridad (escalado desde el CAU) de posible virus, con toda la información recopilada por dicho centro.
- En función de la información recopilada (y toda aquella que él pudiera encontrar) realizará un estudio de las posibles acciones y soluciones ante el virus. En caso de necesitar recuperar los ficheros infectados, esta recuperación y su posterior tratamiento deberán hacerse mediante un método seguro.
- Comunicará al CAU una actualización del catálogo de virus, con la inclusión del nuevo virus detectado.
- Creará un procedimiento de actuación inmediata, para intentar interrumpir la acción del virus a la mayor brevedad posible.
- Distribuirá el método de acción inmediata entre las personas implicadas, normalmente el CAU *(Según procedimiento de actuación a nivel operador, ante un virus -> enlace con B.2.1)* aunque también podrían verse implicadas personas de otros departamentos, como el taller de Mantenimiento, personas responsables de informática de los organismos afectados, etc…

2.3. Proceso de Gestión de Problemas de Seguridad (B.3)

Este proceso tiene una especial relevancia en el caso de incidentes ocasionados por virus.

Una de las principales características de la mayoría de los virus es, una vez que se ha introducido en un sistema, usar la copia como forma de transmisión por el propio sistema. Si el virus consigue su propósito, un posible incidente se convertirá en numerosos incidentes relacionados, es decir, se convertirá en un problema de seguridad.

Será necesario por tanto, definir cómo interviene el responsable de Seguridad en los procesos de resolución de problemas ocasionados por un virus.

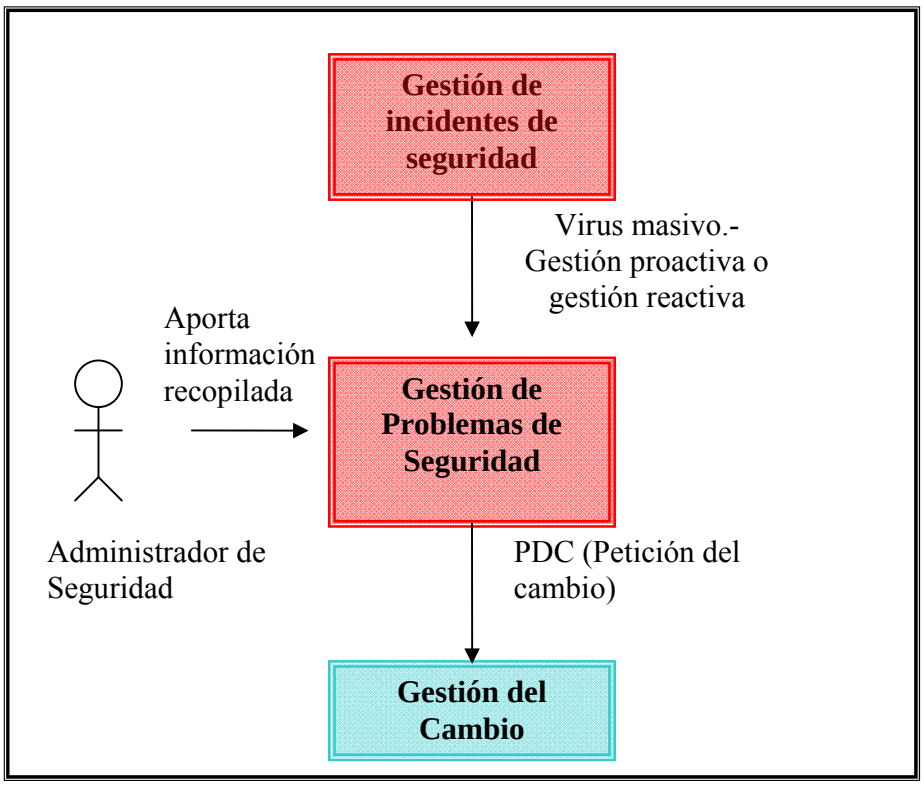


Figura 73.- **Caso de Uso: proceso de Gestión de Problemas de Seguridad.**
(Fuente: propia)

Procedimiento de gestión de Problemas de Seguridad ocasionados por virus.

El administrador de seguridad es el responsable de definir los procedimientos para actuar contra un virus determinado. Para realizar esta función, el administrador necesita recopilar la máxima información posible, esto es vital para la resolución del problema generado por el virus.

- **(B.3.1) Procedimiento de actuación, a nivel Administrador de Seguridad, ante un posible problema ocasionado por un virus.**

Este procedimiento es esencialmente el mismo que el realizado ante incidentes, *(Según procedimiento de actuación a nivel Administrador de Seguridad, ante un virus -> enlace con B.2.2).*

Las diferencias que puede haber con el producido ante un incidente de seguridad, estriban en la importancia del problema, es decir, en un problema de seguridad se supone que se han producido un número determinado de incidentes, el virus ya se ha extendido por la organización, por lo tanto, el impacto en la misma suele ser mayor.

El procedimiento a seguir será el siguiente:

- Recibe el problema de seguridad producido por el virus, escalado desde el CAU, con toda la información recopilada por dicho centro.
- En función de la información recopilada (y toda aquella que él pudiera encontrar) realizará un estudio de las posibles acciones y soluciones ante el problema.

- Creará un procedimiento de actuación inmediata o ampliará, si existe, el creado en su momento para el incidente ocasionado por el virus. En este caso además de intentar interrumpir la acción del virus, es muy posible que sea necesario definir las siguientes acciones:
    - Comunicaciones a otros organismos afectados.
    - Acciones de limpieza del virus.
    - Acciones de mantenimiento de disponibilidad de los sistemas.

    (Según procedimientos de actuación generales ante un virus -> enlace con A.4.1)
    - Distribuirá el método de acción inmediata entre las personas implicadas.

2.4. Proceso de Gestión de Configuración y Cambio (B.4)

Los sistemas están sujetos a continuos cambios, bien porque lo implique la resolución de un problema (que puede ser de seguridad o no) bien porque simplemente dichos sistemas evolucionan.

En dichos cambios será necesario tener en cuenta el nivel de seguridad decidido y aportado por el sistema antivirus de la organización, es decir, los nuevos sistemas que generen los cambios deben de estar integrados en el sistema antivirus (deben de tener antivirus en los distintos niveles que participen en el sistema).

- **(B.4.1) Procedimiento de colaboración del Administrador de Seguridad ante un Cambio. Pertenencia al GGC.**

Este procedimiento simplemente pretende dejar clara la conveniencia de colaboración de los expertos en Seguridad de la organización en los cambios, sobre todo en aquellos que afectan directamente a la seguridad (teniendo en cuenta que siempre es decisión del Gestor del Cambio la composición del grupo GGC):

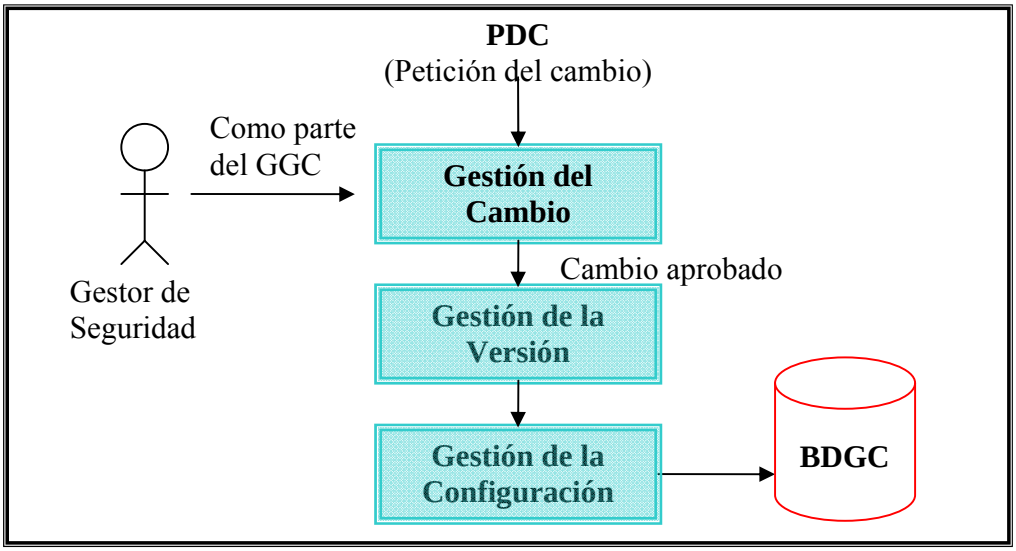


Figura 74.- **Caso de Uso: proceso de Gestión de Problemas de Seguridad.**
(Fuente: propia)

CAPÍTULO VI. COMPROBACIÓN DE LA METODOLOGÍA.

Investigar es ver lo que todo el mundo ha visto y pensar lo que nadie más ha pensado[131].

En este capítulo es donde se va a evaluar si se han logrado los objetivos que se planteaban en el primer capítulo de esta tesis doctoral. Se trata de una validación teórica de la metodología MISITILEON mediante un caso de estudio: la gestión del servicio de antivirus.

1. Objetivo de la Comprobación

El objetivo de la comprobación es verificar si el uso de la metodología propuesta en esta tesis doctoral, MISITILEON, mejora en algunos aspectos la eficiencia de uso de ITIL.

Para validar dicha propuesta se han llevado a cabo una serie de experimentos con el ejemplo concreto descrito en el capítulo anterior.

[131] Albert Szent-Györgi (1893-1986), bioquímico húngaro-estadounidense.

2. Problemática

Un virus informático es un programa con la capacidad de transmitirse entre ordenadores y redes, generalmente sin el conocimiento de los usuarios [OLD01]. Además, la mayoría de ellos tienen la característica de contener código malicioso, que en el mejor de los casos, pretende alterar el funcionamiento normal de la computadora. Dicho código malicioso contenido en los virus es denominado carga[132] dañina, y puede tener distintos objetivos, desde motivos basados en un reto personal del propio autor del virus, hasta realizar daños importantes en los sistemas, con la eliminación de datos o el bloqueo de los sistemas, denominado denegación de servicio[133].

Es evidente que una organización que en la actualidad no desarrolle un Sistema de Gestión de la Seguridad de la Información está poniendo en grave peligro, además de dicha información, su capacidad de funcionamiento.

El hecho de que una organización implemente un sistema de gestión de sus servicios TI, lógicamente, no le exime de la necesidad de gestionar la seguridad; al contrario, la gestión de los servicios y la gestión de la seguridad son disciplinas perfectamente adaptables y su desarrollo facilita la implantación de cualquiera de ellas.

Una vez planteada la necesidad que tienen las organizaciones de gestionar la Seguridad de la Información, así como de gestionar los servicios que ofrecen sus

[132] En inglés: *payload.*
[133] En el apartado 5.3 del capítulo 2 de esta memoria se halla una taxonomía de los virus informáticos más conocidos.

infraestructuras TI, este capítulo trata de evaluar los beneficios que se consiguen con MISITILEON, es decir, con la integración de la gestión del servicio de seguridad dentro de los procesos ITIL.

Seguidamente se representa una simulación de gestión del servicio de antivirus en una organización donde se ha implantado MISITILEON.

3. Evaluación de la implantación de MISITILEON

Para esta evaluación se compararon los efectos que puede ocasionar un virus informático en una organización donde no se utiliza ningún método de gestión de servicios TI, con otra organización donde está implantado MISITILEON.

3.1. Escenario 1: Una organización que NO usa MISITILEON.

Para este primer escenario, se planteó una organización donde no se había implantado ningún método ordenado para gestionar sus servicios, o por lo menos, no se había incluido la gestión de su seguridad dentro de dicho proceso de gestión de servicios.

En dicha organización existe un taller de informática que va a recibir los avisos que se produzcan referidos a los equipos de informática de la organización.

Los avisos le pueden llegar directamente o quizá gestionados por un punto de control, donde distingan si éstos se refieren a equipos informáticos o se trata de alguna anomalía en cualquier otro equipo o sistema, en cuyo caso trasladarán el aviso a otro taller.

En la organización existen expertos en seguridad informática, en este caso, expertos en sistemas antivirus, que en caso de ser requeridos apoyarán al taller de informática en el estudio y tratamiento del incidente ocasionado por el virus.

La jornada laboral (único horario que se ha contabilizado) se ha supuesto de ocho horas, desde las 8:00 hasta las 16:00 horas.

"Un virus ha afectado a la organización, tenemos un problema".-CASO 1

A continuación se presenta una tabla con la descripción de las tareas acontecidas con ocasión de la intrusión de un virus en el sistema informático de la organización, el tiempo de duración de las tareas es una estimación[134].

DESCRIPCIÓN DE TAREAS					
Hora Inicio	**Hora Fin**	**Tipo**	**Descripción**	**Tiempo**	**Tiempo Total**
01/01 d 09:00 h	01/01 d 09:00 h	Hito 1	Aparece una alarma del sistema antivirus en una estación de trabajo.	0	**0**
01/01 d 09:00 h	01/01 d 10:00 h	Tarea 2	El aviso es notificado por el usuario.	1 hora	**1 hora**
01/01 d 10:00 h	01/01 d 11:00 h	Tarea 3	El taller de informática recibe el aviso y lo coloca en la lista de espera, con carácter urgente.	1 hora	**2 horas**
01/01 d 11:00 h	01/01 d 14:00 h	Tarea 4	El aviso permanece en el estado "en lista de espera", mientras el usuario manipula la máquina, con lo que esto puede suponer para los efectos del virus.	3 horas	**5 horas**
01/01 d 14:00 h	01/01 d 15:00 h	Tarea 5	El técnico del taller de informática inspecciona la máquina, constatando que el virus ha sido detectado por el sistema antivirus, y que la máquina NO está infectada.	1 hora	**6 horas**
01/01 d 15:00 h	05/01 d 12:00 h	Tarea 6	Aparecen nuevas alarmas de virus en distintas estaciones de trabajo, son comunicados y posteriormente tratados.	29 horas	**35 horas**

[134] Es una media calculada por la doctorando en base a la experiencia obtenida en varias empresas (IECISA, Intecsa, Nvía, Velice, Mystica, Biodactil,…).

DESCRIPCIÓN DE TAREAS					
Hora Inicio	**Hora Fin**	**Tipo**	**Descripción**	**Tiempo**	**Tiempo Total**
02/01 d 15:00 h	05/01 d 12:00 h	Tarea 7	El técnico del taller de informática inspecciona las máquinas, una a una, constatando que el virus ha sido detectado por el sistema antivirus, y que las máquinas NO están infectadas.	21 horas	**35 horas**
05/01 d 12:00 h	05/01 d 12:00 h	Hito 8	Una estación tiene un funcionamiento anómalo.	0 horas	**0 horas**
05/01 d 12:00 h	05/01 d 13:00 h	Tarea 9	El usuario comunica lo ocurrido.	1 hora	**36 horas**
05/01 d 13:00 h	05/01 d 14:00 h	Tarea 10	El taller de informática recibe el aviso, y lo coloca en la lista de espera, esta vez sin carácter de urgencia.	1 hora	**37 horas**
05/01 d 14:00 h	10/01 d 12:00 h	Tarea 11	El aviso permanece en el estado "en lista de espera", mientras el usuario manipula la máquina, con lo que esto puede suponer para los efectos del virus.	38 horas	**75 horas**
05/01 d 14:00 h	15/01 d 12:00	Tarea 12	Aparecen nuevos avisos de funcionamiento anómalo en distintas estaciones de trabajo, son comunicados y posteriormente tratados.	78 horas	**115 horas**
10/01 d 12:00 h	10/01 d 15:00 h	Tarea 13	El técnico del taller de informática inspecciona la máquina con funcionamiento anómalo, constatando que la máquina no tiene actualizado el antivirus y que posiblemente está infectada.	3 horas	**78 horas**
10/01 d 15:00h	11/01 d 12:00 h	Tarea 14	El técnico lo comunica al administrador del sistema antivirus, que comprueba los motivos por los que no está actualizada esa estación, así como si existen más máquinas no actualizadas[135].	5 horas	**83 horas**
11/01 d 12:00 h	12/01 d 12:00 h	Tarea 15	El administrador del sistema antivirus estudia los efectos del virus y los métodos existentes para su limpieza y lo comunica a los técnicos del taller de mantenimiento.	8 horas	**91 horas**

[135] En el mejor de los casos relacionan este aviso con los anteriormente producidos por las alarmas del sistema antivirus.

DESCRIPCIÓN DE TAREAS					
Hora Inicio	**Hora Fin**	**Tipo**	**Descripción**	**Tiempo**	**Tiempo Total**
12/01 d 12:00h	12/01 d 12:00 h	Hito 16	El administrador del sistema antivirus comunica a los implicados la situación de urgencia, así como el procedimiento de actuación ante el virus.	0 horas	**91 horas**
12/01 d 12:00 h	15/01 d 12:00 h	Tarea 17	Los técnicos del taller de informática proceden a la limpieza del virus, en caso de ser posible, así como al chequeo de TODAS las máquinas que no tenían actualizado el antivirus.	24 horas	**115 horas**

Tabla 17 .- Descripción de tareas CASO 1.
(Fuente: propia)

Algunos puntos de interés en las tareas antes descritas son:

- Los tiempos de todas las tareas son muy elevados, al no haber sido definidos procedimientos de actuación.
- El técnico del taller tiene que revisar máquina a máquina, ya que no hay gestión de problemas.
- El usuario sigue manipulando su máquina:, lo que favorece la expansión del virus.
- No tener un control estricto de la actualización del antivirus, unido a la rápida expansión de éste, puede ocasionar que haya máquinas infectadas y no se trate únicamente de avisos de detección.

Es muy importante tener en cuenta que el problema que se ha representado en este caso, se puede agravar considerablemente, pudiendo incluso llegar a no tener solución, dependiendo de lo dañino que sea el virus:

- Se pueden producir colapsos de red si el virus es por ejemplo un gusano con un índice alto de transmisión, aunque las máquinas que sí tienen actualizado el antivirus lo detecten.
- El virus puede penetrar en la organización antes de que el sistema antivirus pueda detectarlo; esto puede ocurrir incluso con el sistema antivirus actualizado, ya que desde que el virus aparece hasta que los sistemas antivirus lo incluyen en su base de datos pasa un tiempo crítico para el sistema.
- Existen virus que pueden llegar a borrar todos los datos contenidos en los discos duros.
- Si los efectos del virus aparecen mucho tiempo después, será mucho más difícil relacionarlo con el anteriormente detectado por el antivirus.
- Etc.

Se presentan los efectos de este ejemplo práctico en una organización compuesta por 1.000 estaciones de trabajo, donde penetra un virus con una capacidad de crecimiento[136] o transmisión de 5 equipos a la hora y suponiendo que el virus sólo se transmite con los equipos encendidos, es decir, durante la jornada laboral[137]:

EQUIPOS EN LA ORGANIZACIÓN	CRECIMIENTO DEL VIRUS	TIEMPO DE RESPUESTA ANTE EL VIRUS	NÚMERO DE MÁQUINAS INFECTADAS	% DE LA ORGANIZACIÓN INFECTADA
1000	**5 Equipos/hora**	**115 horas**	**575**	**57,5 %**

Tabla 18 .- Datos de evolución de virus en una organización sin MISITILEON.
(Fuente: propia)

[136] Se ha considerado un crecimiento lineal.
[137] Se ha supuesto que la jornada laboral es de 8 horas (15 días * 8 horas = 120 horas).

Seguidamente se muestra una representación (en forma de diagrama de secuencias con escala de tiempos) de la evolución del virus:

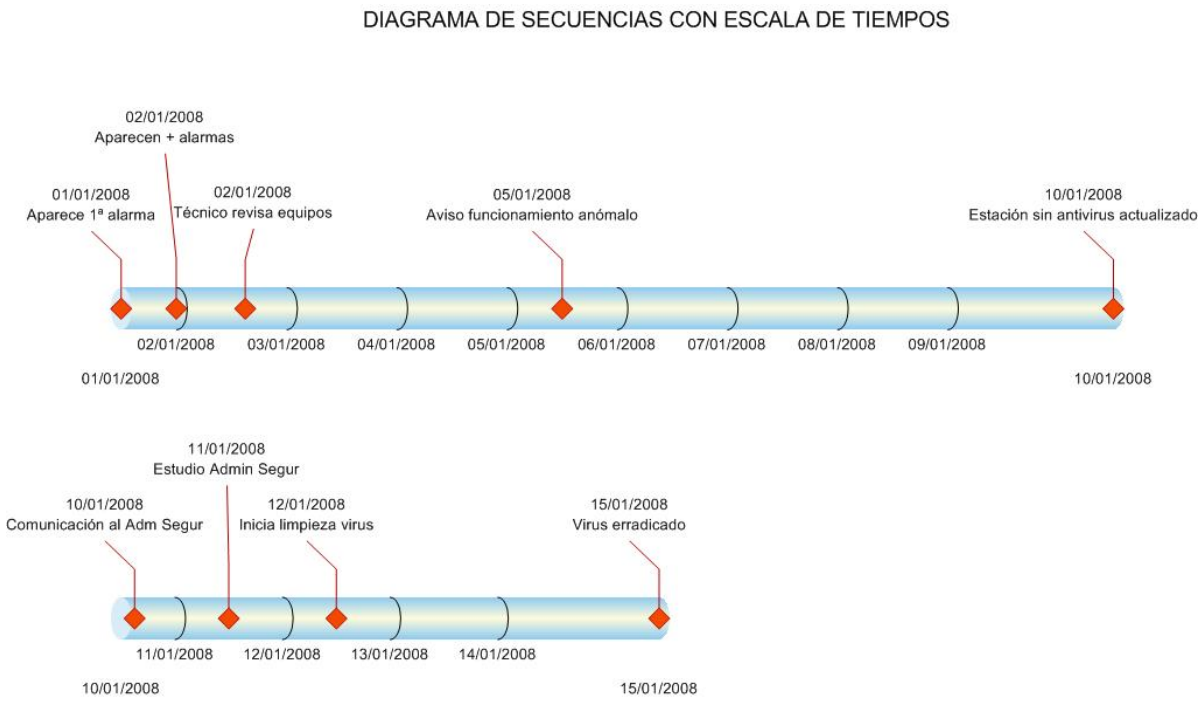


Figura 75.- **Diagrama de secuencias, de evolución del virus, con escala de tiempos, en una organización sin MISITILEON.**
(Fuente: propia)

La presentación más detallada y con acumulación de tiempos del diagrama anterior, sería:

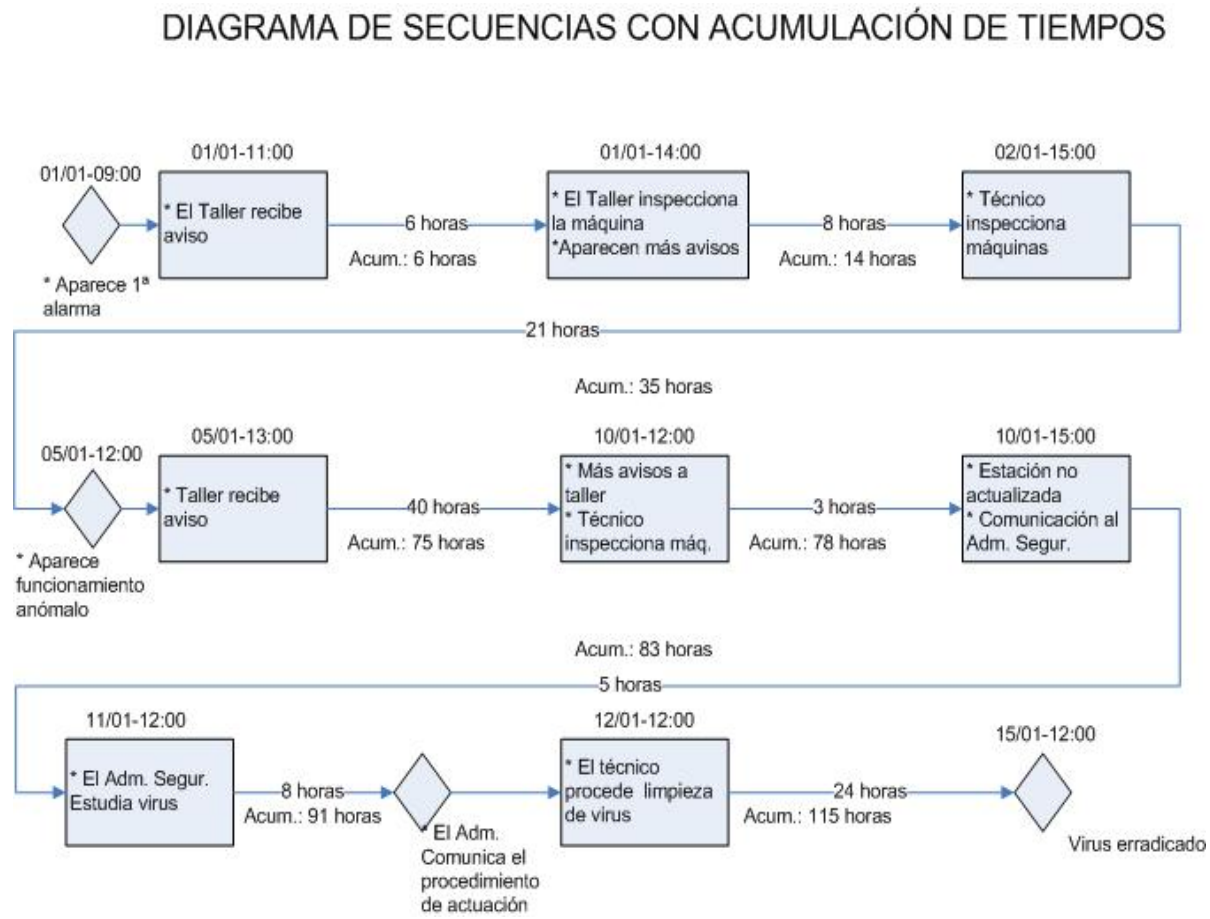


Figura 76.- **Diagrama de secuencias, de evolución del virus, con acumulación de tiempos, en una organización sin MISITILEON.**
(Fuente: propia)

Véase una representación gráfica de la infección en la organización:

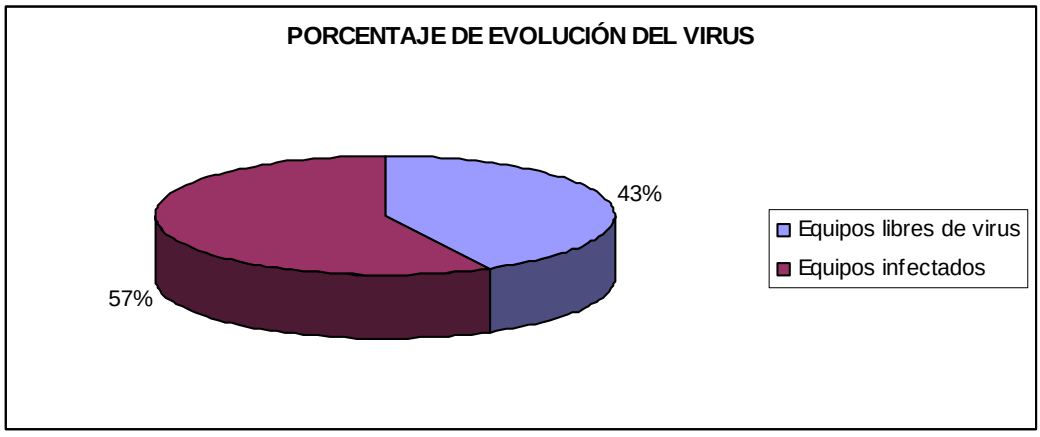


Figura 77.- **Porcentaje de evolución del virus en una organización sin MISITILEON.**
(Fuente: propia)

Una programación es una lista ordenada por tiempos de eventos planificados[138] [WAT97]. Para representar programaciones se suelen usar diagramas de Gantt. Seguidamente se utiliza un diagrama de Gantt para presentar, sino una programación, sí la lista de eventos acaecidos en la organización con ocasión de la infección del virus:

DIAGRAMA DE GANTT DE LA EVOLUCIÓN DEL VIRUS EN LA ORGANIZACIÓN

Id.	Nombre de tarea	Comienzo	Fin	Duración
1	Aparece la primera alarma de virus.	01/01/2008	01/01/2008	0d
2	El aviso es notificado por el usuario	01/01/2008	01/01/2008	1h
3	El Taller recibe el aviso y lo coloca en espera con carácter urgente	01/01/2008	01/01/2008	1h
4	El aviso permanece en lista de espera	01/01/2008	01/01/2008	3h
5	El Taller inspecciona el aviso	01/01/2008	01/01/2008	1h
6	Aparecen nuevas alarmas de virus	02/01/2008	05/01/2008	3d 2h
7	El Taller inspecciona las máquinas	02/01/2008	04/01/2008	3d
8	Funcionamiento anómalo en estación	05/01/2008	05/01/2008	0d
9	El usuario comunica lo ocurrido	05/01/2008	05/01/2008	1h
10	El Taller recibe el aviso y lo coloca en la lista de espera	05/01/2008	05/01/2008	1h
11	El aviso permanece en lista de espera	05/01/2008	10/01/2008	4d 6h
12	El taller continúa recibiendo avisos, que engrosan la lista de espera	05/01/2008	15/01/2008	9d 6h
13	El Técnico descubre estación no actualizada	10/01/2008	10/01/2008	3h
14	El Técnico comunica al Adm. Segur que realiza comprobaciones	10/01/2008	11/01/2008	5h
15	El Adm. Segur. Estudia el virus.	11/01/2008	11/01/2008	1d
16	El Adm. Segur. Comunica el procedimiento de actuación	12/01/2008	12/01/2008	0d
17	El Técnico recibe instrucciones y procede a la limpieza del virus	12/01/2008	14/01/2008	3d
18	El virus es erradicado	15/01/2008	15/01/2008	0d

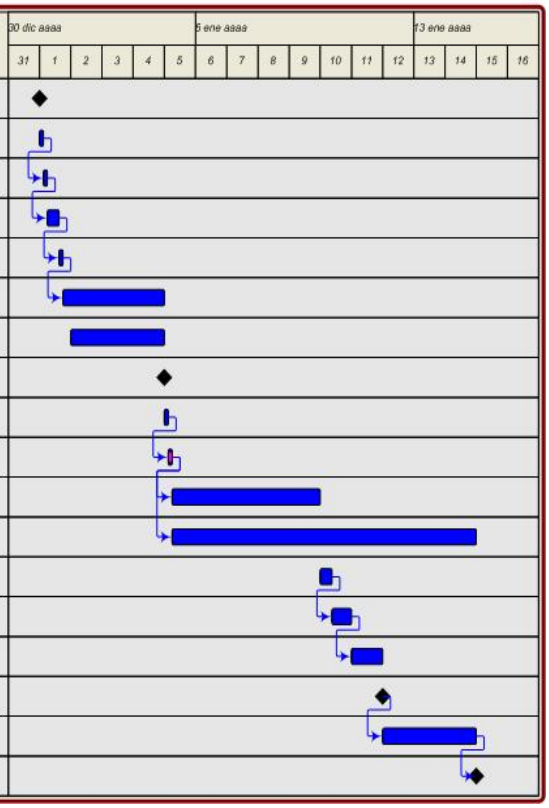


Figura 78.- **Diagrama de GANTT de evolución del virus en una organización sin MISITILEON.**
(Fuente: propia)

[138] Según las técnicas del PSP.

3.2. Escenario 2: Una organización que usa MISITILEON.

Para este segundo escenario se ha considerado una organización que implementa MISITILEON, es decir, donde el proceso que gestiona la Seguridad de la Información está perfectamente integrado en el modelo desplegado por dicha organización para gestionar los servicios TI.

Es importante tener en cuenta que esta integración es completa, se realiza a todos los niveles, desde la definición de la calidad que aporta el servicio hasta el mantenimiento del mismo.

Así, en el caso concreto del servicio antivirus (objeto de esta valoración) se ha considerado que el nivel de dicho servicio se ha definido perfectamente en el ANS[139] entre la empresa suministradora y la propia organización. En esta definición, se habrán concretado las medidas a desarrollar para mantener dicho nivel de calidad, así como los controles que se necesitan para desplegar dichas medidas.

Por otra parte, se habrán definido todos los procedimientos incluidos en cada uno de los procesos que conforman la gestión del sistema. La definición y actualización de dichos procedimientos es fundamental para el buen funcionamiento del proceso de gestión ya que de la exactitud de su cumplimiento depende en gran parte el éxito del proceso global.

[139] Véanse las tablas 11 y 14 del capítulo 4.

Asimismo estarán perfectamente identificadas y definidas las funciones, los roles y las figuras que intervienen en el proceso: CAU, operadores, administradores y gestores de seguridad, técnicos de mantenimiento informático, etc…

Al igual que en el caso anterior, el horario de jornada laboral tomado como referencia es de ocho horas, desde las 8:00 hasta las 16:00 horas.

"Un virus ha afectado a la organización, tenemos un problema".-CASO 2

Seguidamente, se presenta la tabla que describe las tareas (con sus procedimientos asociados) que se producirán con ocasión de la intrusión de un virus en el sistema informático de la organización:

DESCRIPCIÓN DE TAREAS						
Hora Inicio	**Hora Fin**	**Tipo**	**Descripción**	**Tiempo**	**Tiempo Total**	**Tiempo Ganado**
01/01 d 09:00 h	01/01 d 09:00 h	Hito	El software antivirus instalado en una estación de trabajo produce una alarma de posible virus[140].	0	**0**	**0**
01/01 d 09:00 h	01/01 d 09:05 h	Tarea	El usuario lo comunica inmediatamente al CAU y no manipula la máquina, con la consiguiente pérdida de actividad del posible virus[141].	5 min.	**5 min.**	**55 min.**

[140] Según se ha configurado en el apartado de Sistemas de alarmas (A.2.2.3) de Configuración de controles de seguridad (A.2.2).
[141] Según se ha definido en el Procedimiento de comunicación de posible virus, a nivel usuario (B.1.1) del Proceso de recogida de incidentes de seguridad (B.1).

DESCRIPCIÓN DE TAREAS						
Hora Inicio	**Hora Fin**	**Tipo**	**Descripción**	**Tiempo**	**Tiempo Total**	**Tiempo Ganado**
01/01 d 09:05 h	01/01 d 09:15 h	Tarea	El operador del CAU recibe un aviso de virus, lo que le supone una atención inmediata, y se pone en contacto con el usuario para recopilar el máximo de información. El operador consultará (en función de la información recibida) el catálogo de virus[142].	10 min.	**15 min.**	**50 min.** **Total: 1 hora y 45 min.**
--------	--------		Tarea 4 no existe aquí			**3 horas**
01/01 d 09:15 h	01/01 d 10:00 h	Tarea	El operador, en este momento, debe ser capaz de decidir si puede actuar ante el virus o debe escalar el incidente al Administrador de seguridad[143].	45 min.	**1 hora**	**15 min.** **Total: 4 horas 45 min.**
01/01 d 10:00 h	01/01 d 12:00 h	Tarea	Suponiendo que el virus no es conocido (no está en catálogo) y es escalado al administrador de seguridad, éste recibe el incidente con toda la información recopilada por el usuario y hace un estudio de las posibles acciones y soluciones para el virus.	2 horas	**3 horas**	**- 2 horas** **Total: 2 horas 45 min.**
01/01 d 12:00 h	01/01 d 12:00 h	Hito	El Administrador comunica al usuario una actualización del catálogo de posibles virus[144].	1 min.	**3 horas**	**- 1 min.** **Total: 2 horas 44 min.**

[142] Según Procedimiento de discriminación de llamadas de servicio, a nivel operador (B.1.2) del Proceso de recogida de incidentes de seguridad (B.1).
[143] Según Procedimiento de actuación, a nivel operador, ante incidentes de seguridad (B.2.1) del Proceso de gestión de incidentes de seguridad (B.2).
[144] Según Procedimiento de actuación, a nivel administrador, ante incidentes de seguridad (B.2.2) del Proceso de gestión de incidentes de seguridad (B.2).

DESCRIPCIÓN DE TAREAS						
Hora Inicio	**Hora Fin**	**Tipo**	**Descripción**	**Tiempo**	**Tiempo Total**	**Tiempo Ganado**
01/01 d 12:00 h	02/01 d 12:00 h	Tarea	El operador del CAU recibe más avisos de virus, lo que le supone una atención inmediata. Se pone en contacto con los usuarios para recopilar el máximo de información. El operador consultará (en función de la información recibida) el catálogo de virus. Al tratarse del mismo virus, el incidente queda registrado y en espera de que el administrador cree el procedimiento de actuación inmediata.	8 horas	**11 horas**	**21 horas** **Total: 23 horas 44 min.**
01/01 d 12:00 h	02/01 d 12:00 h	Tarea	El Administrador crea un procedimiento de actuación inmediata ante el virus, considerando la posibilidad de máquinas infectadas que no lo hayan detectado, y por lo tanto, los efectos sobre ellas, y lo distribuye entre las personas implicadas[145].	8 horas	**11 horas**	**13 horas** **Total: 36 horas 44 min.**
--------	--------		Tarea 8 no existe aquí			**0**
--------	--------		Tarea 9 no existe aquí			**1 hora**
--------	--------		Tarea 10 no existe aquí			**1 hora**
--------	--------		Tarea 11 no existe aquí			**38 horas**
--------	--------		Tarea 12 no existe aquí			**78 horas**
--------	--------		Tarea 13 no existe aquí			**3 horas**
--------	--------		Tarea 14 no existe aquí			**5 horas**
--------	--------		Tarea 15 no existe aquí			**8 horas**

[145] Según Procedimiento de actuación, a nivel administrador, ante incidentes de seguridad (B.2.2) del Proceso de gestión de incidentes de seguridad (B.2).

DESCRIPCIÓN DE TAREAS						
Hora Inicio	**Hora Fin**	**Tipo**	**Descripción**	**Tiempo**	**Tiempo Total**	**Tiempo Ganado**
02/01 d 12:00 h	05/01 d 12:00 h	Tarea	Dependiendo del número de incidentes recibidos, el problema se remitirá al gestor de problemas de seguridad, que suele ser el propio administrador de seguridad, dándole entidad de problema[146].	24 horas	**35 horas**	**- 24 horas** **Total: 133 horas 44 min.**
02/01 d 12:00 h	02/01 d 12:00 h	Hito	Los operadores, técnicos de informática y otras personas implicadas, reciben el procedimiento de actuación ante el virus, creado por el administrador de seguridad.	11 horas	**46 horas**	**- 11 horas** **Total: 122 horas 44 min.**
02/01 d 12:00 h	05/01 d 12:00 h	Tarea	Los operadores, técnicos de informática y otras personas implicadas, actúan según el procedimiento de actuación y erradican los efectos del virus.	24 horas	**69 horas**	**0**

Tabla 19 .- Descripción de tareas CASO 2.
(Fuente: propia)

Es importante destacar las siguientes consideraciones:

- En este escenario, se han estimado los mismos tiempos que en el supuesto anterior para aquellas acciones que son comunes a ambos casos, es decir, el estudio del virus por parte del administrador de seguridad y las tareas de limpieza del virus en la organización. Se puede decir, con toda seguridad, que el tiempo empleado para la limpieza de las estaciones será menor ya que serán menos las infectadas, al actuar antes contra el virus.

[146] Según Procedimiento de actuación, a nivel administrador de seguridad, ante problemas de seguridad (B.3.1) del Proceso de gestión de problemas de seguridad (B.3).

- Se ha considerado que en la organización no hay máquinas con el sistema antivirus sin actualizar. MISITILEON emplea todos los recursos disponibles para mantener los niveles de calidad de la seguridad acordados. En este caso en la *Definición de los Controles de seguridad (A.2.1), Configuración (A.2.2) y Mantenimiento de dichos controles (A.2.3),* existiendo un completo *Procedimiento de Actualización del sistema antivirus (A.2.3.1)*, que se encarga precisamente de que todo el parque de la organización mantenga el antivirus actualizado.

- En base a esta gestión, MISITILEON, además da la posibilidad de gestionar el problema de forma **proactiva**, que (a diferencia de la forma reactiva) permite detectar el problema antes de que se produzcan incidentes. Para ello, además de definir diversos niveles de protección antivirus (A.2.1), dentro de la *Configuración de los controles de seguridad (A.2.2)*, existe un apartado para definir los *Archivos de registro de detecciones (A.2.2.2)* así como el *Sistema de Alarmas (A.2.2.3)*, con el fin de detectar e informar lo antes posible de la aparición del virus en la organización.

- La gestión de problemas permite ver el problema de forma global y llegar a soluciones genéricas, sin tener que tratar cada máquina individualmente.

- La exacta definición de los procedimientos de actuación, consigue que todas las personas involucradas sepan qué hacer en cada momento. De igual forma, el usuario, una vez detectado el aviso de virus, sabe que debe de dejar de actuar sobre la máquina, desfavoreciendo la expansión del virus.

- Otra de las grandes ventajas de utilizar MISITILEON para la gestión de la seguridad, se produce una vez solucionados los incidentes.

Como continuación o podría decirse, solución del problema de seguridad, en muchos de los casos se producirá una Petición de Cambio. Este cambio tiene como fin solucionar la causa de los incidentes producidos en el sistema.

El administrador de seguridad ha sido la persona que más ha estudiado el incidente de seguridad y las causas de éste, lo que implica que debería de ser parte integrante del GGC, para aportar todos sus conocimientos sobre el tema. *Según el Procedimiento de colaboración del administrador de seguridad ante un cambio (B.4.1).*

A continuación se presentan los resultados de este ejemplo práctico, con los mismos datos que en el apartado anterior: una organización compuesta por 1.000 estaciones de trabajo, un virus con una capacidad de crecimiento[147] o transmisión de 5 equipos a la hora y suponiendo que el virus sólo se transmite con los equipos encendidos, es decir, durante la jornada laboral[148].

Esta vez la organización utiliza MISITILEON, así que dispone de una gestión de servicios que incluye el servicio de seguridad (es decir, gestión del sistema antivirus).

[147] Se ha considerado un crecimiento lineal.
[148] Se ha supuesto que la jornada laboral es e 8 horas (15 días * 8 horas = 120 horas).

EQUIPOS EN LA ORGANIZACIÓN	CRECIMIENTO DEL VIRUS	TIEMPO DE RESPUESTA ANTE EL VIRUS	NÚMERO DE MÁQUINAS INFECTADAS.	% DE LA ORGANIZACIÓN INFECTADA
1000	**5 Equipos/hora**	**35 horas**	**175**	**17,5 %**

Tabla 20 .- Datos de evolución de virus, en una organización con MISITILEON.
(Fuente: propia)

Se muestra una representación, en forma de diagrama de secuencias con escala de tiempos, de la evolución del virus:

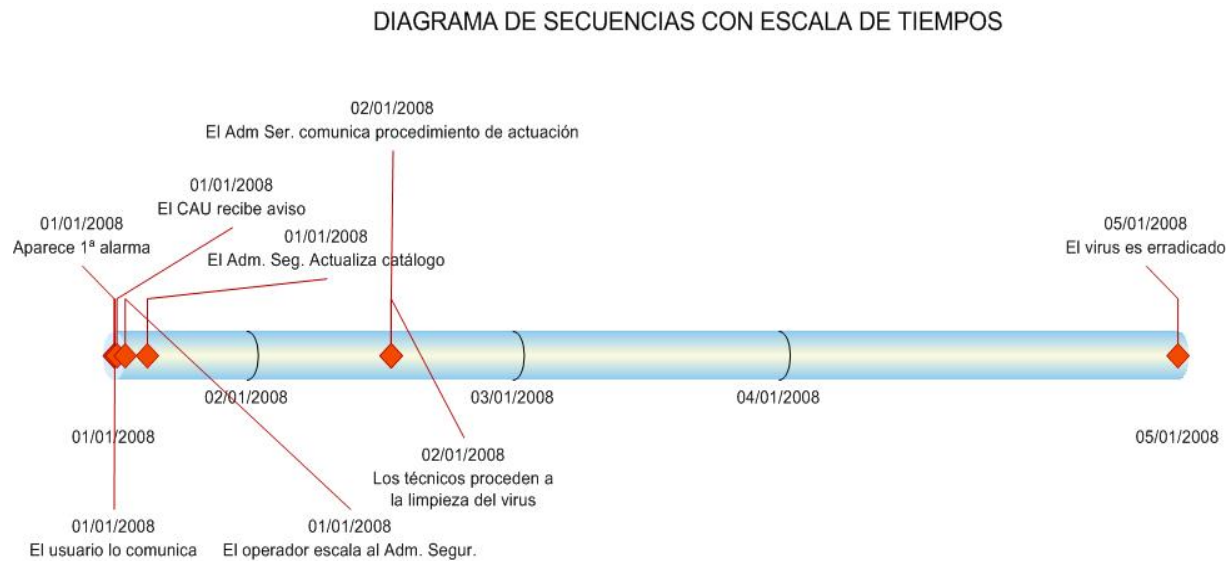


Figura 79.- **Diagrama de secuencias, de evolución del virus, con escala de tiempos, en una organización con MISITILEON.**
(Fuente: propia)

La presentación más detallada y con acumulación de tiempos del diagrama anterior, sería:

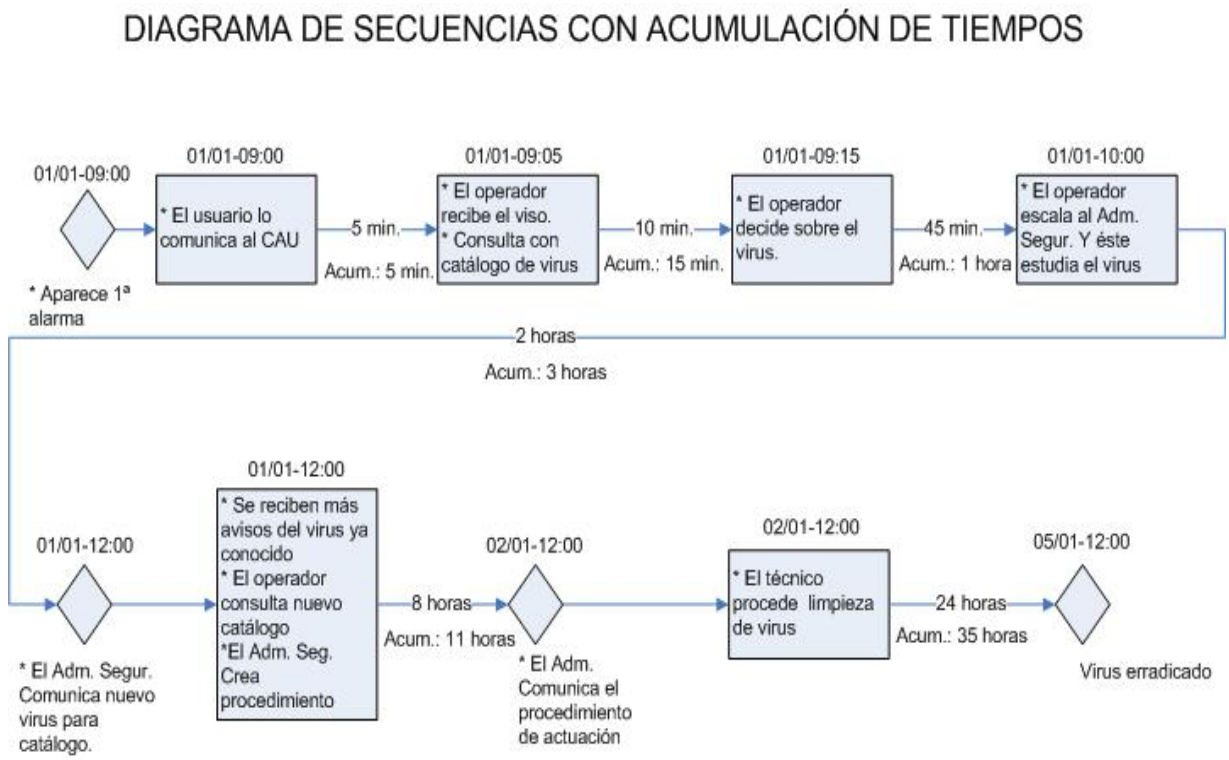


Figura 80.- **Diagrama de secuencias en UML, de la evolución del virus, con acumulación de tiempos, en una organización con MISITILEON.**
(Fuente: propia)

Véase una representación gráfica de la infección en la organización:

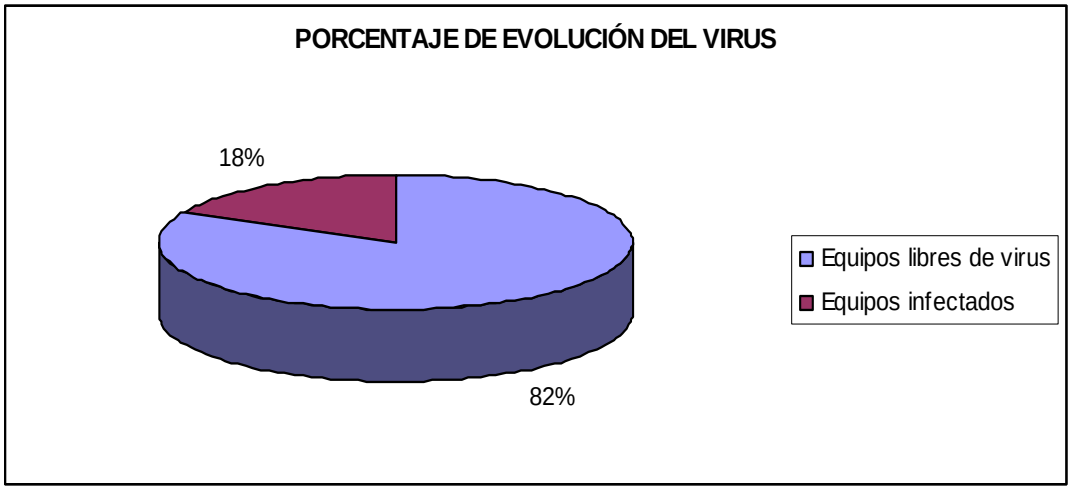


Figura 81.- **Porcentaje de evolución del virus en una organización con MISITILEON.**
(Fuente: propia)

En el siguiente gráfico se utiliza un diagrama de Gantt para presentar la lista de eventos acaecidos en la organización con ocasión de la infección del virus:

DIAGRAMA DE GANTT DE LA EVOLUCIÓN DEL VIRUS EN LA ORGANIZACIÓN

Id.	Nombre de tarea	Comienzo	Fin	Duración
1	Aparece la primera alarma de virus.	01/01/2008	01/01/2008	0d
2	El usuario lo comunica al CAU.	01/01/2008	01/01/2008	,08h
3	El operador recibe aviso y consulta con el catálogo de virus	01/01/2008	01/01/2008	,25h
4	El operador decide sobre el virus	01/01/2008	01/01/2008	,75h
5	El operador escala al Adm. Segur. El incidente y éste estudia el virus.	01/01/2008	01/01/2008	2h
6	El Adm. Segur. Comunica al operador un nuevo virus para el catálogo.	01/01/2008	01/01/2008	0d
7	El operador recibe más avisos de virus y consulta nuevo catálogo.	01/01/2008	02/01/2008	1d
8	El Adm. Segur. Crea un procedimiento de actuación inmediata ante el virus.	01/01/2008	02/01/2008	1d
9	El Adm. Segur. Comunica el procedim. de actuación ante el virus	02/01/2008	02/01/2008	0d
10	Los técnicos recibe el procedimiento de actuación y limpian el virus.	02/01/2008	05/01/2008	3d
11	El virus es erradicado	05/01/2008	05/01/2008	0d

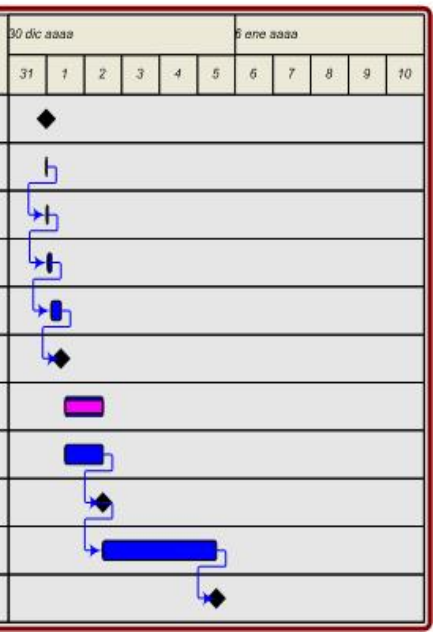


Figura 82.- **Diagrama de GANTT, de evolución del virus, en una organización con MISITILEON.**
(Fuente: propia)

4. Resultados

En este último apartado del capítulo se pueden apreciar las ventajas de emplear la metodología propuesta en esta tesis, frente a no usarla.

Como se puede observar en los diagramas de las figuras 77 y 81, y en las tablas 18 y 20, el porcentaje de equipos infectados es mucho menor empleando MISITILEON que si no se emplea.

Se puede ver la comparativa de la evolución del virus en ambos casos en la figura siguiente:

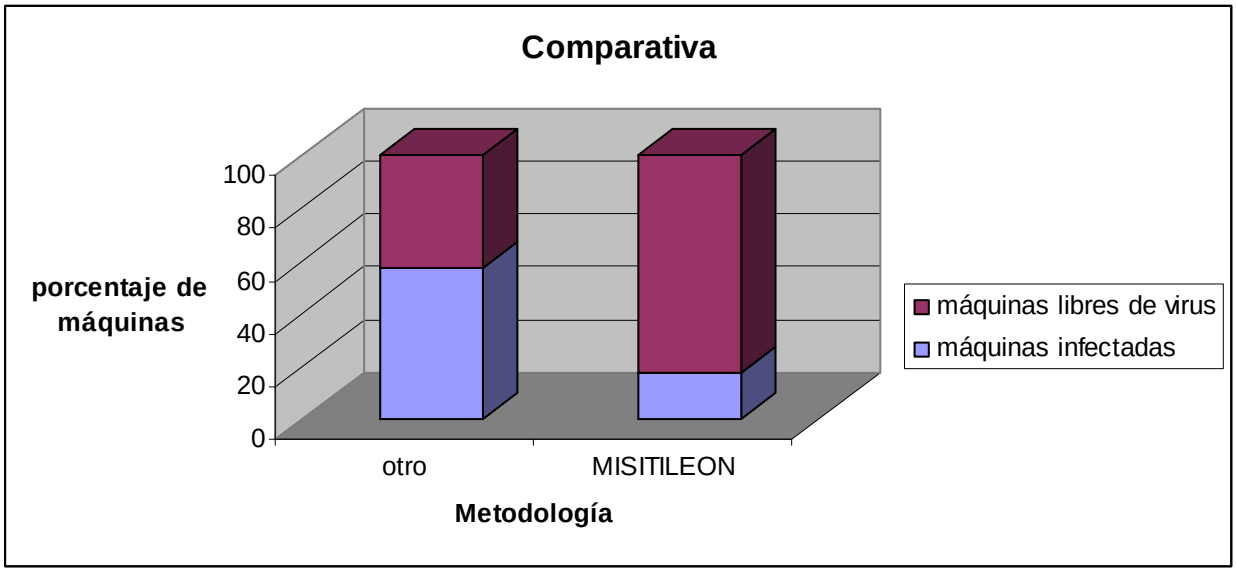


Figura 83.- **Comparativa de la evolución del virus.**
(Fuente: propia)

Como se aprecia en la figura 83 la diferencia en cuanto a porcentaje de máquinas infectadas por el virus es notable. Además, hay que señalar la enorme diferencia de tiempo de reacción ante el ataque de dicho virus, en el caso de no usar MISITILEON se tardarían 115 horas en solucionarlo, mientras que empleando la metodología propuesta sólo serían necesarias 35 horas.

CAPÍTULO VII. SISTEMA DE EVALUACIÓN DE CONOCIMIENTOS MISITILEON.

La práctica es un maestro excepcional[149].

1. Introducción

En este capítulo se presenta la aplicación software realizada a medida para MISITILEON. Esta aplicación será una herramienta muy útil para distintos perfiles de usuario. Por un la do los usuarios "al uso" pueden realizar autoevaluaciones de sus conocimientos en la metodología, aprender con las correcciones y conclusiones propuestas, etc. Por otro lado estará el perfil de administrador, que podrá tener pleno acceso a los contenidos de la aplicación, modificando y actualizando sus contenidos cuando proceda. Además, esta herramienta puede ser útil para posibles auditores que quisieran evaluar el nivel de implantación de la metodología en una determinada organización. También podría servir para estudiantes que quisieran realizar cuestionarios para autoevaluar sus conocimientos, etc.

En el siguiente apartado se muestran las pantallas principales de la aplicación con una breve explicación de cómo usarlas y para que sirven. En el CD que se incluye con esta memoria de tesis doctoral se incluye todo el software necesario para instalar y utilizar la aplicación.

[149] Plinio el Joven (62-113) escritor romano.

2. Tecnología empleada

Para llevar a cabo la implementación de la herramienta de asesoramiento, se ha empleado tecnología basada en software de libre distribución. Para la implementación se ha elegido JAVA.

2.1. Java

Java es un lenguaje de programación con el que se puede realizar cualquier tipo de programa. En la actualidad es un lenguaje muy extendido y cada vez cobra más importancia tanto en el ámbito de Internet como en la informática en general. Está desarrollado por la compañía Sun Microsystems y siempre enfocado a cubrir las necesidades tecnológicas más punteras.

Ya que se ha tomado como premisa que la aplicación fuera independiente de la plataforma de ejecución, se ha elegido JAVA por ser un lenguaje de programación ligero, multiplataforma, de código libre, etc. Además, JAVA se puede considerar como uno de mejores lenguajes de programación, es un lenguaje maduro dotado de fama suficientemente demostrada por los casos de éxito.

2.2. MySQL

La aplicación de MISITILEON emplea una base de datos como repositorio de contenidos. Para la base de datos se ha elegido My-SQL. Las razones de esta elección son las siguientes:

- MySQL software es *Open Source*.
- Velocidad al realizar las operaciones, lo que le hace uno de los gestores con mejor rendimiento.
- Bajo costo en requerimientos para la elaboración de bases de datos, ya que debido a su bajo consumo puede ser ejecutado en una máquina con escasos recursos sin ningún problema.
- Facilidad de configuración e instalación. Soporta gran variedad de Sistemas Operativos.
- Baja probabilidad de corromper datos, incluso si los errores no se producen en el propio gestor, sino en el sistema en el que está.
- Su conectividad, velocidad, y seguridad hacen a MySQL Server altamente apropiado para acceder a bases de datos en Internet.
- El software MySQL usa la licencia GPL[150].

[150] *General Public License*.

2.3. Struts

Para el *framework* de la herramienta MISITILEON, se ha estudiado la implementación del modelo MVC (Modelo-Vista-Controlador) de Struts. Se ha elegido Struts, sobre todo para poder facilitar un mantenimiento posterior de trabajos futuros.

Las ventajas que aporte Struts y que han servido para decantarse por esta implementación de MVC han sido las siguientes:

- La utilización de esta metodología conlleva una serie de ventajas que ayudan a reducir el tiempo requerido para el desarrollo y facilitan el mantenimiento de la aplicación web.
- Transporte automático de los datos introducidos en el cliente (JSP) hasta el controlador (*Action*) mediante formularios (*ActionForm*).
- Transporte automático de los datos enviados por el controlador (*Action*) a la parte de presentación (JSP) mediante formularios (*ActionForm*).
- Implementa lo común a todas las aplicaciones en la parte de Controlador (*ActionServlet*); la parte propia de cada aplicación es fácilmente configurable (struts-config.xml).
- La separación de los componentes en capas (MVC[151]) simplifica notablemente el desarrollo y su mantenimiento.

[151] Modelo Vista Controlador.

3. Manejo del Sistema de Evaluación de Conocimientos MISITILEON

En este apartado se van a describir brevemente las distintas acciones que se pueden llevar a cabo con la aplicación diseñada para la metodología propuesta en esta tesis doctoral. Su manejo, a nivel de usuario, es muy sencillo e intuitivo. En el CD que se anexa junto a esta memoria se encuentra todo lo necesario para instalar y poder hacer uso de esta aplicación.

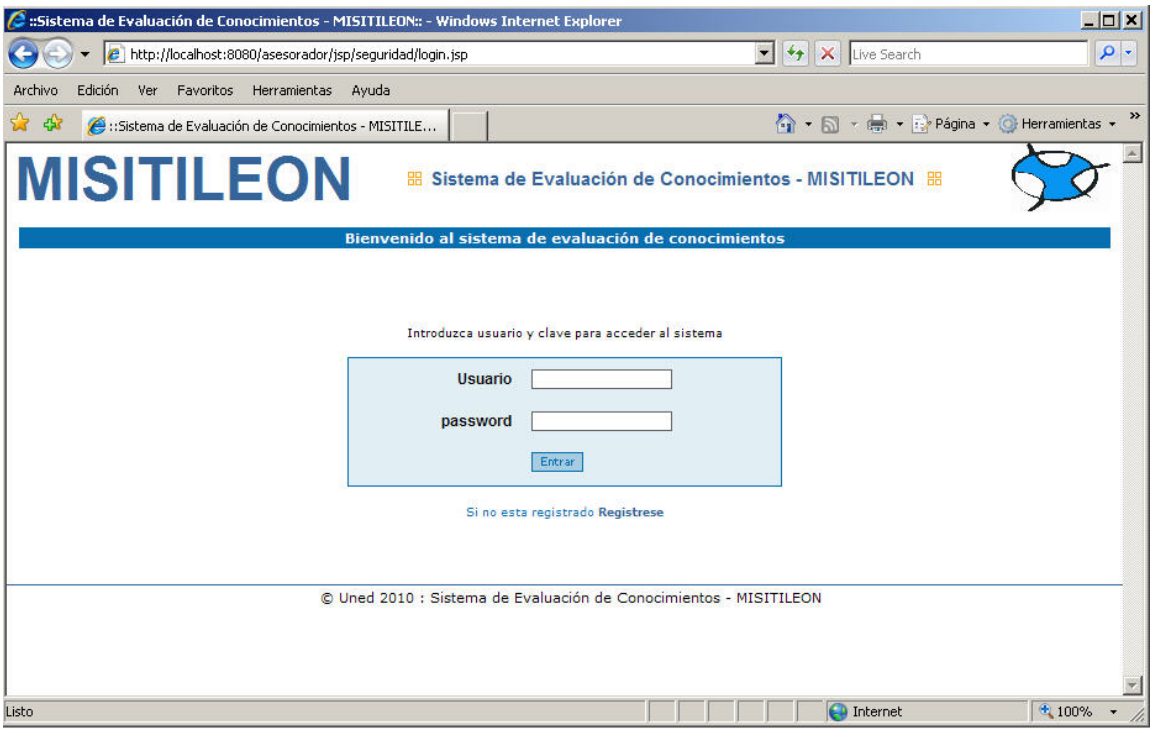


Figura 84.- **Registro.**

Esta es la primera pantalla con la que se encuentra la persona que vaya a hacer uso de la aplicación de MISITILEON: Sistema de Evaluación de Conocimientos. Como se

indica en la línea de instrucciones, el usuario debe identificarse adecuadamente (mediante un nombre de usuario y una clave) para poder acceder a la aplicación.

Si es la primera vez que se va a acceder a la aplicación (y por tanto aún no se dispone de usuario y contraseña) se debe pinchar en la opción "Regístrese" para pasar a la pantalla de "Alta de Usuario", que se explica a continuación.

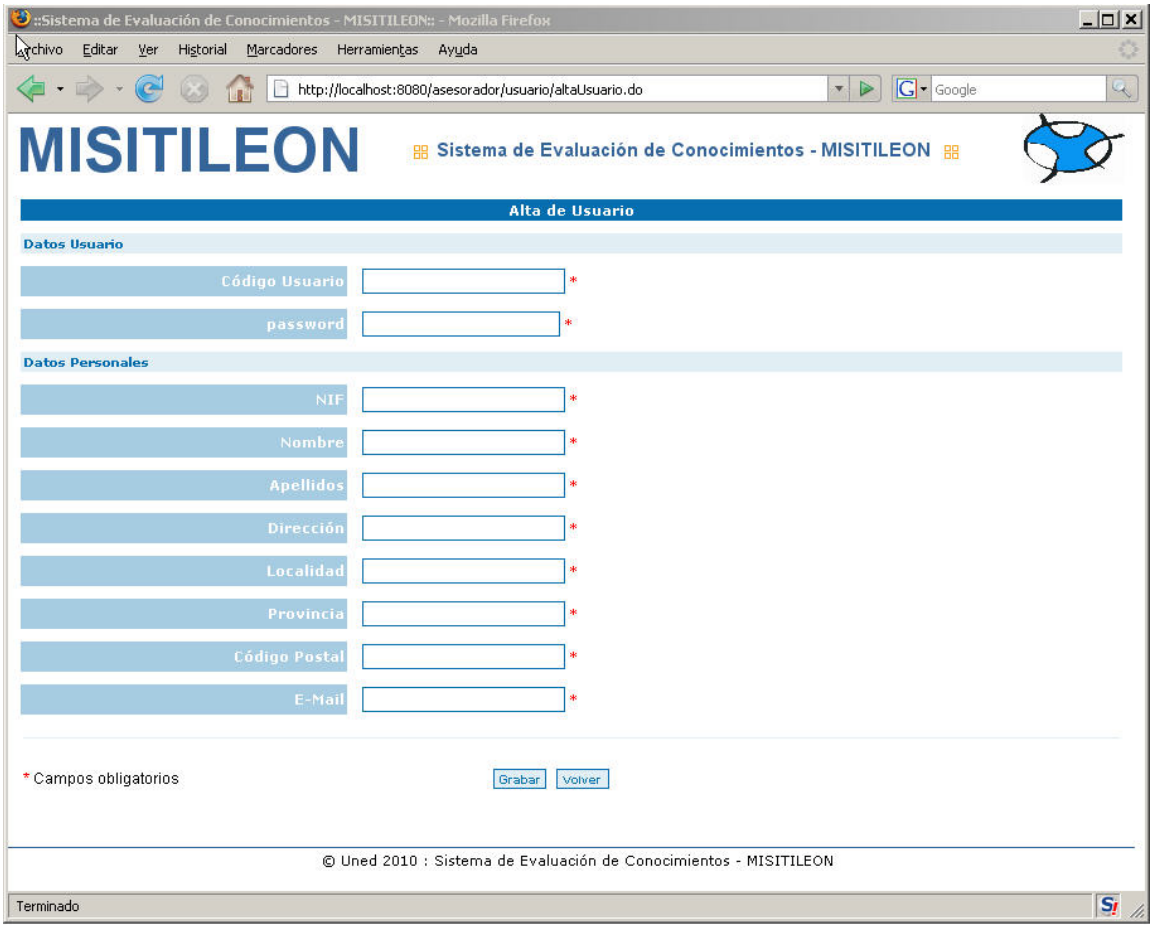


Figura 85.- **Alta usuario.**

La figura 85 muestra el formulario que hay que cumplimentar para dar de alta a un nuevo usuario de la aplicación. Esta tarea la puede realizar el administrador o el propio

usuario, pero en ese caso (como es lógico) nunca podrá darse de alta con perfil de administrador.

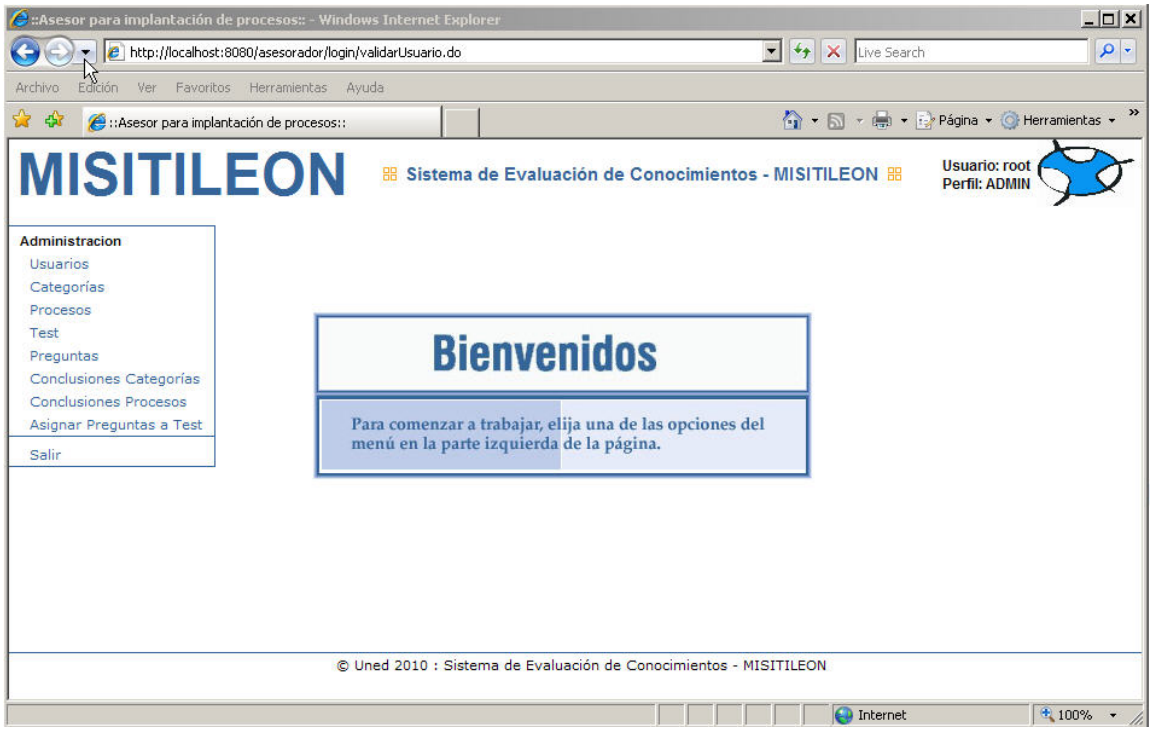


Figura 86.- **Menú.**

Una vez identificado (se puede observar en la parte superior derecha el nombre de usuario y su perfil) el usuario se encuentra con esta pantalla de la figura 86 como menú principal. En ella tiene en la parte izquierda una serie de opciones por las que podrá ir navegando según lo que desee hacer.

El menú de la izquierda será distinto en función de cada perfil. Dependiendo del perfil que tenga la persona que va a utilizar la aplicación (usuario o administrador), podrá realizar unas actividades u otras. En el caso del administrador (dispone de plenos derechos)

podrá además introducir preguntas en los tests, redactar conclusiones, dar de alta a nuevos usuarios, etc.

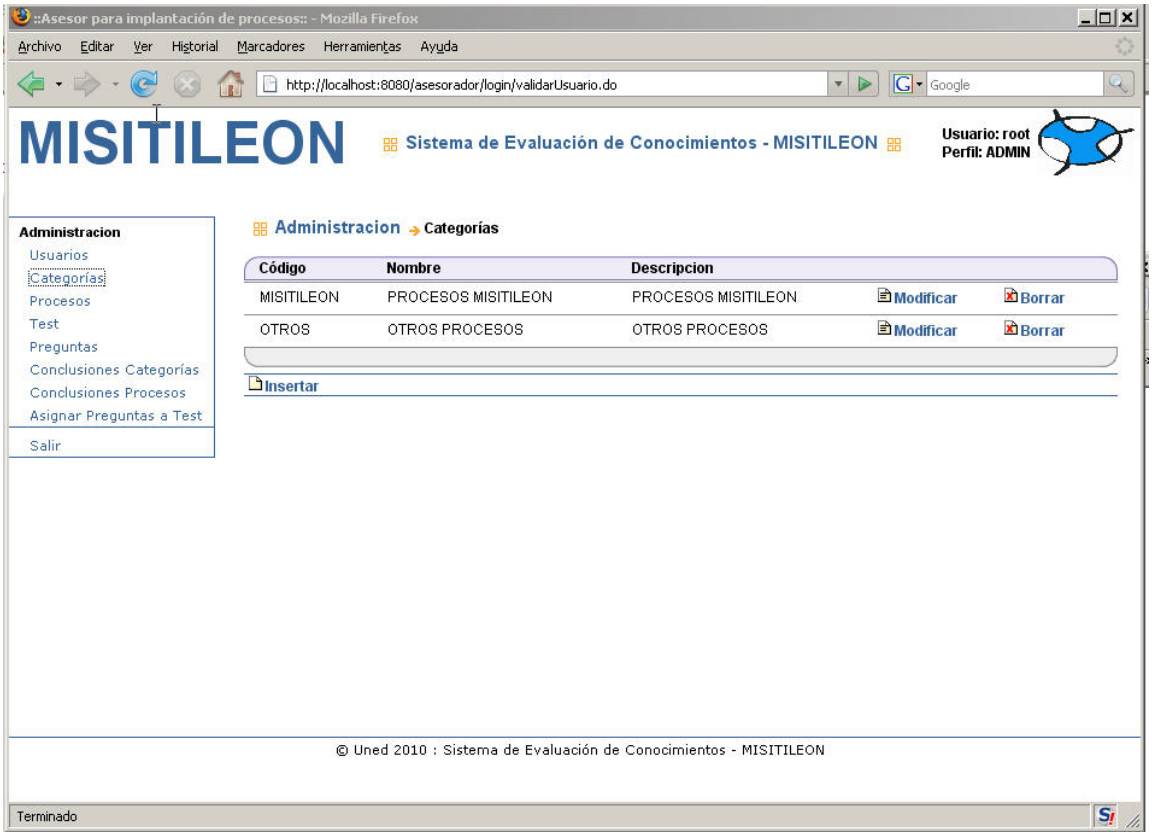


Figura 87.- **Categorías.**

La figura 87 muestra el menú de un usuario con perfil de administrador. Si en el menú de la izquierda se selecciona la opción "Categorías", aparecen en pantalla los grupos generales en los que se engloban todos los tests. Por un lado se pueden realizar tests con preguntas exclusivamente relacionadas con MISITILEON, pero también se pueden realizar tests de otros procesos de ITIL. El usuario ordinario sólo podrá realizar dichos tests, el administrador será el que pueda modificar o borrar estas categorías.

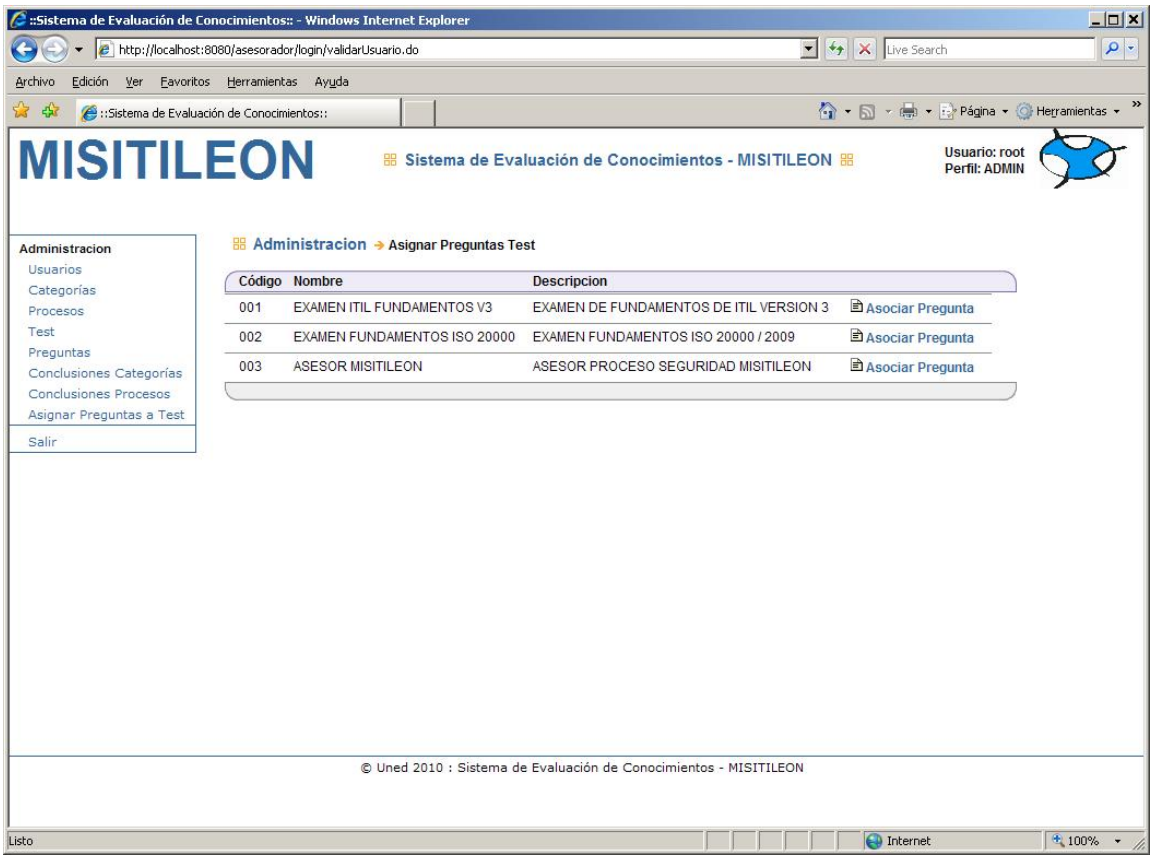


Figura 88.- **Preguntas test.**

Siguiendo con el perfil de administrador (que lógicamente es el más completo) si en el menú de la izquierda se selecciona la opción "Asignar Preguntas a Test", aparecen en pantalla todos los grupos a los que se puede ir añadiendo preguntas de test.

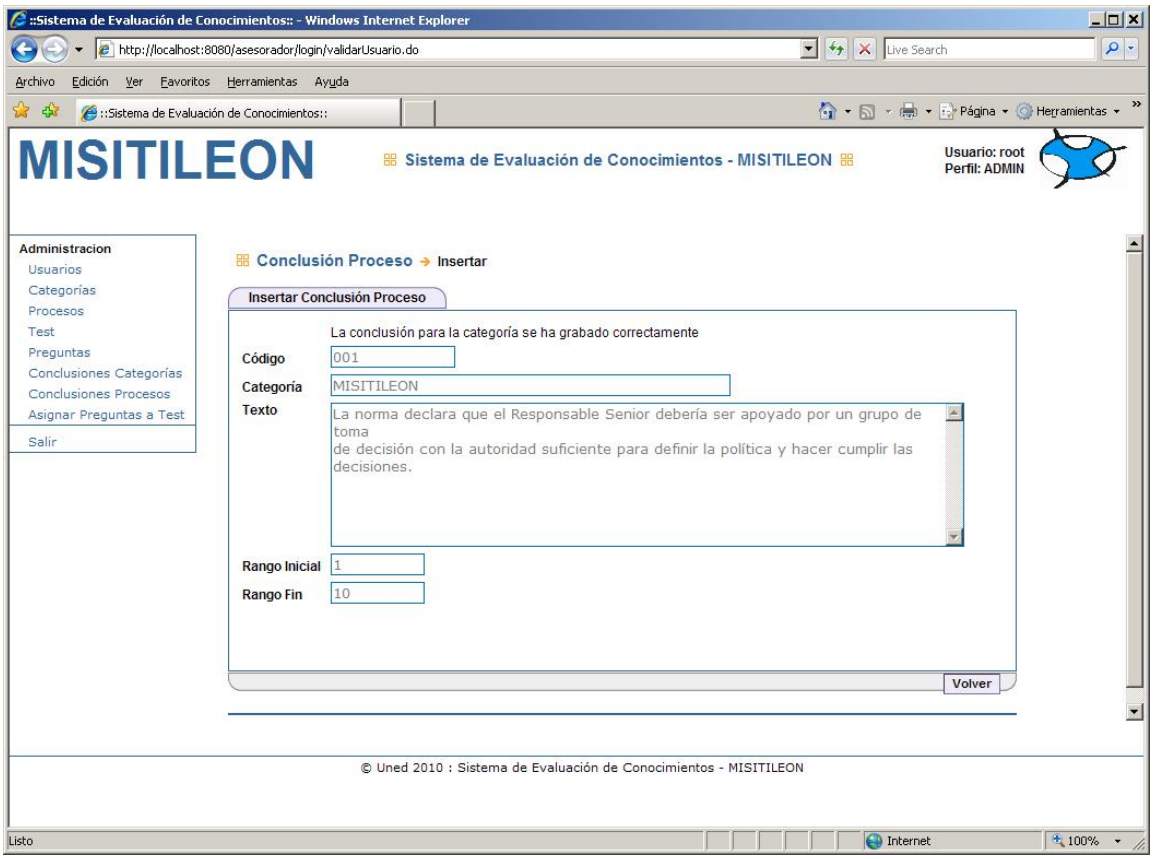


Figura 89.- **Alta conclusiones proceso 1.**

En el menú de la izquierda (siguiendo con el perfil de Administrador) si se selecciona la opción "Conclusiones Procesos", como se puede apreciar en la figura 89, lo que aparece en pantalla es cuadro de texto en el que se pueden escribir una serie de conclusiones que quedarán grabadas para que el usuario pueda aprender con ellas cuando esté utilizando la aplicación.

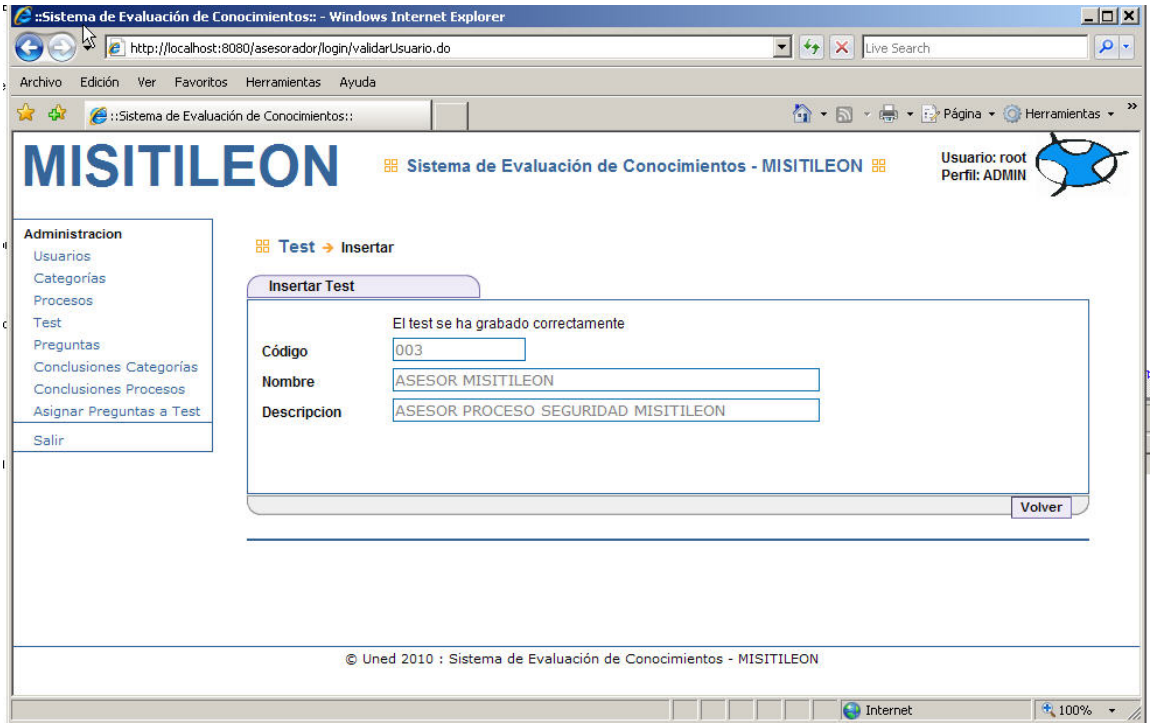


Figura 90.- **Alta test correcta.**

Una vez que se insertan las preguntas de test se puede verificar que dicha acción se ha realizado correctamente gracias al aviso que aparece en la pantalla de la figura 90.

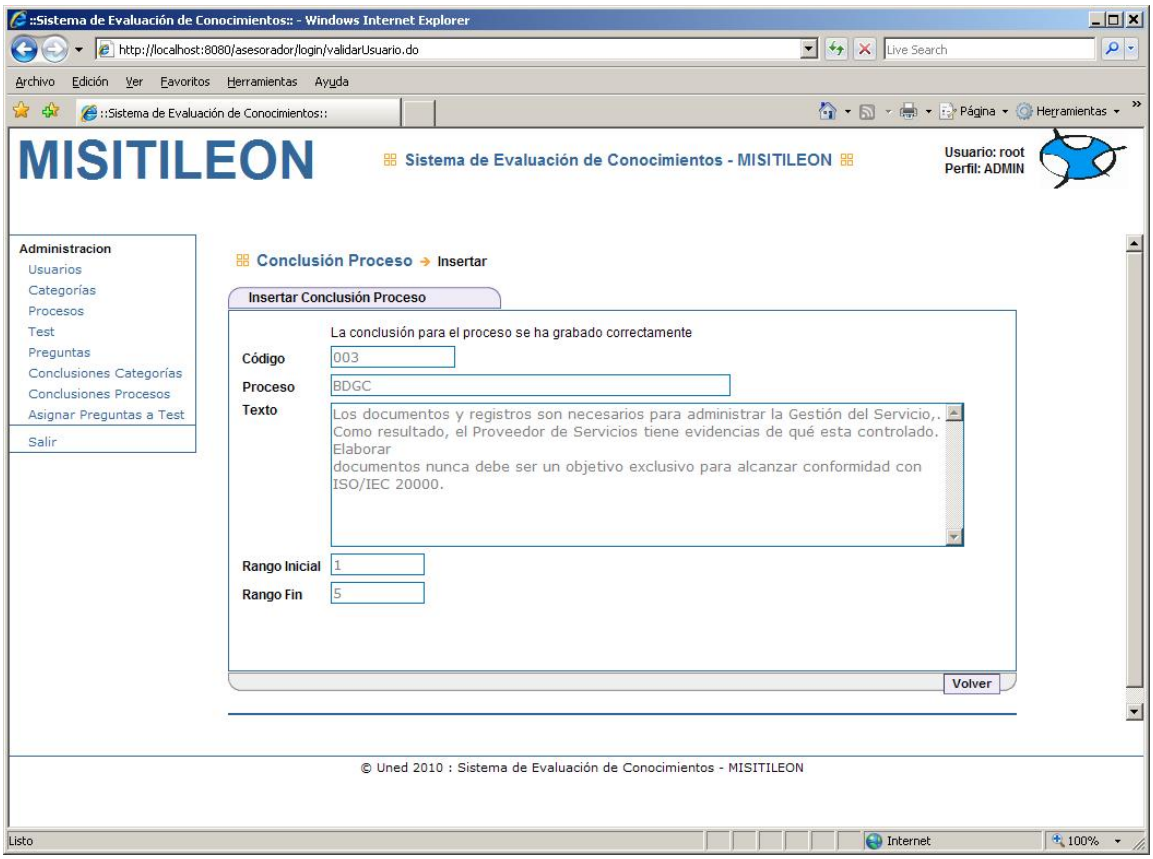


Figura 91.- **Conclusiones proceso 2.**

En la figura 91 se puede ver la pantalla en la que el administrador puede escribir conclusiones, tal como se veía en la figura 89, pero en este caso son conclusiones por proceso y en el caso anterior eran conclusiones por categoría.

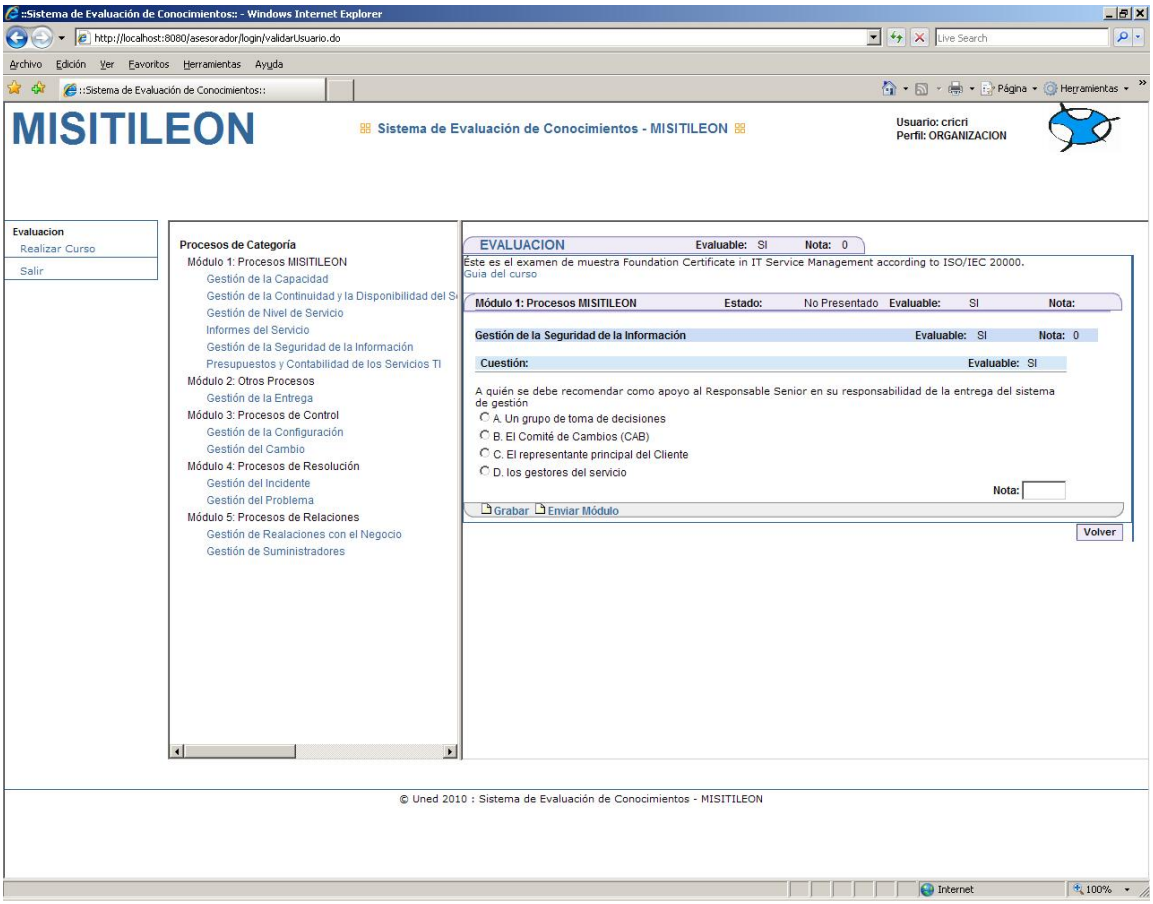


Figura 92.- **Evaluación.**

Esta es la pantalla con la que se encuentra un usuario cuando quiere realizar las preguntas de test. Se puede observar en la figura 92 que hay una pregunta con 4 posibles respuestas y se debe seleccionar sólo una de ellas.

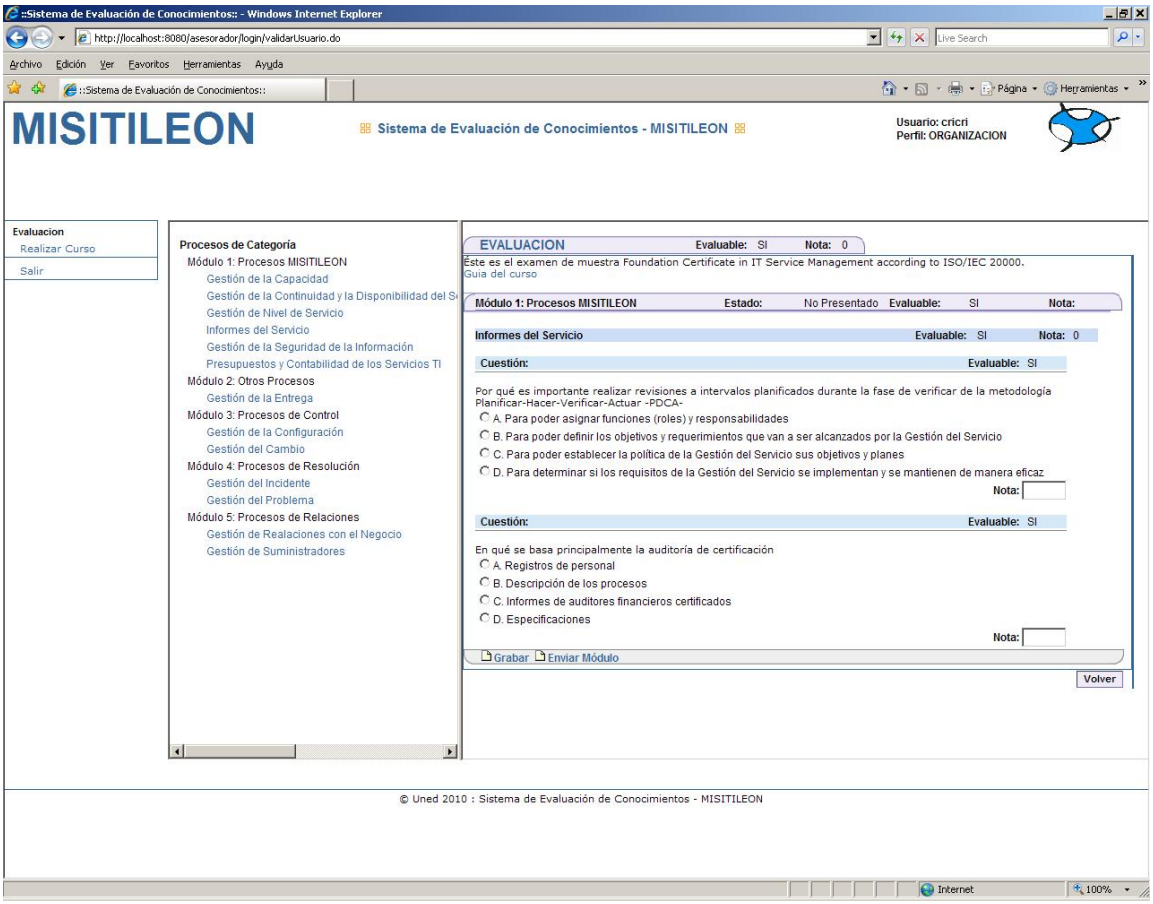


Figura 93.- **Evaluación 1.**

La figura 93 muestra otra pantalla importante con la que se encontrará el usuario.

Para poder utilizar la aplicación (y así conocer el detalle de sus funcionalidades) hay que instalar el software contenido en el CD anexo a esta memoria.

CAPÍTULO VIII. CONCLUSIONES Y LÍNEAS FUTURAS.

En este capítulo se hace una síntesis de los hallazgos realizados en la tesis doctoral y se presentan algunas posibles líneas de investigación futuras, así como una serie de reflexiones finales.

1. Conclusiones de la tesis.

ITIL, teóricamente, fue creado para negocios de todos los tamaños: pequeños, medianos y grandes. Como se ha venido subrayando durante esta memoria de Tesis Doctoral, hoy en día, ITIL no está teniendo la oportunidad que tal vez le corresponde en el Mercado de la Gestión de Servicios, fundamentalmente desechado por ser caro y complicado. MISITILEON es una metodología que pretende cambiar la perspectiva general y ayudar a los gestores y personal de TI a entender el verdadero espíritu de ITIL.

El primer objetivo planteado en el Capítulo 1 de esta memoria ha quedado cubierto, ya que MISITILEON presenta una aproximación mejorada, más práctica y sencilla a ITIL. Este es un modelo de procesos pensado para ser implantado con rapidez y facilidad. Es un modelo reducido en profundidad y no en ámbito, ideal para PYMES o para grandes entidades con alto grado de dispersión y autonomía (colegios, franquicias, pequeños centros de producción o logística, etc). MISITILEON comienza simplificando los procesos y flujos

de trabajo prácticos de ITIL que han servido para la mayoría de los negocios por todo el mundo. Por tanto MISITILEON implementa una solución similar a ITIL en menos tiempo.

El segundo objetivo de la tesis era verificar la idoneidad del modelo propuesto, lo cual ha quedado probado con los datos, tablas y gráficas aportados el Capítulo 6 (Comprobación de la Metodología).

Y el tercer gran objetivo de este trabajo ha quedado cubierto con la aportación práctica: la aplicación Sistema de Evaluación de Conocimientos MISITILEON, que se explica en el Capítulo 7 y que está incluida en el Anexo 5[152].

- ***Beneficios de la Implantación de MISITILEON en las empresas españolas.***

Por la propia estructura empresarial del mercado español y su nivel de evolución en TI, pocas empresas hoy en España han alcanzado un nivel de madurez suficiente, en la gestión de sus servicios tecnológicos, como para poder abordar con éxito un proyecto de esta envergadura sin trastornar seriamente el funcionamiento de todo el resto de la organización.

Estas han sido las razones por las que un importante número de empresas españolas, hoy por hoy, no se plantean la implantación de ITIL, por ser una metodología que se

[152] CD adjunto a esta memoria.

percibe demasiado extensa, sistemática y "burocrática" y cuyos beneficios no alcanzan a identificar.

Con este panorama, la opción de implantar MISITILEON es la solución a los problemas de muchas PYMES. Ya se ha presentado en detalle las mejoras que incorpora dicha metodología, con lo cual los peligros de un enfoque global de ITIL quedarían solventados.

2. Líneas de Investigación Futuras.

Como evidente línea futura de investigación se tiene el primer enfoque de la seguridad en ITIL[153]. Esta era una de las dos opciones lógicas que se plantearon a la hora de decidir integrar mayor seguridad en ITIL. Se seleccionó el segundo enfoque (la seguridad como un servicio más ofrecido por MISITILEON) pero esta otra opción podría ser igualmente interesante. Un pequeño desarrollo de esta posible línea de investigación se encuentra a continuación.

El enfoque tratado en este punto pretende encajar y relacionar los procesos y procedimientos propios de MISITILEON con aquellos "nuevos" que se incluirán en la metodología evolucionada (que se podría llamar MISITILEON II) encargados de proporcionar la debida seguridad al conjunto de la gestión de servicios, es decir, aquellos otros procesos que hacen que los procesos propios de la metodología sean seguros. Estos nuevos procedimientos deberán tratarse como un concepto configurable, adaptable a las posibilidades de infraestructura y a las necesidades de negocio de cada organización.

Seguidamente se presentan algunos ejemplos que detallan y clarifican el enfoque de seguridad que habría que darle a MISITILEON II:

1º.- El CAU, como único punto de contacto con el cliente, estará sometido a procesos de seguridad como: identificación, autenticación, no repudio e integridad.

[153] Propuesto en el apartado 1.4 del capítulo 4 de esta memoria: Dos posibles enfoques para el tratamiento de la Seguridad.

Se observarán los siguientes procedimientos de seguridad:

- Autenticación y no repudio, en el acceso del usuario al CAU para comunicar incidentes.
- Autenticación e identificación, en el acceso del operador al CAU para la Gestión del Incidente.
- Integridad en el almacenamiento y comunicación de incidentes.

2º.- El proceso de Gestión de la Versión de MISITILEON II, debe estar directamente relacionado con funciones propias de la seguridad, como pueden ser el análisis de vulnerabilidades o el cumplimiento en las sucesivas liberaciones de la configuración de los requisitos específicos de Seguridad.

Al igual que en MISITILEON, dentro del marco MISITILEON II, este proceso de Gestión de la Versión se relacionará especialmente con los procesos de Gestión del Cambio y Gestión de la Configuración.

Es importante aclarar que ITIL deja del lado del cliente el análisis de vulnerabilidades, lo que no significa que en esta "ampliación" de seguridad en MISITILEON II no sea conveniente realizar una conexión entre el resultado de esos análisis y los procesos que se vean afectados por ellos.

Continuando con las líneas de investigación futuras, se podrían hacer muchas mejoras y añadir nuevas funcionalidades a la aplicación MISITILEON: Sistema de Evaluación de Conocimientos. En esta tesis se ofrecía esta aplicación como un complemento a la metodología propuesta, pero no era el objetivo principal. Por ello, podría desarrollarse en un futuro una herramienta mucho más completa y potente.

Y para finalizar, no cabe duda de que en poco tiempo la nueva versión de ITIL estará en el mercado internacional, por lo que seguramente se podría mejorar MISITILEON con las novedades y cambios que aporte ITIL Versión 4.

3. Reflexiones Finales.

Desde la más remota antigüedad la acumulación de información ha sido sinónimo de poder, como ya indicaba Sun Tzu en el sigo V a. C, a lo largo del siglo XX los sistemas de tratamiento de la información han evolucionado desde la cinta de papel perforado a las redes de computadores conectados a Internet. El potencial de cálculo de los computadores, en el siglo actual, se duplica cada seis meses y la capacidad de almacenamiento de datos aumenta de forma exponencial. Así mismo se anuncia para la presente década la aparición de nuevas tecnologías de computación (cuántica, óptica, biológica) que permitirán el proceso verdaderamente simultáneo de miles de operaciones semejantes. En este siglo la introducción masiva de los sistemas informáticos en la administración, la defensa, el comercio, la industria, el mundo de los negocios, el ocio, etc, ha significado una revolución en las sociedades más avanzadas[154].

[154] Reflexión de Jesús María Minguet Melián.

BIBLIOGRAFÍA

[AMB07] Ambrojo, J.C. *Las fábricas de software buscan especialización y costes laborales más bajos.* ElPais.com. 2007.

[CAM04] Campbell, J.D. *Interaction in collaborative computer supported diagram development.* Computers in human behaviour. Vol 20, pp. 289-310.

[CAP04] Capell, P. *Benefits of Improvement Efforts.* Special Report CMU/SEI-2004-SR-010.

[COA03] Egozi, Stephenson, Kampman. *WhitePaper: Computer Associates: Formulación de las Mejores Prácticas para Entornos TI Complejos* (2003). Publicado por Computer Associates, Oficina del CTO.

[COM08a] *El Reto de ITIL está en la Administración Pública.* Computer World. Junio 2008.

[COM08b] *Ayudaré a introducir la metodología ITIL en el ámbito formativo.* Computer World. Junio 2008.

[CUE02] Cuevas G. *Gestión del Proceso Software*. Editorial Centro de Estudios Ramón Areces 2002.

[DIA04] Díaz, G. *Seguridad en las comunicaciones y en la información.* UNED 2004.

[DYB05] Dyba, T. *An Empirical Investigation of the Key Factors for Success in Software Process Improvement.* IEEE Transactions os Software Engineering. Vol 31, Nº5, pp 251-264.

[GAF02] Garfinkel, S. *Web security, privacy & commerce.* O´Reilly 2002.

[GAR02] Gartner. *ITIL vs COBIT*, 2002.

[GHO02] Ghosh, S. *Principles of secure network systems design.* Springer 2002.

[GOM08] Gómez J. *Los sinsabores de ITIL v3*. Computerworld. Octubre 2008.

[GON03a] González A. *Guía Rápida Word Office 2003*. Paraninfo.

[GON03b] González A. *Guía Rápida Excel Office 2003*. Paraninfo.

[HUI05] Huidobro, J. *Seguridad en redes y sistemas informáticos.* Thomson 2005.

[ISO04] ISO 13335-1:2004. *Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management.*

[ISO05] ISO/IEC 17799:2005. *Information technology. Security techniques. Code of practice for information security management*.

[ITS07] itSMf 2007 *Fundamentos de Gestión de Servicios TI basados en ITIL*. 2007. ISBN 978987530280.

[ITSV307] Alison Cartlidge, Ashley Hanna, Colin Rudd, Ivor Macfarlane, John Windebank, Stuart Rance *An Introductory Overview of ITIL® V3* Version 1.0., en the IT infrastructure library. (2007). ISBN 0-9551245-8-1.

[ITS08] Bon, J. *Fundamentos de la Gestión de Servicios de TI Basada en ITIL V3*. VHP. 2008.

[JAK02] *Jakarta Struts.* O'Reilly, 2002.

[JAK03] *Jakarta Struts Cookbook.* O'Reilly, 2003.

[LAP92] J. C. Laprie. *Dependability: Basic concepts and terminology*. Springer-Verlag. 1992.

[MAR95] Martín, Q. *La informática como elemento dinamizador de las nuevas tecnologías en la empresa*, en Esic Market. Núm. 88. Abril-Junio. Madrid. ISSN: 0212-1867. 1995.

[MIN03] Minguet, J., Hernández, J. *La calidad el software y su medida*. Editorial Cetro de estudios Ramón Areces 2003.

[MSA05] *Security Administration.* Microsoft Operations Framework (2005), publicado por Microsoft Corporation.

[MSM05] *Security Management*. Microsoft Operations Framework (2005), publicado por Microsoft Corporation.

[NIA06] Niazi M., Wilson D., Zowghi D. *Critical Success Factors for Software Process Improvement Implementation: An empirical study.* Software Process Improvement and practice. Vol 11, 193-211. 2006.

[OGCPRO06] *Provisión de Servicio.* Traducción de Service Delivery (2001), publicado por TSO. ISBN 0-11-330017-4.

[OGCSM99] Cazemier, Overbeek, Peters. *Security Management*, ITIL Managing IT services (1999), publicado por TSO. ISBN 0-11-330014X.

[OGCSOP06] *Soporte de Servicio*. Traducción de Service Support (2000), publicado por TSO. ISBN 0-11-330015-8.

[OLD01] Oldfield, P. *Virus Informáticos al descubierto*, traducido por Javier Acebes, publicado por Sophos plc. 2001.

[OLO92] Tomas Olovsson. *A Structured Approach to Computer Security*. Technical Report 122. Chalmers University of Technology. 1992.

[PFL97] Pfleeger, Charles P., *Security in Computing*, Prentice Hall PTR, 1997.

[PRE05] Pressman R. *Ingeniería del Software. Un enfoque práctico.* McGrawHill 2005.

[RAE01] Real Academia Española. *Diccionario de la Lengua Española.* Vigésima segunda edición. 2001.

[RAE09] Real Academia Española. *Nueva Gramática de la Lengua Española. El español de todo el mundo.* Asociación de Academias de la Lengua Española 2009.

[RUI07] Ruiz E., Cerrada C., Calvo-Manzano J., Arcilla M., *Una Propuesta organizativa de los procesos de SD y SS en ITIL*. Revista REICIS Vol.3, Num. 2. Octubre 2007.

[RUI08] Ruiz E., Arcilla M., Calvo-Manzano J. *A solution for establishing the Information Technology Service Management processes implementation sequence*. Congreso EUROSPI, 2008.

[RUI09b] Ruiz E., Minguet J., Castro M. *Filling the gap of Information Security Management inside ITIL®: proposals for posgraduate students*. Congreso EDUCON Abril 2010.

[RUI00] Ruiz E., Minguet J. *MISITILEON: Propuesta para solucionar las carencias de ITIL® en la Gestión de la Seguridad de la Información*. Congreso 39JAIIO. Argentina 2010.

[SAN09] Sancristobal E., Ruiz E., Castro M. *Integrating and Reusing of Virtual Labs in Open Source LMS*. Congreso EDUCON Abril 2010.

[SED02] SEDISI. *Métricas de la sociedad de la información*. Ministerio de Ciencia y Tecnología. 2002.

[SED03] SEDISI. *Métricas de la sociedad de la información*. Ministerio de Ciencia y Tecnología 2003.

[STA06] Standish Group. *Third Quarter Research Report*. The Standish Group International, Inc., West Yarmouth, M A, 2006.

[SOM04] Sommerville I. *Software Engineering.* Fifth Edition, Addison Wesley.2004.

[STR09] Stroud R. *ITIL es un marco del que tomas las piezas que quieras utilizar y obvias el resto si quieres.* http://www.idg.es/cio/mostrarArticulo.asp?id=193231&seccion=

[TIP00] Tipton, H. *Information security Management.* Auerbach 2000.

[TOR05] Torrente, S. *Modelo de IDS de Ámbito de Nodo Basado en Redes Neuronales*. Tesis Doctoral. UNED 2005.

[VER08] Verdaguer, C. *Implantación secuencial de ITIL en las empresas españolas*. Data.TI Nº 258. Octubre 2008.

[VPCMDB06] David Chiu. *The IT Service Structure: insight gained trough implementing a CMDB.* ViewPoint-CMDB Leadership (2006) publicado por BMC Software Inc.

[WAT97] Watt S. Humphrey. *Introducción al Proceso Software Personal*. Traducido por Javier Zapata Martínez (2001), y publicado por Pearson Education, S.A. con ISBN: 84-7829-052-4.

[WIT00] Withers, D.H. *Software Engineering Best Practices applied to the Modeling Process.* Simulation Conference Proceedings. Winter. Vol Nº1, pp 432-439. ISBN: 0-7803-6579-8. Orlando (USA). 2000.

Referencias WEB

[RefWeb-1] Security Magazine
http://www.secmag.com
Fecha de la última consulta: 6 de mayo de 2006.

[RefWeb-2] AENOR
http://www.aenor.es/desarrollo/inicio/home/home.asp
Fecha de la última consulta: 23 de octubre de 2008.

[RefWeb-3] EXIN
http://www.exin.org/news/~/media/Documents/Publications/ITSMGLOBALBP%20volume1_8%202_Secured%20pdf.ashx
Fecha de la última consulta: 23 de octubre de 2008.

[RefWeb-4] BSI
http://www.bsi-global.com/
Fecha de la última consulta: 23 de octubre de 2008.

[RefWeb-5] itSMF
http://www.itsmfi.org/
Fecha de la última consulta: 10 de abril de 2010.

[RefWeb-6] itSMF España
http://www.itsmf.es/
Fecha de la última consulta: 10 de abril de 2010.

[RefWeb-7] OGC
http://www.ogc.gov.uk/
Fecha de la última consulta: 10 de abril de 2010.

[RefWeb-8] ITIL
http://www.itil.co.uk/
Fecha de la última consulta: 10 de abril de 2010.

[RefWeb-9] CMMi
http://www.sei.cmu.edu/cmmi/general/
Fecha de la última consulta: 6 de enero de 2008.

[RefWeb-10] CoBIT
http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981
Fecha de la última consulta: 16 de enero de 2007.

[RefWeb-11] ISO 20000 Certificaciones
http://www.itlibrary.org/index.php?page=ISO_20000_Certification_Register
Fecha de la última consulta: 6 de enero de 2005.

[RefWeb-12] Certificaciones ITIL v3
http://www.osiatis.es/formacion/Formacion_ITIL_web_V3Bridge.pdf
Fecha de la última consulta: 1 de marzo de 2010.

[RefWeb-13] artículo de la web "la tecla de escape"
http://latecladeescape.com/w0/ingenieria-del-software/metodologias-de-desarrollo-del-software.html#ixzz0dAiCF5Sn
Fecha de la última consulta: 1 de marzo de 2010.

[RefWeb-14] Dimension Data
http://www.dimensiondata.com/es/
Fecha de la última consulta: 2 de marzo de 2010.

[RefWeb-15] ISO 27000
http://www.iso27000.es/
Fecha de la última consulta: 2 de marzo de 2010.

[RefWeb-16] ITIL
http://es.wikipedia.org/wiki/ITIL
Fecha de la última consulta: 2 de marzo de 2010.

[RefWeb-17] The Computer Security Institute
http://www.gocsi.com/
Fecha de la última consulta: 6 de febrero de 2009.

[RefWeb-18] MIS Training Institute
http://www.misti.com/
Fecha de la última consulta: 6 de febrero de 2009.

[RefWeb-19] ISSA: Information Systems Security Associations
http://www.issa.org/
Fecha de la última consulta: 6 de febrero de 2009.

[RefWeb-20] Butler W. Lampson
http://research.microsoft.com/lampson/
Fecha de la última consulta: 6 de enero de 2009.

[RefWeb-21] Virgil D. Gligor
http://www.enee.umd.edu/~gligor/
Fecha de la última consulta: 6 de enero de 2009.

[RefWeb-22] Cyber crime bleeds U.S.coorporations, survey shows
http://www.gocsi.com/press/20020407.html
Fecha de la última consulta: 22 de febrero de 2008.

[RefWeb-23] Guía de Seguridad Informática (SEDISI)
http://www.sedisi.es/05_Estudios/guia01.htm
Fecha de la última consulta: 23 de febrero de 2008.

[RefWeb-24] AETIC
http://www.aetic.es/
Fecha de la última consulta: 12 de enero de 2009.

[RefWeb-25]
http://es.wikipedia.org/wiki/HTTP
Fecha de la última consulta: 13 de enero de 2010.

[RefWeb-26]
http://es.wikipedia.org/wiki/FTP
Fecha de la última consulta: 13 de enero de 2010.

[RefWeb-27]
http://es.wikipedia.org/wiki/POP3
Fecha de la última consulta: 13 de enero de 2010.

[RefWeb-28]
http://es.wikipedia.org/wiki/POP4
Fecha de la última consulta: 15 de abril de 2010.

[RefWeb-29]
http://es.wikipedia.org/wiki/SMTP
Fecha de la última consulta: 6 de mayo de 2010.

[RefWeb-30]
http://es.wikipedia.org/wiki/ISO/IMAP

Fecha de la última consulta: 13 de enero de 2010.

[RefWeb-31]

http://www.cafeonline.com.mx/virus/tipos-virus.html

Fecha de la última consulta: 6 de mayo de 2010.

[RefWeb-32]

http://www.isp2002.co.cl/

Fecha de la última consulta: 10 de abril de 2010.

[RefWeb-33]

http://www.itsmf.es/index.php?option=com_content&view=article&id=45&Itemid=189

Fecha de la última consulta: 6 de mayo de 2010.

ANEXOS

ANEXO 1. Metodologías.

CMMi

Áreas de proceso

El modelo CMMI v1.2 (CMMI-DEV) contiene las siguientes 22 áreas de proceso:

- Análisis de Causas y Resolución (CAR)
- Gestión de la Configuración (CM)
- Análisis de Decisiones y Resolución (DAR)
- Gestión Integrada de Proyectos (IPM)
- Medición y Análisis (MA)
- Innovación y Despliegue Organizacionales (OID)
- Definición de Procesos Organizacionales (OPD)
- Enfoque Organizacional en Procesos (OPF)
- Rendimiento de Procesos Organizacionales (OPP)
- Formación Organizacional (OT)
- Monitorización y Control de Proyecto (PMC)
- Planificación de Proyecto (PP)
- Aseguramiento de Calidad de Procesos y Productos (PPQA)
- Integración de Producto (PI)
- Gestión Cuantitativa de Proyectos (QPM)
- Gestión de Requerimientos (REQM)
- Desarrollo de Requerimientos (RD)

- Gestión de Riesgos (RSKM)
- Gestión de Acuerdos con Proveedores (SAM)
- Solución Técnica (TS)
- Validación (VAL)
- Verificación (VER)

Historia

CMMi es el sucesor de CMM. CMM fue desarrollado desde 1987 hasta 1997. En 2002, se lanzó CMMi Versión 1.1, luego en Agosto de 2006 siguió la versión 1.2. El objetivo del proyecto CMMi es mejorar la usabilidad de modelos de madurez integrando varios modelos diferentes en un solo marco (*framework*). Fue creado por miembros de la industria, el gobierno y el SEI[155]. Entre los principales patrocinadores se incluyen la Oficina del Secretario de Defensa (OSD) y la National Defense Industrial Association.

Dos representaciones: Representación Continua (*Continuous Representation*) y Escalonada (*Staged Representation*)

El modelo para software (CMM-SW) establece 5 Niveles de Madurez (*Maturity Level*) para clasificar a las organizaciones, en función de qué áreas de procesos consiguen sus objetivos y se gestionan con principios de ingeniería. Es lo que se denomina un *modelo escalonado*, o centrado en la madurez de la organización. La selección de las Áreas de

[155] SEI, *Software Engineering Insttitute*.

Proceso (PAs[156]) está prefijada, habiendo 7 PAs para el nivel de madurez 2 (ML[157]2), 11 para el ML3, 2 para el ML4 y 2 más para el ML5.

El modelo para ingeniería de sistemas (SE-CMM) establece 6 Niveles de Capacidad posibles para cada una de las 22 áreas de proceso implicadas en la ingeniería de sistemas. La organización puede decidir cuáles son las PAs que quiere mejorar determinando así su perfil de capacidad.

En el equipo de desarrollo de CMMi había defensores de ambos tipos de representaciones. El resultado fue la publicación del modelo con dos representaciones: continua y escalonada. No son equivalentes, y cada organización puede optar por adoptar la que se adapte a sus características y prioridades de mejora. Sí existe una "*stagging*" equivalente que nos dice que un Nivel de Madurez equivale a tener en un conjunto de PA determinado un determinado Nivel de Capacidad.

La visión continua de una organización mostrará la representación de nivel de capacidad de cada una de las áreas de proceso del modelo.

La visión escalonada definirá a la organización dándole en su conjunto un nivel de madurez del 1 al 5.

[156] PA, *Process Area*.
[157] ML, *Maturity Level*.

Niveles de capacidad de los procesos (representación continua)

Los 6 niveles definidos en CMMi para medir la capacidad de los procesos son:

- 0.- **Incompleto**: El proceso no se realiza, o no se consiguen sus objetivos.
- 1.- **Ejecutado**: El proceso se ejecuta y se logra su objetivo.
- 2.- **Gestionado**: Además de ejecutarse, el proceso se planifica, se revisa y se evalúa para comprobar que cumple los requisitos.
- 3.- **Definido**: Además de ser un proceso gestionado se ajusta a la política de procesos que existe en la organización, alineada con las directivas de la empresa.
- 4.- **Cuantitativamente gestionado**: Además de ser un proceso definido se controla utilizando técnicas cuantitativas.
- 5.- **Optimizando**: Además de ser un proceso cuantitativamente gestionado, de forma sistemática se revisa y modifica o cambia para adaptarlo a los objetivos del negocio. Mejora continua.

Componentes

Área de proceso: Conjunto de prácticas relacionadas que son ejecutadas de forma conjunta para conseguir un conjunto de objetivos.

♦ Componentes Requeridos

- **Objetivo genérico**: Los objetivos genéricos asociados a un nivel de capacidad establecen lo que una organización debe alcanzar en ese nivel de capacidad.

El logro de cada uno de esos objetivos en un área de proceso significa mejorar el control en la ejecución del área de proceso.

- **Objetivo específico**: Los objetivos específicos se aplican a una única área de proceso y localizan las particularidades que describen qué se debe implementar para satisfacer el propósito del área de proceso.

♦ Componentes Esperados

- **Práctica genérica**: Una práctica genérica se aplica a cualquier área de proceso porque puede mejorar el funcionamiento y el control de cualquier proceso.

- **Práctica específica**: Una práctica específica es una actividad que se considera importante en la realización del objetivo específico al cual está asociado.

Las prácticas específicas describen las actividades esperadas para lograr la meta específica de un área de proceso.

♦ Componentes Informativos

- Propósito
- Notas introductorias

- Nombres
- Tablas de relaciones práctica - objetivo
- Prácticas
- Productos típicos
- Sub-prácticas. Una sub-práctica es una descripción detallada que sirve como guía para la interpretación de una práctica genérica o específica.
- Ampliaciones de disciplina. Las ampliaciones contienen información relevante de una disciplina particular y relacionada con una práctica específica.
- Elaboraciones de prácticas genéricas. Una elaboración de una práctica genérica es una guía de cómo la práctica genérica debe aplicarse al área de proceso.

Evaluación (*Appraisal*)

Muchas organizaciones valoran el medir su progreso llevando a cabo una evaluación (*appraisal*) y ganando una clasificación del nivel de madurez o de un nivel de capacidad de logro. Este tipo de evaluaciones son realizadas normalmente por una o más de las siguientes razones:

- Para determinar cómo se comparan los procesos de la organización con las mejores prácticas CMMi y determinar qué mejoras se pueden hacer.
- Para informar a los clientes externos y proveedores acerca de cómo se comparan los procesos de la organización con las mejores prácticas CMMi.
- Para cumplir los requisitos contractuales de uno o más clientes.

Las valoraciones de las organizaciones utilizando un modelo CMMi deben ajustarse a los requisitos definidos en el documento *Appraisal Requirements for CMMi* (ARC). La evaluación se enfoca en identificar oportunidades de mejora, y comparar los procesos de la organización con las mejores prácticas CMMi. Los equipos de evaluación usan el modelo CMMi y un método conforme a ARC para guiar su evaluación y reporte de conclusiones. Los resultados de la evaluación son usados para planificar mejoras en la organización. Hay tres clases de evaluación (Clase A, B y C). El SCAMPI es un Método de evaluación que cumple todos los requerimientos ARC. Una evaluación de clase A es más formal y es la única que puede resultar en una clasificación de nivel.

SCAMPI: Standard CMMI Appraisal Method for Process Improvement

El *Standard CMMi Appraisal Method for Process Improvement* (SCAMPI) es el método oficial del SEI para proveer puntos de referencia de sistemas de calificación en relación con los modelos CMMi. SCAMPI se usa para identificar fortalezas y debilidades de los procesos, revelar riesgos de desarrollo/adquisición, y determinar niveles de capacidad y madurez. Se utiliza ya sea como parte de un proceso o programa de mejora, o para la calificación de posibles proveedores. El método define el proceso de evaluación constando de preparación; las actividades sobre el terreno; observaciones preliminares, conclusiones y valoraciones; presentación de informes y actividades de seguimiento.

COBIT

PLANIFICAR Y ORGANIZAR (PO)

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI pueda contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada. Este dominio cubre los siguientes cuestionamientos típicos de la gerencia:

- ¿Están alineadas las estrategias de TI y del negocio?
- ¿La empresa está alcanzando un uso óptimo de sus recursos?
- ¿Entienden todas las personas dentro de la organización los objetivos de TI?
- ¿Se entienden y administran los riesgos de TI?
- ¿Es apropiada la calidad de los sistemas de TI para las necesidades del negocio?

ADQUIRIR E IMPLEMENTAR (AI)

Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como la implementación e integración en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio. Este dominio, por lo general, cubre los siguientes cuestionamientos de la gerencia:

• ¿Los nuevos proyectos generan soluciones que satisfagan las necesidades del negocio?

• ¿Los nuevos proyectos son entregados a tiempo y dentro del presupuesto?

• ¿Trabajarán adecuadamente los nuevos sistemas una vez sean implementados?

• ¿Los cambios afectarán las operaciones actuales del negocio?

ENTREGAR Y DAR SOPORTE (DS)

Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales. Por lo general aclara las siguientes preguntas de la gerencia:

• ¿Se están entregando los servicios de TI de acuerdo con las prioridades del negocio?

• ¿Están optimizados los costes de TI?

• ¿Es capaz la fuerza de trabajo de utilizar los sistemas de TI de manera productiva y segura?

• ¿Están implantadas de forma adecuada la confidencialidad, la integridad y la disponibilidad?

MONITORIZAR Y EVALUAR (ME)

Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitorización del control interno, el cumplimiento regulatorio y la aplicación del gobierno. Por lo general abarca las siguientes preguntas de la gerencia:

• ¿Se mide el desempeño de TI para detectar los problemas antes de que sea demasiado tarde?

• ¿La Gerencia garantiza que los controles internos son efectivos y eficientes?

• ¿Puede vincularse el desempeño de lo que TI ha realizado con las metas del negocio?

• ¿Se miden y reportan los riesgos, el control, el cumplimiento y el desempeño?

LOS PROCESOS REQUIEREN CONTROLES

Control se define como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad razonable que los objetivos de negocio se alcanzarán, y los eventos no deseados serán prevenidos o detectados y corregidos. Un objetivo de control de TI es una declaración del resultado o fin que se desea lograr al implantar procedimientos de control en una actividad de TI en particular. Los objetivos de control de COBIT son los requerimientos mínimos para un control efectivo de cada proceso de TI.

La guía se puede obtener del modelo de control estándar. Sigue los principios que se evidencian en la siguiente analogía: cuando se ajusta la temperatura ambiente (estándar) para el sistema de calefacción (proceso), el sistema verificará de forma constante (comparar) la temperatura ambiente (inf. de control) e indicará (actuar) al sistema de calefacción para que genere más o menos calor.

La gerencia operacional usa los procesos para organizar y administrar las actividades de TI en curso. COBIT brinda un modelo genérico de procesos 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 operacional de TI y para la gerencia administrativa. Para lograr un gobierno efectivo, los gerentes operacionales deben implementar los controles necesarios dentro de un marco de control definido para todos los procesos TI. Ya que los objetivos de control de TI de COBIT están organizados por procesos de TI, el marco de trabajo brinda vínculos claros entre los requerimientos de gobierno de TI, los procesos de TI y los controles de TI. Cada uno de los procesos de TI de COBIT tiene un objetivo de control de alto nivel y un número de objetivos de control detallados. Como un todo, representan las características de un proceso bien administrado. Los objetivos de control detallados se identifican por dos caracteres que representan el dominio más un número de proceso y un número de objetivo de control. Además de los objetivos de control detallados, cada proceso COBIT tiene requerimientos de control genéricos que se identifican con PCn, que significa número de control de proceso. Se deben tomar como un todo junto con los objetivos de control del proceso para tener una visión completa de los requerimientos de control.

PC1 Dueño del proceso

Asignar un dueño para cada proceso COBIT de tal manera que la responsabilidad sea clara.

PC2 Reiterativo

Definir cada proceso COBIT de tal forma que sea repetitivo.

PC3 Metas y objetivos

Establecer metas y objetivos claros para cada proceso COBIT para una ejecución efectiva.

PC4 Roles y responsabilidades

Definir roles, actividades y responsabilidades claros en cada proceso COBIT para una ejecución eficiente.

PC5 Desempeño del proceso

Medir el desempeño de cada proceso COBIT en comparación con sus metas.

PC6 Políticas, planes y procedimientos

Documentar, revisar, actualizar, formalizar y comunicar a todas las partes involucradas cualquier política, plan ó procedimiento que impulse un proceso COBIT. Los controles efectivos reducen el riesgo, aumentan la probabilidad de la entrega de valor y aumentan la eficiencia debido a que habrá menos errores y un enfoque administrativo más

consistente. Además, COBIT ofrece ejemplos ilustrativos para cada proceso, los cuales no son exhaustivos o anticuados / caducos, de:

• Entradas y salidas genéricas
• Actividades y guías sobre roles y responsabilidades en una gráfica RACI
• Metas de actividades clave (las cosas más importantes a realizar)
• Métricas.

Además de evaluar qué controles son requeridos, los propietarios de procesos deben entender qué entradas requieren de otros procesos y que requieren otros de sus procesos. COBIT brinda ejemplos genéricos de las entradas y salidas clave para cada proceso incluyendo los requerimientos externos de TI. Existen algunas salidas que son entradas a todos los demás procesos, marcadas como _TODOS‘ en las tablas de salidas, pero no se mencionan como entradas en todos los procesos, y por lo general incluyen estándares de calidad y requerimientos de métricas, el marco de trabajo de procesos de TI, roles y responsabilidades documentados, el marco de control empresarial de TI, las políticas de TI, y roles y responsabilidades del personal. El entendimiento de los roles y responsabilidades para cada proceso es clave para un gobierno efectivo. COBIT proporciona una gráfica RACI (quién es responsable, quién rinde cuentas, quién es consultado y quien informado) para cada proceso. Rendir cuentas significa: “la responsabilidad termina aquí”, ésta es la persona que provee autorización y direccionamiento a una actividad. Responsabilidad se refiere a la persona que realiza la actividad. Los otros dos roles (consultado e informado) garantizan que todas las personas que son requeridas están involucradas y dan soporte al proceso.

CONTROLES DEL NEGOCIO Y CONTROLES DE TI

El sistema empresarial de controles internos impacta a TI en tres niveles:

• Al nivel de dirección ejecutiva, se fijan los objetivos de negocio, se establecen políticas y se toman decisiones de cómo aplicar y administrar los recursos empresariales para ejecutar la estrategia de la compañía. El enfoque genérico hacia el gobierno y el control se establece por parte del consejo y se comunica a todo lo largo de la empresa. El ambiente de control de TI es guiado por este conjunto de objetivos y políticas de alto nivel.

• Al nivel de procesos de negocio, se aplican controles para actividades específicas del negocio. La mayoría de los procesos de negocio están automatizados e integrados con los sistemas aplicativos de TI, dando como resultado que muchos de los controles a este nivel estén automatizados. Estos se conocen como controles de las aplicaciones. Sin embargo, algunos controles dentro del proceso de negocios permanecen como procedimientos manuales, como la autorización de transacciones, la separación de funciones y las conciliaciones manuales. Los controles al nivel de procesos de negocio son, por lo tanto, una combinación de controles manuales operados por el negocio, controles de negocio y controles de aplicación automatizados. Ambos son responsabilidad del negocio en cuanto a su definición y administración aunque los controles de aplicación requieren que la función de TI dé soporte a su diseño y desarrollo.

• Para soportar los procesos de negocio, TI proporciona servicios, por lo general de forma compartida, por varios procesos de negocio, así como procesos operacionales y de

desarrollo de TI que se proporcionan a toda la empresa, y mucha de la infraestructura de TI provee un servicio común (es decir, redes, bases de datos, sistemas operativos y almacenamiento). Los controles aplicados a todas las actividades de servicio de TI se conocen como controles generales de TI. La operación formal de estos controles generales es necesaria para que dé confiabilidad a los controles en aplicación. Por ejemplo, una deficiente administración de cambios podría poner en riesgo (por accidente o de forma deliberada) la confiabilidad de los chequeos automáticos de integridad.

CONTROLES GENERALES DE TI Y CONTROLES DE APLICACIÓN

Los controles generales son aquellos que están incrustados en los procesos y servicios de TI. Algunos ejemplos son:

- Desarrollo de sistemas
- Administración de cambios
- Seguridad

Los controles incluidos en las aplicaciones del proceso de negocios se conocen por lo general como controles de aplicación. Ejemplos:

- Integridad (Completitud)
- Precisión
- Validez
- Autorización

• Segregación de funciones

COBIT asume que el diseño e implementación de los controles de aplicación automatizados son responsabilidad de TI, y están cubiertos en el dominio de Adquirir e Implementar, con base en los requerimientos de negocio definidos, usando los criterios de información de COBIT. La responsabilidad operacional de administrar y controlar los controles de aplicación no es de TI, sino del propietario del proceso de negocio. TI entrega y da soporte a los servicios de las aplicaciones y a las bases de datos e infraestructura de soporte. Por lo tanto, los procesos de TI de COBIT abarcan a los controles generales de TI, pero no los controles de las aplicaciones, debido a que son responsabilidad de los dueños de los procesos del negocio, y como se describió anteriormente, están integrados en los procesos de negocio. La siguiente lista ofrece un conjunto recomendado de objetivos de control de las aplicaciones identificados por ACn, número de Control de Aplicación (por sus siglas en inglés):

Controles de origen de datos/ autorización

AC1 Procedimientos de preparación de datos

Los departamentos usuarios implementan y dan seguimiento a los procedimientos de preparación de datos. En este contexto, el diseño de los formatos de entrada asegura que los errores y las omisiones se minimicen. Los procedimientos de manejo de errores durante la generación de los datos aseguran de forma razonable que los errores y las irregularidades son detectados, reportados y corregidos.

AC2 Procedimientos de autorización de documentos fuente

El personal autorizado, actuando dentro de su autoridad, prepara los documentos fuente de forma adecuada y existe una segregación de funciones apropiada con respecto a la generación y aprobación de los documentos fuente.

AC3 Recolección de datos de documentos fuente

Los procedimientos garantizan que todos los documentos fuente autorizados son completos y precisos, debidamente justificados y transmitidos de manera oportuna para su captura.

AC4 Manejo de errores en documentos fuente

Los procedimientos de manejo de errores durante la generación de los datos aseguran de forma razonable la detección, el reporte y la corrección de errores e irregularidades.

AC5 Retención de documentos fuente

Existen procedimientos para garantizar que los documentos fuente originales son retenidos o pueden ser reproducidos por la organización durante un lapso adecuado de tiempo para facilitar el acceso o reconstrucción de datos así como para satisfacer los requerimientos legales.

Controles de entrada de datos

AC6 Procedimientos de autorización de captura de datos

Los procedimientos aseguran que solo el personal autorizado capture los datos de entrada.

AC7 Verificaciones de precisión, integridad y autorización

Los datos de transacciones, ingresados para ser procesados (generados por personas, por sistemas o entradas de interfases) están sujetos a una variedad de controles para verificar su precisión, integridad y validez. Los procedimientos también garantizan que los datos de entrada son validados y editados tan cerca del punto de origen como sea posible.

AC8 Manejo de errores en la entrada de datos

Existen y se siguen procedimientos para la corrección y re-captura de datos que fueron ingresados de manera incorrecta.

Controles en el Procesamiento de datos

AC9 Integridad en el procesamiento de datos

Los procedimientos para el procesamiento de datos aseguran que la separación de funciones se mantiene y que el trabajo realizado de forma rutinaria se verifica. Los procedimientos garantizan que existen controles de actualización adecuados, tales como totales de control de corrida-a-corrida, y controles de actualización de archivos maestros.

AC10 Validación y edición del procesamiento de datos

Los procedimientos garantizan que la validación, la autenticación y la edición del procesamiento de datos se realizan tan cerca como sea posible del punto de generación. Los individuos aprueban decisiones vitales que se basan en sistemas de inteligencia artificial.

AC11 Manejo de errores en el procesamiento de datos

Los procedimientos de manejo de errores en el procesamiento de datos permiten que las transacciones erróneas sean identificadas sin ser procesadas y sin una indebida interrupción del procesamiento de otras transacciones válidas.

Controles de Salida de datos

AC12 Manejo y retención de salidas

El manejo y la retención de salidas provenientes de aplicaciones de TI siguen procedimientos definidos y tienen en cuenta los requerimientos de privacidad y de seguridad.

AC13 Distribución de salidas

Los procedimientos para la distribución de las salidas de TI se definen, se comunican y se les da seguimiento.

AC14 Cuadre y conciliación de salidas

Las salidas cuadran rutinariamente con los totales de control relevantes. Las pistas de auditoría facilitan el rastreo del procesamiento de las transacciones y la conciliación de datos alterados.

AC15 Revisión de salidas y manejo de errores

Los procedimientos garantizan que tanto el proveedor como los usuarios relevantes revisan la precisión de los reportes de salida. También existen procedimientos para la identificación y el manejo de errores contenidos en las salidas.

AC16 Provisión de seguridad para reportes de salida

Existen procedimientos para garantizar que se mantiene la seguridad de los reportes de salida, tanto para aquellos que esperan ser distribuidos como para aquellos que ya están entregados a los usuarios. Controles de límites

AC17 Autenticidad e integridad

Se verifica de forma apropiada la autenticidad e integridad de la información generada fuera de la organización, ya sea que haya sido recibida por teléfono, por correo de voz, como documento en papel, fax o correo electrónico, antes de que se tomen medidas potencialmente críticas.

AC18 Protección de información sensitiva durante su transmisión y transporte

Se proporciona una protección adecuada contra accesos no autorizados, modificaciones y envíos incorrectos de información sensitiva durante la transmisión y el transporte.

Generadores de mediciones

Una necesidad básica de toda empresa es entender el estado de sus propios sistemas de TI y decidir qué nivel de administración y control debe proporcionar la empresa. La obtención de una visión objetiva del nivel de desempeño propio de una empresa no es sencilla. ¿Qué se debe medir y cómo? Las empresas deben medir dónde se encuentran y dónde se requieren mejoras, e implementar un juego de herramientas gerenciales para monitorizar esta mejora. Para decidir cuál es el nivel correcto, la alta dirección debe preguntarse a sí misma: ¿Cómo de lejos debemos ir, y está justificado el coste por el beneficio? COBIT atiende estos temas por medio de:

- Modelos de madurez que facilitan la evaluación por medio de *benchmarking* y la identificación de las mejoras necesarias en la capacidad.
- 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[158].
- Metas de actividades para facilitar el desempeño efectivo de los procesos.

[158] *balanced scorecard.*

MODELOS DE MADUREZ

Cada vez con más frecuencia, se les pide a los directivos de empresas corporativas y públicas que se considere cómo de bien se está administrando la TI. Como respuesta a esto, se debe desarrollar un plan de negocio para mejorar y alcanzar el nivel apropiado de administración y control sobre la infraestructura de información. Aunque pocos argumentarían que esto no es algo bueno, se debe considerar el equilibrio del coste y el beneficio y estas preguntas relacionadas:

• ¿Qué está haciendo nuestra competencia en la industria, y cómo estamos posicionados en relación a ellos?

• ¿Cuáles son las mejores prácticas aceptables en la industria, y cómo estamos posicionados con respecto a estas prácticas?

• Con base en estas comparaciones, ¿se puede decir que estamos haciendo lo suficiente?

• ¿Cómo identificamos lo que se hay que hacer para alcanzar un nivel adecuado de administración y control sobre nuestros procesos de TI? Puede resultar difícil proporcionar respuestas significativas a estas preguntas. La dirección de TI está buscando constantemente herramientas de evaluación por *benchmarking* y herramientas de auto-evaluación como respuesta a la necesidad de saber qué hacer de manera eficiente. Comenzando con los procesos y los objetivos de control de alto nivel de COBIT, el propietario del proceso se debe poder evaluar de forma progresiva, contra los objetivos de control. Esto responde a tres necesidades:

1. Una medición relativa de dónde se encuentra la empresa.
2. Una manera de decidir hacia dónde ir de forma eficiente.
3. Una herramienta para medir el avance hacia la meta.

El modelado de la madurez para la administración y el control de los procesos de TI 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 SEI definió para la madurez de la capacidad del desarrollo de software. Cualquiera que sea el modelo, las escalas no deben ser demasiado granulares, ya que eso haría que el sistema fuera difícil de usar y sugeriría una precisión que no es justificable debido a que en general, el fin es identificar dónde se encuentran los problemas y cómo fijar prioridades para las mejoras. El propósito no es avaluar el nivel de adherencia a los objetivos de control. Los niveles de madurez están diseñados como perfiles de procesos de TI que una empresa reconocería como descripciones de estados posibles actuales y futuros. No están diseñados para ser usados como un modelo limitante, donde no se puede pasar al siguiente nivel superior sin haber cumplido todas las condiciones del nivel inferior. Si se usan los procesos de madurez desarrollados para cada uno de los 34 procesos TI de COBIT, la administración podrá identificar:

- El desempeño real de la empresa—Dónde se encuentra la empresa hoy.
- El estatus actual de la industria—La comparación.
- El objetivo de mejora de la empresa—Dónde desea estar la empresa.

Se ha definido un modelo de madurez para cada uno de los 34 procesos de TI, con una escala de medición creciente a partir de 0, no existente, hasta 5, optimizado. El desarrollo se basó en las descripciones del modelo de madurez genérico.

COBIT es un marco de referencia desarrollado para la administración de procesos de TI con un fuerte enfoque en el control. Estas escalas deben ser prácticas en su aplicación y razonablemente fáciles de entender. El tema de procesos de TI es esencialmente complejo y subjetivo, por lo tanto, es más fácil abordarlo por medio de evaluaciones fáciles que aumenten la conciencia, que logren un consenso amplio y que motiven la mejora. Estas evaluaciones se pueden realizar ya sea contra las descripciones del modelo de madurez como un todo o con mayor rigor, en cada una de las afirmaciones individuales de las descripciones. De cualquier manera, se requiere experiencia en el proceso de la empresa que se está revisando.

0 No existente.

Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.

1 Inicial.

Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen

enfoques *ad hoc* que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.

2 Repetible.

Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

3 Definido.

Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.

4 Administrado.

Es posible monitorizar y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.

5 Optimizado.

Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

La ventaja de un modelo de madurez es que es relativamente fácil para la dirección ubicarse a sí misma en la escala y evaluar qué se debe hacer si se requiere desarrollar una mejora. La escala incluye al 0 ya que es muy posible que no existan procesos en lo absoluto. La escala del 0-5 se basa en una escala de madurez simple que muestra como un proceso evoluciona desde una capacidad no existente hasta una capacidad optimizada. Sin embargo, la capacidad administrativa de un proceso no es lo mismo que el desempeño. La capacidad requerida, como se determina en el negocio y en las metas de TI, puede no requerir aplicarse al mismo nivel en todo el ambiente de TI, es decir, de forma inconsistente o solo a un número limitado de sistemas o unidades. La medición del desempeño, como se cubre en los próximos párrafos, es esencial para determinar cual es el desempeño real de la empresa en sus procesos de TI. Aunque una capacidad aplicada de forma apropiada reduce los riesgos, una empresa debe analizar los controles necesarios para asegurar que el riesgo sea mitigado y que se obtenga el valor de acuerdo al apetito de riesgo y a los objetivos del negocio. Estos controles son dirigidos por los objetivos de control de COBIT.

La capacidad, el desempeño y el control son dimensiones de la madurez de un proceso.

El modelo de madurez es una forma de medir cómo de bien están desarrollados los procesos administrativos, esto es, qué capacidad tienen en realidad. Qué tan bien desarrollados o capaces deberían ser, principalmente dependen de las metas de TI y en las necesidades del negocio subyacentes a la cuales sirven de base. Cuánta de esa capacidad es realmente utilizada actualmente para retornar la inversión deseada en una empresa. Por ejemplo, habrá procesos y sistemas críticos que requieren de una mayor administración de la seguridad que otros que son menos críticos. Por otro lado, el grado y sofisticación de los controles que se requiere aplicar en un proceso están más definidos por el apetito de riesgo de una empresa y por los requerimientos aplicables.

Las escalas del modelo de madurez ayudarán a los profesionales a explicarle a la gerencia dónde se encuentran los defectos en la administración de procesos de TI y a establecer objetivos donde se requieran. El nivel de madurez correcto estará influenciado por los objetivos de negocio de una empresa, por el ambiente operativo y por las prácticas de la industria. Específicamente, el nivel de madurez en la administración se basará en la dependencia que tenga la empresa en la TI, en su sofisticación tecnológica y, lo más importante, en el valor de su información. Un punto de referencia estratégico para una empresa que ayuda a mejorar la administración y el control de los procesos de TI se puede encontrar observando los estándares internacionales y las mejores prácticas. Las prácticas emergentes de hoy en día se pueden convertir en el nivel esperado de desempeño del mañana y por lo tanto son útiles para planificar dónde desea estar la empresa en un lapso de tiempo. Los modelos de madurez se desarrollan empezando con el modelo genérico cualitativo al cual se añaden, en forma creciente, algunos principios contenidos en los siguientes atributos, a través de niveles:

• Conciencia y comunicación

• Políticas, estándares y procedimientos

• Herramientas y automatización

• Habilidades y experiencia

• Responsabilidad y rendición de cuentas

• Establecimiento y medición de metas

La tabla de atributos de madurez muestra las características de cómo se administran los procesos de TI y describe cómo evolucionan desde un proceso no existente hasta uno optimizado. Estos atributos se pueden usar para una evaluación más integral, para un análisis de brechas y para la planeación de mejoras. En resumen, los modelos de madurez brindan un perfil genérico de las etapas a través de las cuales evolucionan las empresas para la administración y el control de los procesos de TI, estos son:

• Un conjunto de requerimientos y los aspectos que los hacen posibles en los distintos niveles de madurez

• Una escala donde la diferencia se puede medir de forma sencilla

• Una escala que se presta a sí misma para una comparación práctica

• La base para establecer el estado actual y el estado deseado

• Soporte para un análisis de brechas para determinar qué se requiere hacer para alcanzar el nivel seleccionado

• Tomado en conjunto, una vista de cómo se administra la TI en la empresa

Los modelos de madurez COBIT se enfocan en la capacidad, y no necesariamente en el desempeño. No son un número al cual hay que llegar, ni están diseñados para ser una base formal de certificación con niveles discretos que formen umbrales difíciles de atravesar. Sin embargo, se diseñaron para ser aplicables siempre, con niveles que brindan una descripción que una empresa pueda reconocer como la mejor para sus procesos. El nivel correcto está determinado por el tipo de empresa, por su medio ambiente y por la estrategia. El desempeño, o la manera en que la capacidad se usa y se implanta, es una decisión de rentabilidad. Por ejemplo, un alto nivel de administración de la seguridad quizá se tenga que enfocar sólo en los sistemas empresariales más críticos. Para finalizar, mientras los niveles de madurez más altos aumentan el control del proceso, la empresa aún necesita analizar, con base en los impulsadores de riesgo y de valor, cuáles mecanismos de control debe aplicar. Las metas genéricas de negocio y de TI, como se definen en este marco de trabajo, ayudarán a realizar este análisis. Los objetivos de control de COBIT guían los mecanismos de control y éstos se enfocan en qué se hace en el proceso; los modelos de madurez se enfocan principalmente en qué tan bien se administra un proceso.

Un ambiente de control implantado de forma adecuada, se logra cuando se han conseguido los tres aspectos de madurez (capacidad, desempeño y control). El incremento en la madurez reduce el riesgo y mejora la eficiencia, generando menos errores, más procesos predecibles y un uso rentable de los recursos.

MEDICIÓN DEL DESEMPEÑO

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

• Las metas y métricas de TI que definen lo que el negocio espera de TI (lo que el negocio usaría para medir a TI)

• Metas y métricas de procesos que definen lo que el proceso de TI debe generar para dar soporte a los objetivos de TI (cómo sería medido el propietario del proceso de TI)

• Métricas de desempeño de los procesos (miden qué tan bien se desempeña el proceso para indicar si es probable alcanzar las metas)

COBIT utiliza dos tipos de métrica: indicadores de metas e indicadores de desempeño. Los indicadores de metas de bajo nivel se convierten en indicadores de desempeño para los niveles altos. Los indicadores clave de metas (KGI) definen mediciones para informar a la gerencia (después del hecho) si un proceso TI alcanzó sus requerimientos de negocio, y se expresan por lo general en términos de criterios de información:

• Disponibilidad de información necesaria para dar soporte a las necesidades del negocio

• Ausencia de riesgos de integridad y de confidencialidad

• Rentabilidad de procesos y operaciones

• Confirmación de confiabilidad, efectividad y cumplimiento

Los indicadores clave de desempeño (KPI) definen mediciones que determinan qué tan bien se está desempeñando el proceso de TI para alcanzar la meta. Son los indicadores principales que indican si será factible lograr una meta o no, y son buenos indicadores de las capacidades, prácticas y habilidades. Miden las metas de las actividades, las cuales son las acciones que el propietario del proceso debe seguir para lograr un efectivo desempeño del proceso. Las métricas efectivas deben tener las siguientes características:

• Una alta proporción entendimiento-esfuerzo (esto es, el entendimiento del desempeño y del logro de las metas en contraste con el esfuerzo de lograrlos).

• Deben ser comparables internamente (esto es, un porcentaje en contraste con una base o números en el tiempo).

• Deben ser comparables externamente sin tomar en cuenta el tamaño de la empresa o la industria.

• Es mejor tener pocas métricas (quizá una sola muy buena que pueda ser influenciada por distintos medios) que una lista más larga de menor calidad.

• Debe ser fácil de medir y no se debe confundir con las metas.

Las metas se definen de arriba hacia abajo con base en las metas de negocio que determinarán el número de metas que soportará TI, las metas de TI decidirán las diferentes necesidades de las metas de proceso, y cada meta de proceso establecerá las metas de las actividades. El logro de metas se mide con las métricas de resultado (llamadas indicadores clave de metas o KGI[159]s) y dirigen las metas de más alto nivel. Por ejemplo, la métrica que midió el logro de la meta de la actividad es un motivador de desempeño (llamado indicador

[159] *Key Goal Indicator*.

clave de desempeño o KPI[160]) para la meta del proceso. Las métricas permiten a la gerencia corregir el desempeño y realinearse con las metas.

El modelo del marco de trabajo COBIT

El marco de trabajo COBIT, por lo tanto, relaciona los requerimientos de información y de gobierno a los objetivos de la función de servicio de TI. El modelo de procesos COBIT permite que las actividades de TI y los recursos que los soportan sean administrados y controlados basados en los objetivos de control de COBIT, y alineados y monitoreados usando las métricas KGI y KPI de COBIT.

Para resumir, los recursos de TI son manejados por procesos de TI para lograr metas de TI que respondan a los requerimientos del negocio. Este es el principio básico del marco de trabajo COBIT, como se ilustra en el Cubo COBIT de la figura 99.

[160] *Key Process Indicator*.

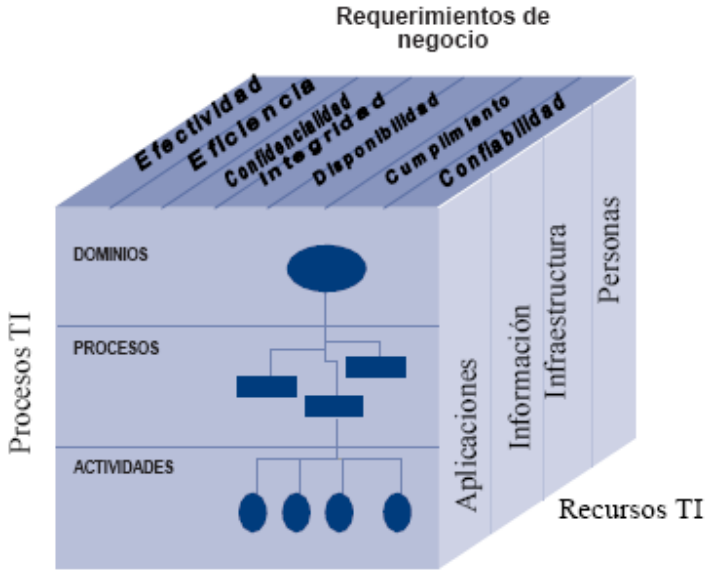


Figura 94.- **Cubo COBIT.**

Nivel de aceptación general de COBIT

COBIT se basa en el análisis y armonización de estándares y mejores prácticas de TI existentes y se adapta a principios de gobierno generalmente aceptados. Está posicionado a un nivel alto, impulsado por los requerimientos del negocio, cubre el rango completo de actividades de TI, y se concentra en lo que se debe lograr en lugar de cómo lograr un gobierno, administración y control efectivos. Por lo tanto, funciona como un integrador de prácticas de gobierno de TI y es de interés para la dirección ejecutiva; para la gerencia del negocio, para la gerencia y gobierno de TI; para los profesionales de aseguramiento y seguridad; así como para los profesionales de auditoría y control de TI. Está diseñado para ser complementario y para ser usado junto con otros estándares y mejores prácticas.

La implantación de las mejores prácticas debe ser consistente con el gobierno y el marco de control de la empresa, debe ser apropiada para la organización, y debe estar integrada con otros métodos y prácticas que se utilicen. Los estándares y las mejores prácticas no son una panacea y su efectividad depende de cómo hayan sido implantados en realidad y de cómo se mantengan actualizados. Son más útiles cuando se aplican como un conjunto de principios y como un punto de partida para adaptar procedimientos específicos. La gerencia y el equipo deben entender qué hacer, cómo hacerlo y porqué es importante hacerlo para garantizar que se utilicen las prácticas.

Para lograr la alineación de las mejores prácticas con los requerimientos del negocio, se recomienda que COBIT se utilice al más alto nivel, brindando así un marco de control general basado en un modelo de procesos de TI que debe ser aplicable en general a toda empresa. Las prácticas y los estándares específicos que cubren áreas discretas, se pueden equiparar con el marco de trabajo de COBIT, brindando así una jerarquía de materiales guía.

COBIT resulta de interés a distintos usuarios:

• Dirección ejecutiva—Para obtener valor de las inversiones y riesgos de TI y para controlar la inversión en un ambiente de TI con frecuencia impredecible.

• Gerencia del negocio—Para obtener certidumbre sobre la administración y control de los servicios de TI, proporcionados internamente o por terceros.

• Gerencia de TI—Para proporcionar los servicios de TI que el negocio requiere para dar soporte a la estrategia del negocio de una forma controlada y administrada.

• Auditores—Para respaldar sus opiniones y/o para proporcionar asesoría a la gerencia sobre controles internos.

Un instituto de investigación sin fines de lucro desarrolló COBIT y lo mantiene actualizado, tomando la experiencia de los miembros de sus asociaciones afiliadas, de los expertos de la industria, y de los profesionales de control y seguridad. Su contenido se basa en una investigación continua sobre las mejores prácticas de TI y se le da un mantenimiento continuo, proporcionando así un recurso objetivo y práctico para todo tipo de usuario.

COBIT está orientado a los objetivos y al alcance del gobierno de TI, asegurando que su marco de control sea integral, que esté alineado con los principios de gobierno empresariales y, por lo tanto, que sea aceptable para los consejos directivos, para la dirección ejecutiva, para los auditores y reguladores. En el apéndice II, se ofrece un mapa que muestra cómo los objetivos de control detallados de COBIT se relacionan con las cinco áreas focales del gobierno de TI y con las actividades de control de COSO.

ISO 20000

El tratamiento de la información hace tiempo que es un punto fundamental en cualquier tipo de organización. En el pasado los procesos de misión crítica del negocio no estaban soportados por sistemas informáticos, sin embargo en la actualidad estos procesos del negocio están soportados cada vez más por diferentes servicios de TI. La TI es imprescindible en las compañías y organizaciones de hoy en día, por tanto, los departamentos de TI se han convertido en imprescindibles para el éxito del negocio de cualquier organización y el alineamiento entre los objetivos de su departamento de TI y del negocio es esencial.

La rápida evolución de la tecnología esta propiciando un significativo crecimiento en la aportación de las TI a los negocios, y cada día más negocios están diseñando y poniendo servicios cada vez mas sofisticados a disposición de sus clientes finales.

Actualmente los servicios de TI sobrepasan las fronteras de las organizaciones convirtiéndose en productos de la compañía, situando a la gestión de los servicios TI como uno de los elementos clave que debe tener en cuenta en su estrategia del negocio, tanto en las previsiones de ingresos y crecimiento, como en las de contingencia y supervivencia de la compañía ante situaciones críticas. Esto es particularmente importante para las organizaciones de sectores industriales y del sector financiero, el sanitario y el de servicios públicos, suministro de agua, electricidad, gas, etc. En estos casos ya no basta con tener

unos excelentes servicios TI, sino que es necesario demostrar a sus accionistas y clientes que disponen de una infraestructura tecnológica y unos servicios fiables y bien gestionados.

Adicionalmente las empresas también tienen que tener en cuenta las implicaciones relacionadas con el cumplimiento de las normativas locales de cada país. Cada vez existen más normas y leyes cuyo cumplimiento es preciso demostrar. Normas como la ley Sarbanes-Oxley o la ley de portabilidad y responsabilidad de seguros médicos de 1996 (*Health Insurance Portability and Accountability Act*) de Estados Unidos contemplan específicamente puntos relacionados con los servicios tecnológicos y su gestión. En la actualidad, los inspectores no exigen la presentación de certificaciones como prueba de cumplimiento, pero la tendencia hace pensar que lo van a hacer en un futuro cercano.

Por todos estos motivos, el correcto servicio proporcionado por la TI a las organizaciones es crítico para el éxito del negocio de la organización, debido a esto, cada vez son más imprescindibles sistemas para medir la correcta gestión de la TI. Estos sistemas, además, deberían llevar a cabo un proceso de mejora continua de esta gestión.

Asimismo, la necesidad de las organizaciones por mantenerse competitivas ante los nuevos retos del mercado, ha propiciado que adopten esquemas de trabajo orientados a procesos para conseguir el cumplimiento de las distintas normativas legales y locales, la satisfacción de sus clientes y todo ello al menor coste posible.

Además, hay que añadir que las preocupaciones en torno a los servicios de TI, tanto internos como subcontratados, crecen debido a que estos servicios pocas veces se ajustan a las necesidades de empresas y clientes.

En este contexto nace en Diciembre de 2005 la norma ISO/IEC 20000 que aborda específicamente la calidad de gestión de los servicios TI que, debido a la necesidad del sector y organismos reguladores, podría convertirse en la norma internacional utilizada por los inspectores para comprobar el cumplimiento de determinadas normativas legales y locales.

ISO/IEC 20000 es aplicable a cualquier organización, grande o pequeña, de cualquier sector o parte del mundo, que se base en servicios de TI. La norma es especialmente apropiada para proveedores internos de servicios de TI, como los departamentos de TI, y para proveedores externos de estos servicios, como las organizaciones de subcontratación de TI.

Esta norma ya está repercutiendo positivamente en algunos de los sectores dependientes de la TI más importantes, como los de externalización de procesos de negocio, telecomunicaciones y finanzas, así como el sector público.

Ante esta situación las compañías y organizaciones de todo el mundo se van a plantear lo que deben hacer respecto a la norma ISO/IEC 20000. Se tratará de responder a

esta cuestión en los siguientes apartados, en los que se intentará exponer de una forma natural, una visión clara de la norma y cómo se puede utilizar la misma para mejorar la gestión de los servicios TI de las compañías.

NORMA ISO/IEC 20000

Es el primer estándar específico para la Gestión de Servicios de TI, y su objetivo principal es aportar los requisitos necesarios, dentro del marco de un sistema completo e integrado, que permita que una organización provea servicios TI gestionados, de calidad y que satisfagan los requisitos de negocio de sus clientes.

Se trata de una especificación que contiene un modelo de gestión de servicios basado en procesos y en las mejores prácticas de la industria, que proporciona una guía para la gestión y auditoría de servicios de TI.

La norma proporciona la base para probar que una organización de TI ha implantado buenas prácticas para la gestión del servicio y que las está usando de forma regular y consistente.

La norma ISO/IEC 20000 define la estructura de un sistema de gestión de los servicios TI (ITSMS, *Information Technologies Service Management System*), regulando tanto la prestación de los servicios como su gestión. Esta norma facilita la definición

adecuada del catálogo de servicios y permite desarrollar de forma efectiva los ANSs que los regulen.

La norma ISO/IEC 20000 está estructurada en dos documentos, bajo el título general *Information technology – Service management*:

- **ISO/IEC 20000-1**. Este documento de la norma recoge el conjunto de los "requisitos obligatorios" que debe cumplir el proveedor de servicios TI, para realizar una gestión eficaz de los servicios que responda a las necesidades de las empresas y sus clientes.

- **ISO/IEC 20000-2**. Esta parte contiene un código de prácticas para la gestión de servicios ("*Code of Practice for Service Management*") que trata cada uno de los elementos contemplados en la parte 1, analizando y aclarando su contenido. En resumen, este documento pretende ayudar a las organizaciones a establecer los procesos de forma que cumplan con los objetivos de la parte 1.


INTERNATIONAL STANDARD

ISO/IEC 20000-1

First edition
2005-12-15

Information technology — Service management —
Part 1:
Specification

Technologies de l'information — Gestion de services —
Partie 1: Spécifications


INTERNATIONAL STANDARD

ISO/IEC 20000-2

First edition
2005-12-15

Information technology — Service management —
Part 2:
Code of practice

Technologies de l'information — Gestion de services —
Partie 2: Code de bonne pratique

Figura 1. Portada Documentos ISO/IEC 20000

ISO/IEC 20000 proporciona al sector una norma internacional para todas la empresas que ofrezcan servicios de TI, tanto a clientes internos como externos, creando un marco de referencia y una terminología común para todos los actores implicados: los proveedores de servicios, sus suministradores y sus clientes.

En este punto es interesante aclarar que la certificación ISO/IEC 20000 sólo se otorga a organizaciones que realizan operaciones de gestión de servicios TI, y que la norma sólo certifica el buen funcionamiento de esas operaciones, por lo tanto, no entran en su

ámbito de competencia la certificación de productos, ni servicios de consultoría relativos a la aplicación de buenas prácticas.

Partiendo de este contexto, se puede considerar que la norma ISO/IEC 20000 va dirigida a:

- Organizaciones que busquen mejorar sus servicios TI, mediante la aplicación efectiva de los procesos para monitorizar y mejorar la calidad de los servicios.
- Negocios que solicitan ofertas para sus servicios.
- Negocios que requieren de un enfoque consistente por parte de todos sus proveedores de servicio en la cadena de suministro.
- Organizaciones TI que necesiten demostrar su capacidad para proveer servicios que cumplan con los requisitos de los clientes.
- Proveedores de servicio TI para medir y comparar la gestión de sus servicios mediante una evaluación independiente.

Historia de ISO/IEC 20000

Los antecedentes de la norma se remontan a 1989 cuando la institución británica BSI (*British Standards Institution*) comenzó la definición de un estándar para la gestión de servicios TI, que finalizó con su publicación como estándar BS 15000 en 1995.

A partir de ese año BSI continuó con el desarrollo del estándar trabajando en una segunda parte, con el objetivo de profundizar en los conceptos de la parte 1 ya publicada. En la realización de aquel trabajo se identificó que sería muy beneficioso para el sector TI que las publicaciones que realizase BS estuvieran alineadas con las publicaciones ITIL de buenas prácticas, impulsadas por el Gobierno Británico. Como consecuencia de este interés se formalizó un acuerdo de alineamiento del que BS 15000 se benefició de los contenidos de ITIL, y posteriormente cuando el estándar pasó a ser ISO/IEC 20000 fue éste quien ejerció su influencia en los contenidos de la nueva versión 3 de ITIL que se publicó en Mayo de 2007.

La segunda parte del estándar se publicó en 1998, y posteriormente se siguió evolucionando la norma que vio la luz en su versión final en el año 2000 como BS 15000 parte 1 y 2.

Como complemento a los documentos "core" de la norma se desarrollaron unos contenidos adicionales para facilitar su adopción, publicándose un esquema de autoevaluación y una guía para los gestores de servicio.

Gracias a la temprana adopción de esta norma por las compañías del sector, se pudo realizar una revisión y evolución de la primera versión de la norma BS 15000, publicando una segunda versión en el año 2002, que incluyó principalmente nuevas cláusulas en los

apartados de responsabilidades de la gestión y la mejora continua con el ciclo de Deming *Plan-Do-Check-Act* (también conocida como PDCA).

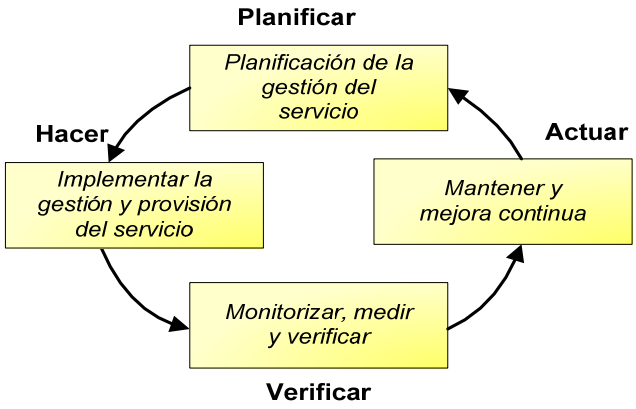


Figura 2. Ciclo de Deming (PDCA)

Desde su publicación en el año 2000 este estándar despertó un rápido interés, y un elevado nivel de adopciones en otros países, por lo que en el mes de Octubre del año 2004 se solicitó a ISO/IEC la elevación de este estándar británico a estándar internacional.

Como consecuencia de la madurez del estándar se utilizó una vía de "*fast track*" en la que se procedió a realizar todas las actividades marcadas para la evaluación del estándar: análisis, debate, comentarios, votaciones de los diferentes organismos de normalización nacionales, cambios finales y creación de las estructuras necesarias para la adopción y evolución de la norma dentro de los organismos ISO/IEC.

Tras 14 meses de trabajo, el 15 de Diciembre de 2005 se publicó el estándar ISO/IEC 20000 1 y 2, retirándose en ese momento el estándar BS 15000.

A partir de ese momento se inicia el plan para la gestión y futura evolución del estándar ISO/IEC 2000, acordándose en Marzo de 2006 por el Comité Técnico Conjunto JTC-1, la creación de un nuevo grupo de trabajo, el WG 25, que se encuadra dentro del subcomité 7 de este organismo (JTC-1 SC7) iniciando sus actividades en Abril del año 2006.

A nivel nacional, el comité AEN/CTN 71 Tecnologías de la Información se encarga en el año 2006 de la traducción de la norma al español, y posteriormente AENOR (organización delegada en España de ISO/IEC) inició el mecanismo de adopción y conversión de la norma ISO 20000 a norma UNE. AENOR recibe la versión traducida de la norma en Junio de 2006 y procede a su localización y publicación como norma UNE-ISO/IEC 20000 en el BOE, el día 25 de Julio de 2007.

En el mes de Julio del año 2007, se certifican en la norma UNE-ISO/IEC 20000-1 las dos primeras compañías españolas (Telefónica Soluciones y el Corte Inglés).

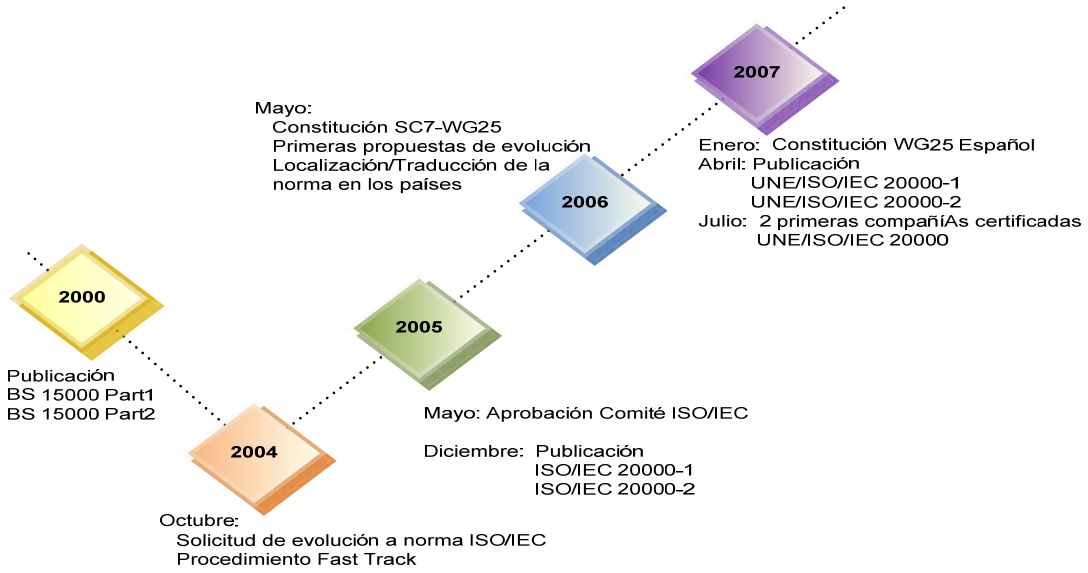


Figura 3. Historia ISO/IEC 20000

La aparición de la norma ISO/IEC 20000 ha supuesto el primer sistema de gestión en servicios de TI certificable bajo norma reconocida a nivel mundial. Hasta el momento de la aparición de esta norma, las organizaciones podían optar por aplicar el conjunto de mejores prácticas dictadas por ITIL o certificar su gestión contra el estándar local británico BS 15000.

Ante todo, la certificación ISO/IEC 20000 permite demostrar de una forma independiente que una entidad dispone de controles y procedimientos adecuados y cumple con las mejores prácticas para prestar coherentemente un servicio de TI de calidad y rentable.

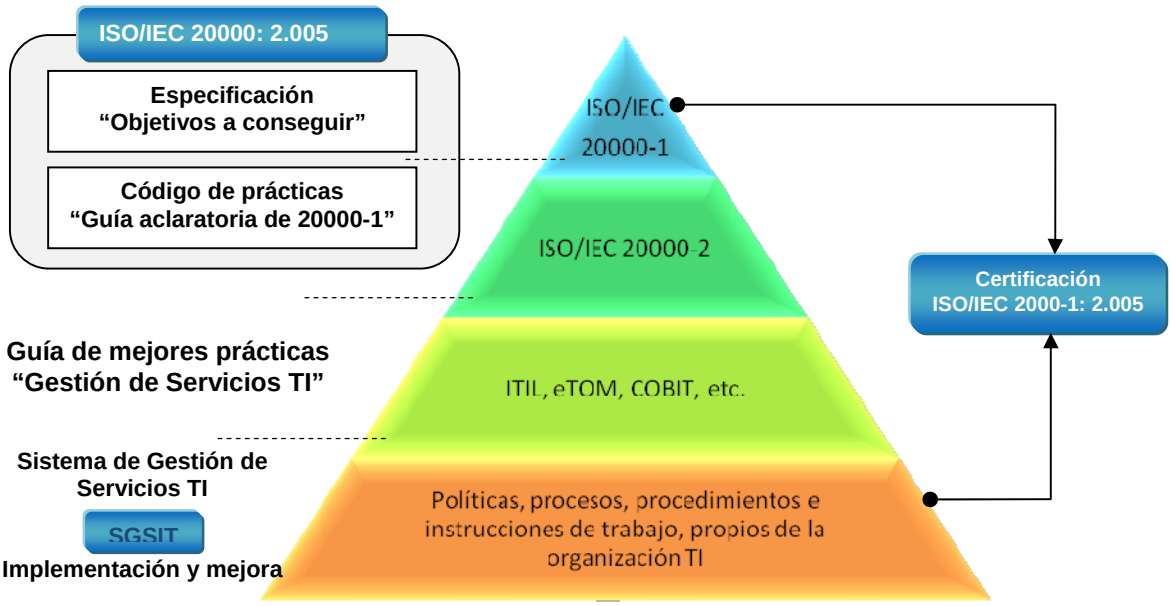


Figura 4. Ámbito de actuación de la norma ISO/IEC 20000

A continuación, se enumeran algunas de las ventajas clave que esto aporta a las organizaciones:

- Los proveedores de servicios de TI responden mejor a los servicios regidos por aspectos comerciales que a los impulsados por la tecnología.
- Los proveedores de servicios externos pueden utilizar la certificación como elemento diferencial y ampliar el negocio, ya que dicha certificación se va convirtiendo cada vez más en un requisito contractual.
- Ofrece la posibilidad de seleccionar y gestionar a los proveedores de servicios externos con mayor eficacia.

- Más oportunidades de mejorar la eficacia, fiabilidad y coherencia de los servicios de TI que repercuten en los costes y el servicio.
- Las auditorías de certificación permiten la evaluación periódica de los procesos de gestión de servicios, lo que ayuda a mantener y mejorar la eficacia.
- El proceso de certificación puede reducir la cantidad de auditorías a proveedores y disminuir los costes.
- La ISO/IEC 20000 es completamente compatible con la metodología ITIL de orientación sobre las mejores prácticas para procesos de gestión de servicios de TI.
- La ISO/IEC 20000 es completamente compatible y complementaria al resto de normas ISO internacionales del campo de los servicios de TI, como por ejemplo la ISO 27001.

Contenido de la norma ISO/IEC 20000

Como ya se ha comentado anteriormente, esta norma se estructura en torno a la utilización de procesos integrados para la gestión de los servicios TI, posicionándolos en un modelo de referencia y, estableciendo todo aquello que es obligatorio para la buena gestión de los servicios TI.

Estos procesos dan cobertura a las necesidades del ciclo de vida de los servicios, contemplando muchos de los procesos incluidos en la versión 2 de ITIL y otros adicionales,

algunos de los cuales han sido posteriormente adoptados por ITIL en su versión 3, publicada dos años más tarde.

La especificación y los requisitos de ISO/IEC 20000 representan un consenso para la industria en estandarización de calidad para la gestión de los servicios TI.

En este apartado se va a tratar cada una de las secciones que forman la norma y sus componentes, reflejando cuales son sus objetivos y el número de requisitos de control que según la norma deben cumplir.

Es importante destacar que la norma no enumera sus requisitos de control, por lo que las cifras que aparecen reflejadas podrían variar con respecto a otros documentos. Esto es debido a que la norma establece sus requisitos en párrafos, que en algunos casos se pueden considerar "multirrequisito" y puede haber autores que consideren solamente estos párrafos. En nuestro caso, el número de requisitos se ha establecido, descomponiendo los párrafos con requisitos múltiples en requisitos unitarios.

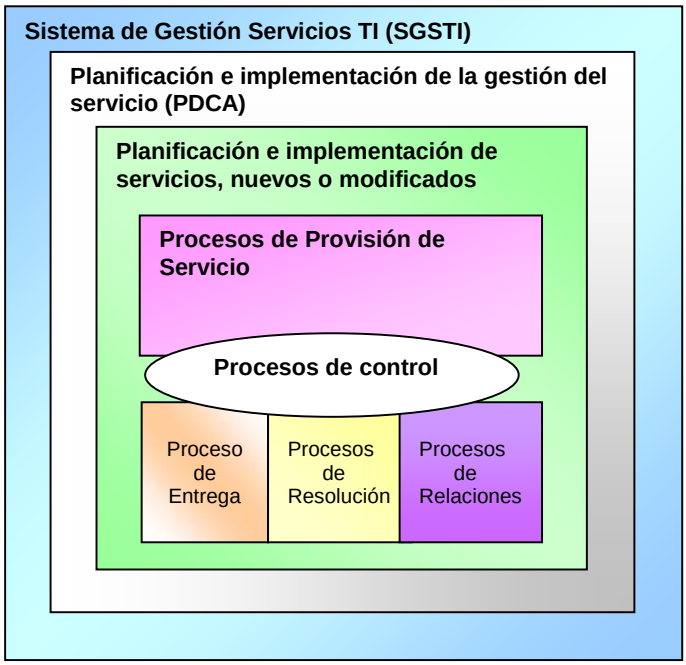


Figura 5. Marco de referencia ISO/IEC 20000

Tal y como se puede ver en la figura anterior, la norma ISO/IEC 20000 cubre las siguientes secciones:

- **El Sistema de Gestión de Servicios TI (SGSTI).** Esta sección contempla la política y las actividades de trabajo necesarias para que una organización pueda realizar una eficiente implantación y gestión posterior de los servicios TI.

El Sistema de Gestión de los Servicios TI cubre los aspectos de Responsabilidad de la dirección, Requisitos de la documentación, Competencia, Concienciación y Formación.

Para cubrir este objetivo la norma contempla 17 requisitos de control a cumplir.

- **Planificación e Implementación de la Gestión del Servicio.** En la actualidad es absolutamente necesario lograr una gestión efectiva de los servicios TI, pero no es suficiente ya que también es necesario lograr que la calidad de los servicios mejore de forma continua.

  Por este motivo uno de los objetivos fundamentales de la norma ISO/IEC 20000 es validar la mejora continua de la calidad de la gestión de los servicios, y para ello ha utilizado el modelo de mejora de la calidad definido por W. Edwards Deming aplicado inicialmente en la industria de la fabricación y empleado con éxito en otras normas ISO/IEC (9000, 27001, etc…).

  Adicionalmente a ISO/IEC 20000, las organizaciones pueden utilizar COBIT para materializar las medidas de los avances en el logro de nuevos niveles de mejora a medida que la gestión de los servicios gana en madurez.

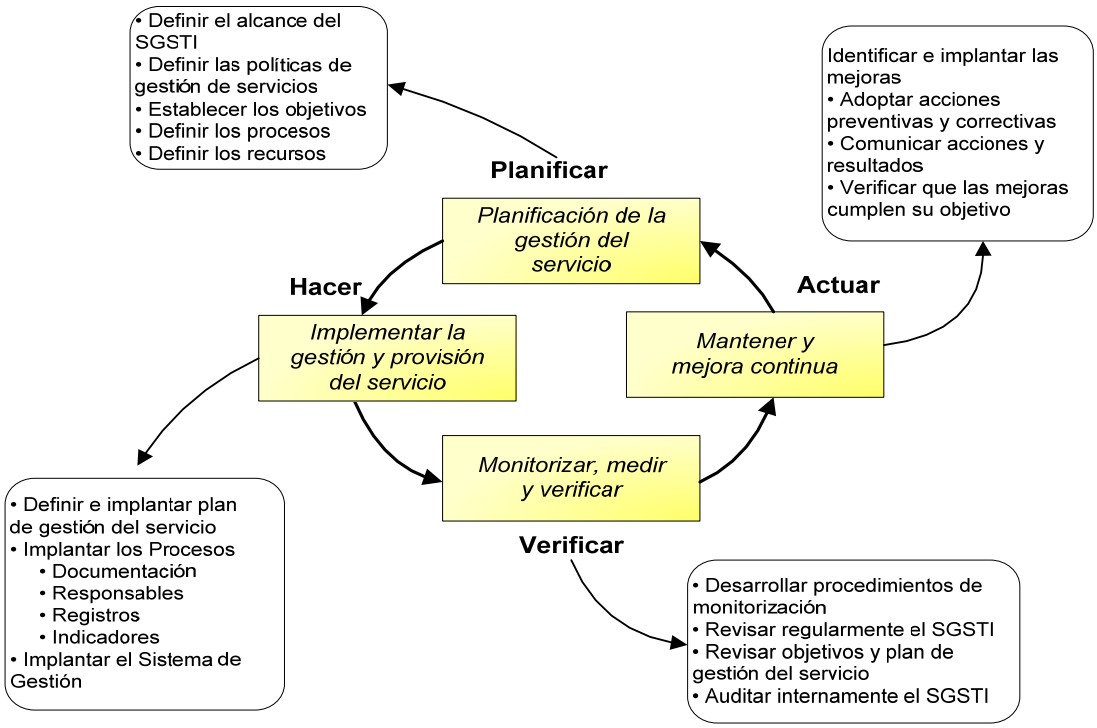


Figura 6. Mejora continua de la calidad en ISO/IEC 20000

En la figura anterior, pueden verse los distintos apartados que cubre esta sección de la norma, que se detallan a continuación:

1. **La planificación de la gestión del servicio (Planificar)**. Tiene como objetivo planificar la implantación y la provisión de la gestión del servicio, contemplando aspectos como, el alcance de la gestión del servicio, los enfoques de planificación, los eventos a considerar, el alcance y contenidos del plan, etc.

Entre los principales aspectos que se contemplan en este apartado podemos mencionar:

- Definición del alcance del SGSTI
- Definición de las políticas de gestión de servicios
- Establecer los objetivos
- Definir los procesos
- Definir los recursos

Para cubrir este apartado la norma contempla 13 requisitos de control a cumplir.

2. **Implementación de la gestión del servicio y la provisión del servicio (Hacer).** Tiene como misión implantar los objetivos de la gestión del servicio y el plan definidos. Entre los aspectos más relevantes que trata se pueden mencionar los siguientes:

   2.1. Definir e implantar el Plan de Gestión del Servicio

   2.2. Implantar los Procesos (documentación, responsables, registros, indicadores)

   2.3. Implantar el Sistema de Gestión

Para cubrir este apartado la norma contempla 9 requisitos de control a cumplir.

3. **Monitorización, medición y revisión (Verificar).** Su objetivo es monitorizar, medir y revisar que los objetivos y el plan de gestión del servicio definidos se están cumpliendo, poniendo de manifiesto la capacidad de los procesos para alcanzar los resultado planificados.

   Como aspectos más relevantes se pueden señalar los siguientes:

- Desarrollo de procedimientos de monitorización
- Revisiones periódicas del SGSTI
- Revisar objetivos y plan de gestión del servicio

Para cubrir este apartado la norma contempla 9 requisitos de control a cumplir.

4. **Mejora continua (Actuar).** Su objetivo es mejorar la eficacia y la eficiencia de la entrega y de la gestión del servicio, contemplando aspectos como la política de mejora y la planificación de las mejoras del servicio.

   Los aspectos más relevantes son:

   - Identificar e implantar las mejoras
   - Adoptar acciones preventivas y correctivas
   - Comunicar acciones y resultados
   - Verificar que las mejoras cumplen su objetivo

   Para cubrir este apartado la norma contempla 16 objetivos de control a cumplir.

- **Planificación e Implementación de Servicios, Nuevo o Modificados.** Esta sección de la norma contiene un solo proceso que tiene como objetivo asegurar que la creación de nuevos servicios, las modificaciones a los existentes e incluso la

eliminación de un servicio, se puedan gestionar y proveer con los costes, calidad y plazos acordados.

Para ello, hay que gestionar el ciclo completo de la provisión y entrega de los servicios, realizando una planificación unificada e integrada, considerando los costes y el impacto a nivel organizativo, técnico y comercial que pudiera derivar de su entrega y gestión, asegurando que todas las partes implicadas conocen y cumplen con el plan y los compromisos acordados.

Este proceso esbozado en la norma ISO/IEC 20000, e inexistente en ITIL tanto en la versión 2 como en la versión 3, comienza en el cliente y finaliza con el servicio entregado y operativo, o eliminado. Para lograr que todo funcione adecuadamente y sin duplicar actividades, se debe sincronizar el funcionamiento del resto de procesos de gestión del servicio involucrados: Relaciones con el negocio, la Gestión de nivel de servicio, Generación de informes del servicio, etc., realmente debe actuar como un "proceso director" que permita coordinar y encadenar la participación de todos los procesos de la gestión del servicio implicados.

Este proceso contempla 16 requisitos de control a cumplir.

- **Procesos de Provisión de Servicio.** En esta sección se tratan los requisitos necesarios para cubrir la provisión de los servicios que el cliente necesita, y todo aquello que es necesario en TI para poder prestar estos servicios.

Para conseguir su objetivo ISO/IEC 20000 estructura esta sección en un conjunto de procesos con objetivos específicos y unitarios para evitar posibles conflictos.

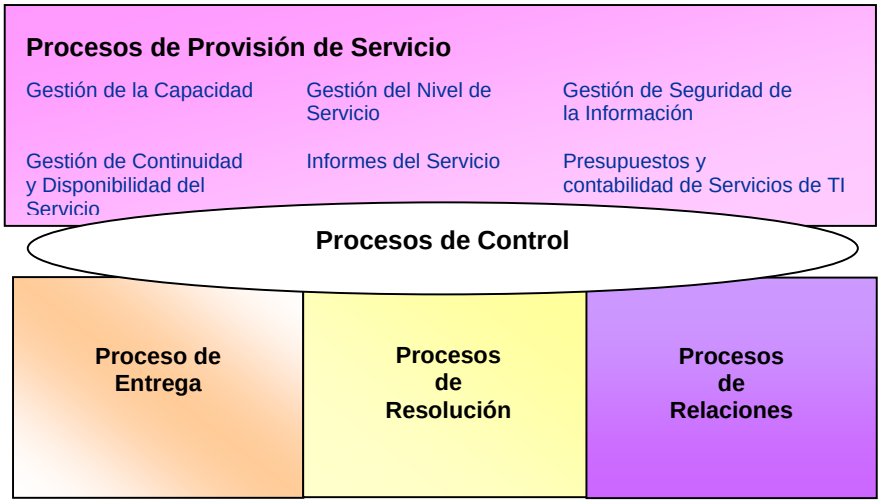


Figura 7. Procesos de Provisión del Servicio

Seguidamente se va a dar un repaso por los procesos que componen esta sección para conocer sus objetivos.

1. **Gestión de Nivel de Servicio.** Este proceso es aparentemente igual que el de ITIL, sin embargo se aligera de contenido en la norma, ya que parte de las funciones contempladas en ITIL se reparten en otros procesos, alguno de los cuales no tiene equivalencia en ITIL versión 2 ni en versión 3.

En ISO/IEC 20000 se establecen procesos específicos para actividades que en ITIL se realizan dentro de este proceso: Relaciones con el Negocio que se encarga de gestionar

la relación con los clientes; Planificación e Implementación de servicios, nuevos o modificados; Generación de Informes de Servicio y Gestión de Suministradores, estos dos últimos procesos ya se han contemplado en la versión 3 de ITIL.

En la norma, el objetivo del proceso de gestión de nivel de servicio es definir y acordar con las partes los acuerdos de nivel de servicio, para posteriormente registrarlos adecuadamente y gestionar su cumplimiento y evolución. Controla si se están consiguiendo los niveles de servicio acordados, y en caso necesario determina los motivos y promueve las acciones de mejora adecuadas.

Este apartado contempla 9 requisitos de control a cumplir.

2. **Generación de Informes del Servicio.** El objetivo de este proceso es generar los informes de servicio acordados, fiables, precisos y en plazo, de forma que permitan verificar si se están cumpliendo los requisitos y necesidades de los usuarios, e informar de la toma de decisiones con el fin de lograr una comunicación eficaz.

Este proceso contempla 10 requisitos de control a cumplir.

3. **Gestión de la Continuidad y Disponibilidad del Servicio.** El objetivo de este proceso es conseguir que los compromisos de disponibilidad y continuidad puedan cumplirse en la forma en que se han acordado con los clientes.

Este proceso debe controlar los riesgos y mantener la continuidad del servicio, tanto en situaciones de fallos o mal funcionamiento (disponibilidad) como en casos catástrofes y desastres (continuidad).

Para cubrir este objetivo la norma contempla 13 requisitos de control a cumplir.

4. **Elaboración de Presupuesto y Contabilidad de los Servicios de TI.** El objetivo de este proceso es presupuestar y contabilizar los costes de la provisión del servicio.

Como se puede observar en el objetivo de la norma no se contempla la facturación de los servicios; esto es debido a que en la práctica muchos proveedores de servicios no realizan una facturación formal de los servicios a sus clientes, principalmente las unidades internas de TI de las compañías. Por este motivo, la norma considera esta actividad como opcional. Sin embargo, hay que recomendar a los proveedores que si hacen uso de la facturación el mecanismo utilizado debe estar plenamente definido y entendido por todas las partes. También hay que tener en cuenta que la facturación debe estar alineada con las prácticas contables tanto del país como las más específicas de la organización del proveedor del servicio.

Para cubrir este objetivo la norma contempla 7 requisitos de control a cumplir.

5. **Gestión de la Capacidad.** El objetivo de este proceso es asegurar que el proveedor del servicio tiene en todo momento la capacidad suficiente para

cubrir la demanda acordada, actual y futura, de las necesidades del negocio del cliente.

Para poder realizar una gestión eficiente de la capacidad es necesario elaborar un plan de capacidad que este dirigido a las necesidades reales del negocio. El plan de capacidad contempla aspectos como los requisitos de capacidad de rendimiento, de evolución prevista tanto por cambios internos como por cambios externos, como por ejemplo legislativos, etc.

Para cubrir este objetivo la norma contempla 8 requisitos de control a cumplir.

6. **Gestión de Seguridad de la Información.** El objetivo de este proceso es gestionar la seguridad de la información de manera eficaz para todas las actividades del servicio.

Para establecer una gestión de la seguridad es necesario establecer, y comunicar a todo el personal, una política de seguridad que contemple los controles adecuados para gestionar los riesgos asociados al acceso a los servicios o a los sistemas.

Para cubrir este objetivo la norma contempla 13 objetivos de control a cumplir.

Adicionalmente, para aquellas organizaciones que requieran un alto nivel en la gestión de la seguridad de la información existe una norma específica, ISO/IEC 27001, que proporciona un código de prácticas para la gestión de la seguridad de la información.

- **Procesos de Relaciones.** Los proveedores de servicio TI tienen dos puntos externos de relación, por una parte se encuentra la relación con el negocio y los clientes a los que da servicio, y por la otra está la relación con sus suministradores, fundamental para el soporte y evolución del servicio.

Una adecuada gestión de estas relaciones posibilita el control adecuado de los dos factores externos a la organización que son claves para la realización de una correcta gestión del servicio TI.

En esta sección ISO/IEC 20000 trata los requisitos necesarios para cubrir estas relaciones mediante dos procesos específicos: Gestión de Relaciones con el Negocio y Gestión de Suministradores.

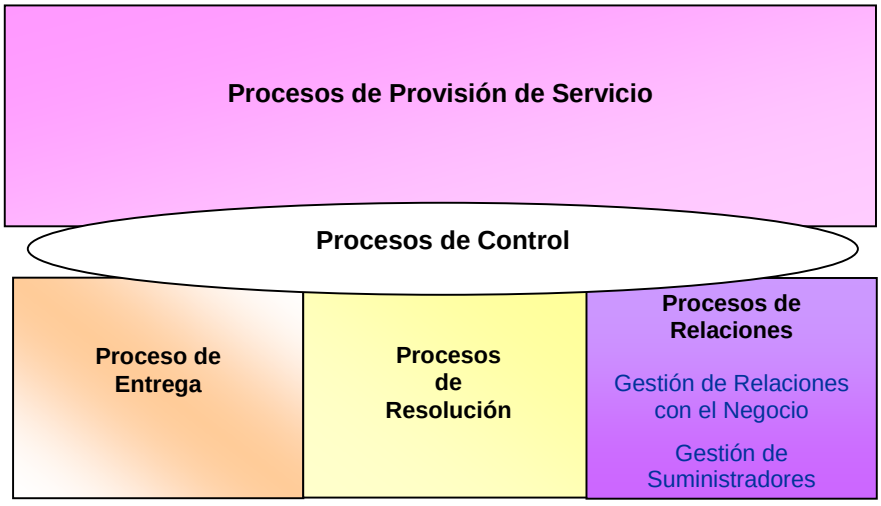


Figura 8. Procesos de Relaciones

Finalmente es interesante mencionar que esta sección de ISO/IEC 20000 también ha influenciado a ITIL, que en su versión 3 ha incluido un proceso específico para la gestión de suministradores. Sin embargo, no han incluido ningún proceso específico para gestionar de forma adecuada la relación con los clientes.

7. **Gestión de las Relaciones con el Negocio.** El objetivo de este proceso es establecer y mantener una buena relación entre el proveedor del servicio y el cliente, basándose en el entendimiento del cliente y de los fundamentos de su negocio.

La gestión de la relación con el negocio asegura que todas las partes implicadas en la provisión de un servicio, incluyendo también al propio cliente, están identificadas y gestionadas, responsabilizándose de dar una respuesta adecuada a las demandas del cliente gracias a su función de interfaz entre el negocio y las áreas de TI.

Esto se consigue negociando y acordando los niveles de servicio a proveer, monitorizando e informando acerca del rendimiento del servicio, y creando una relación de negocio eficaz entre la organización TI y sus clientes.

En este proceso se vela por la satisfacción del cliente atendiendo sus reclamaciones y revisando periódicamente los acuerdos y contratos establecidos. Adicionalmente también debe permanecer al tanto de las necesidades del negocio y de los principales cambios en el mismo para preparar una respuesta a dichas necesidades.

Para cubrir este objetivo la norma establece 15 requisitos de control a cumplir.

8. **Gestión de Suministradores.** El objetivo de este proceso es gestionar los suministradores para garantizar la provisión, sin interrupciones, de servicios de calidad.

Actualmente la creación de valor, ya sea en tecnología, marketing o fabricación, se está volviendo tan complejo que un solo departamento o compañía no esta en disposición de poder dominarlo en solitario.

Esta situación está llevando a las organizaciones, que buscan mejorar su rendimiento, a considerar que competencias son esenciales para su negocio, potenciándolas internamente y ampliando sus capacidades mediante socios tanto en actividades internas como externas.

Este proceso da cobertura a la gestión de suministradores mediante los controles necesarios para normalizar y acordar con todas las partes los acuerdos de servicio alineados con los SLAs establecidos con los clientes. También contempla el comportamiento de estos acuerdos de servicio mediante la monitorización y revisión de las prestaciones obtenidas frente a los objetivos establecidos, identificando y proponiendo acciones de mejora.

Para finalizar es importante destacar que este proceso no contempla la selección de suministradores al considerar que es una actividad previa, fuera del ámbito de las actividades de gestión.

Para cubrir este objetivo la norma establece 15 requisitos de control a cumplir.

- **Procesos de Resolución.** Los procesos de resolución son gestión del incidente y gestión del problema; estos procesos tienen un alto grado de relación aunque tienen objetivos diferenciados.

Gestión del incidente se encarga de la recuperación de los servicios a los usuarios tan pronto como sea posible, y gestión del problema tiene la misión de identificar y eliminar las causas de los incidentes para que no vuelvan a producirse.

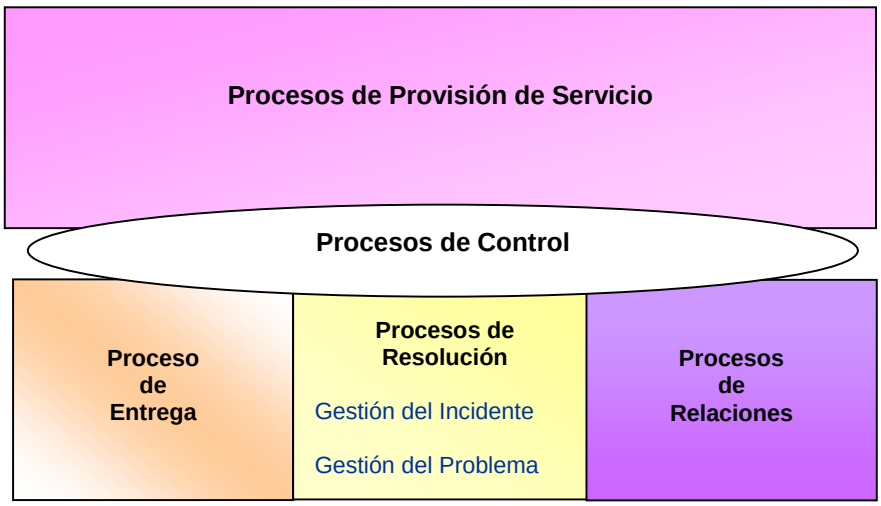


Figura 9. Procesos de Resolución

9. **Gestión del Incidente.** El objetivo de este proceso es restaurar el servicio acordado con el negocio tan pronto como sea posible o responder a peticiones de servicio.

Para conseguir el objetivo es necesario tratar de forma adecuada los sucesos que provocan la degradación o pérdida del funcionamiento normal de un servicio, priorizando la atención de las incidencias de acuerdo a los compromisos de servicio establecidos, y reduciendo el impacto provocado gracias a una resolución oportuna.

Para cubrir este objetivo la norma establece 9 requisitos de control a cumplir.

10. **Gestión del Problema.** El objetivo de este proceso es minimizar los efectos negativos sobre el negocio de las interrupciones del servicio, mediante la identificación y el análisis reactivo y proactivo de la causa de los incidentes y la gestión de los problemas para su cierre.

Uno de los aspectos más relevantes de este proceso es identificar la causa raíz de los fallos que ocurren o que potencialmente pueden ocurrir, al objeto de asegurar la estabilidad de los servicios, y que los problemas no ocurran o se vuelvan a repetir.

Gracias a su correcta implantación es posible mejorar la calidad global de los servicios TI, estabilizar el entorno de producción manteniendo el funcionamiento normal del negocio y acometer proyectos de mejora que permitan erradicar fallos en el servicio.

Para cubrir este objetivo la norma establece 9 requisitos de control a cumplir.

- **Procesos de Control.** La gestión de la configuración y del cambio son dos procesos sobre los que pivotan el resto de procesos de la gestión del servicio TI, gracias a ellos el proveedor de servicios puede controlar adecuadamente los cambios que se producen en los componentes del servicio y la infraestructura que los soporta, y disponer de una base de información precisa y actualizada de la configuración, elemento indispensable para la toma de decisiones de todos los procesos, incluido gestión del cambio.

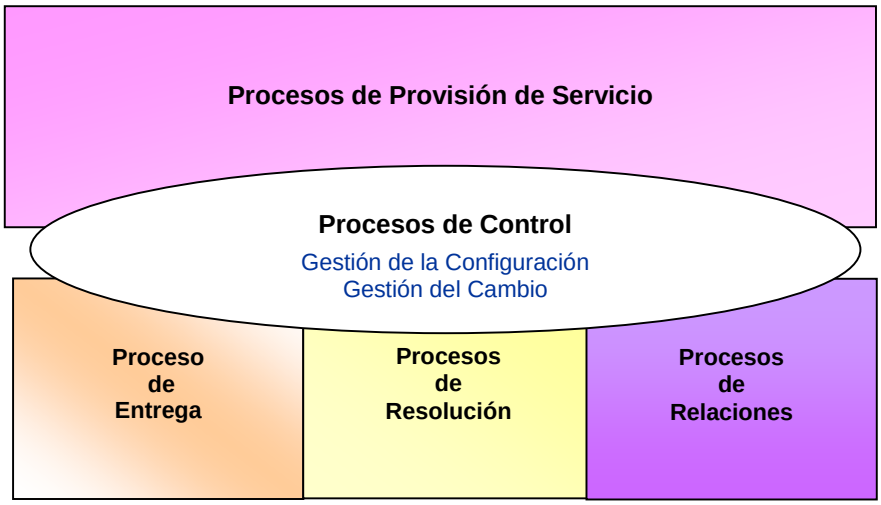


Figura 10. Procesos de Control

11. **Gestión de la Configuración.** El objetivo de este proceso es definir y controla los componentes del servicio y de la infraestructura, manteniendo información precisa y actualizada sobre la configuración.

Este proceso se ocupa de la identificación, control y verificación de los Elementos de Configuración (CI - *Configuration Item*) que componen un servicio, registrando su estado y dando información para el apoyo al resto de los procesos de Gestión de TI. Por lo

tanto, gestión de la configuración es el proceso que garantiza que la información necesaria para la adecuada gestión de los servicios TI esta correctamente registrada y administrada.

Para cubrir este objetivo la norma establece 15 requisitos de control a cumplir.

12. **Gestión del Cambio.** El objetivo de este proceso es asegurar que todos los cambios son evaluados, aprobados, implementados y revisados de una manera controlada.

Este proceso controla los cambios de forma eficiente de acuerdo con los compromisos de servicio y con el mínimo impacto en el entorno de producción. Par ello implanta una gestión integral de los cambios proporcionando una visión conjunta que facilita el análisis de los riesgos y la toma de medidas adecuadas para garantizar el éxito de los cambios y minimizar su impacto negativo en el negocio de los clientes.

Para cubrir este objetivo la norma establece 13 requisitos de control a cumplir.

- **Procesos de Entrega**

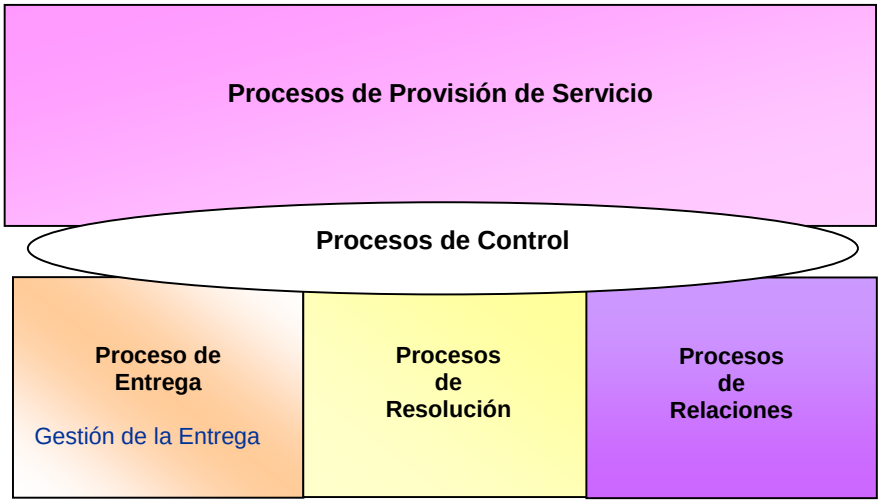


Figura 11. Procesos de Entrega

- **Gestión de la Entrega.** El objetivo de este proceso es entregar, distribuir y realizar el seguimiento de uno o más cambios en la entrega en el entorno de producción real.

Gestión de la entrega realiza la planificación y gestión de los recursos que permite distribuir correctamente un lanzamiento al cliente. Para realizar con éxito esta tarea, este proceso tiene una visión global de los servicios, con lo que se garantiza que todos los aspectos que afecten a las entregas, tanto técnicos como no técnicos, se analizan y tratan globalmente.

Para cubrir este objetivo la norma establece 16 objetivos de control a cumplir.

En la imagen siguiente se incluye un resumen de lo tratado en este apartado, y para finalizar es importante resaltar que los requisitos de control ISO/IEC 20000 son totalmente

prácticos y orientados a "hacer" aquellas actividades que son claves en una gestión de servicios TI de alta calidad.

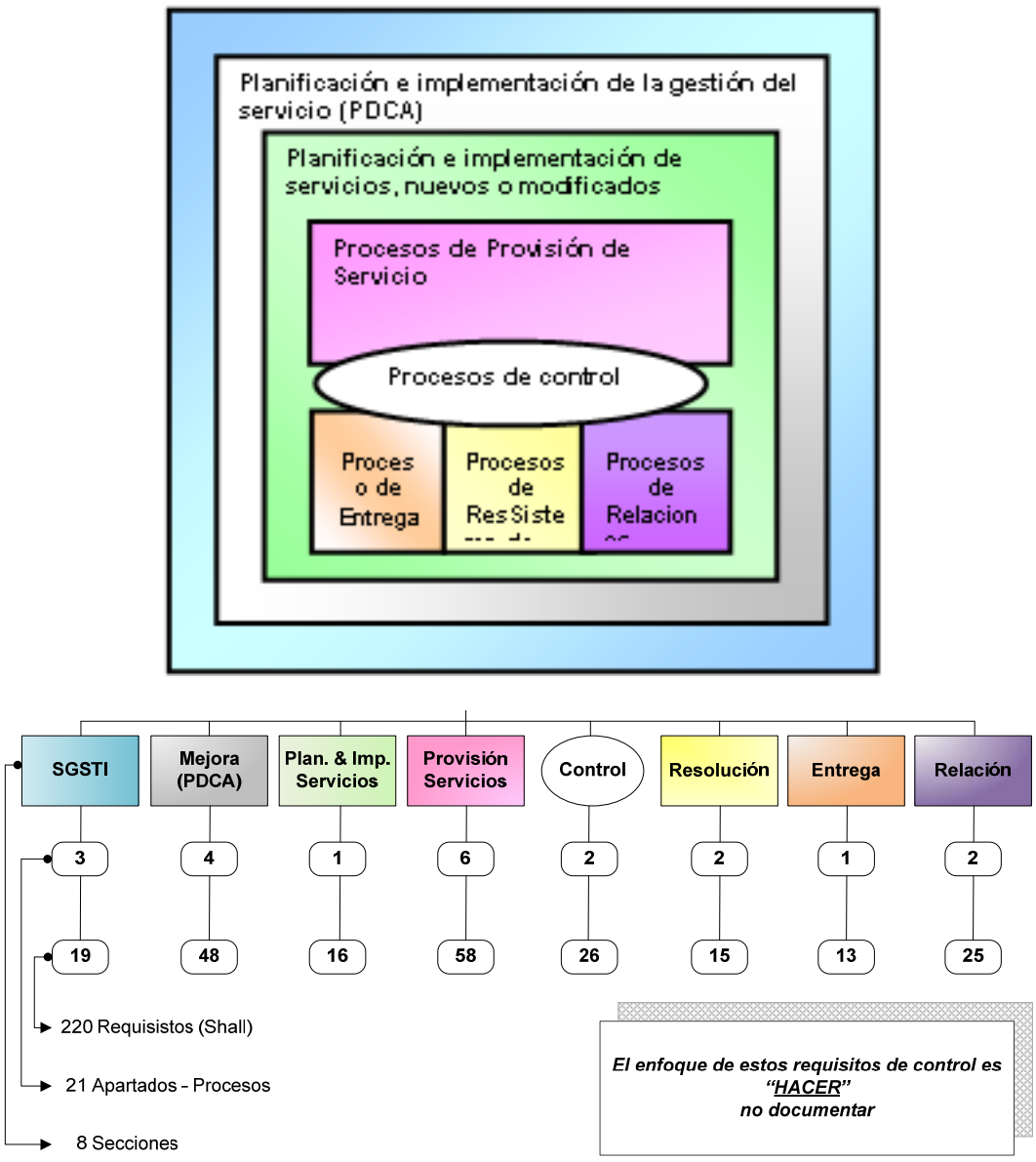


Figura 12. Requisitos de Control de ISO/IEC 20000-1

Seguidamente se aportan algunos ejemplos extraídos de la norma:

- La implementación de nuevos servicios o modificaciones en los existentes, incluyendo la eliminación de un servicio, debe ser planificada y aprobada a través de un proceso formal de gestión del cambio (Planificación e Implementación de Servicios, nuevos o modificados).

- Los SLAs se deben revisar periódicamente por las partes, para asegurar que se encuentran actualizados y continúan siendo eficaces con el transcurso del tiempo.

- El proveedor del servicio y los clientes se deben reunir, al menos una vez al año, para la revisión del servicio y para discutir cualquier cambio en el alcance del mismo, en el SLA, en el contrato (si existe) o en las necesidades del negocio. (Gestión de las relaciones con el negocio).

ANEXO 2. Seguridad.

La Seguridad Informática y sus componentes

En diversas iniciativas internacionales, incluidas las emprendidas por la organización ISO con sus guías, se han clarificado los componentes fundamentales de la seguridad desde la perspectiva de la modelización. Así se distinguen: los activos, las amenazas, las vulnerabilidades, los impactos y las salvaguardas.

Los **activos** son los recursos del SI o relacionados con éste, necesarios para que la organización opere correctamente y alcance los objetivos propuestos por su dirección. Los activos se podrán agrupar y jerarquizar en función de su composición y estarán relacionados entre sí por el riesgo al que están expuestos. Las características a retener de cada activo son: su código, descripción, precio unitario, coste de reposición, tiempo máximo de carencia, nivel de mantenimiento de la integridad y el nivel de confidencialidad. Los activos pueden ser físicos o lógicos, tangibles o intangibles y se pueden encuadrar en: las personas, el centro de datos y las instalaciones, los ordenadores centrales, el software de base, los ordenadores departamentales y personales, y la informática de usuario final, incluyendo un posible centro de información, la producción y las aplicaciones que se procesan, el desarrollo de dichas aplicaciones, los datos y las bases de datos, las comunicaciones y la documentación.

Las **vulnerabilidades** son las debilidades de los activos de la organización, las cuales podrían ser utilizadas por las amenazas para causar daño al sistema. La vulnerabilidad está ligada a la organización (procedimientos inadaptados, dejadez,…) a las personas (cansancio, falta de sensibilización,…) a los equipos, al entorno (accesibilidad a los locales, mala localización, escasa protección contra incendios, intrusión,…).

El **impacto** es la medida del daño producido a la organización por un incidente posible. Se centra sobre los activos y por tanto puede medirse económicamente.

El **riesgo** es la probabilidad subjetiva de que se produzca un impacto dado en la organización una vez materializada una amenaza debido a la vulnerabilidad de un activo. El riesgo residual es le riesgo remanente una vez tenidas en cuenta las salvaguardas a aplicar.

Una **salvaguarda** es todo dispositivo, físico o lógico, capaz de reducir el riesgo. Las salvaguardas, según su naturaleza, pueden clasificarse en:

- Preventivas: procedimientos organizativos y medidas técnicas tendentes a impedir que las amenazas se materialicen. Actúan principalmente sobre la vulnerabilidad, reduciendo por tanto su riesgo.
- Protectoras o curativas: medidas técnicas y organizativas que tienen por objeto limitar las consecuencias de una amenaza una vez materializada, es decir, limitar el impacto.

A continuación se presenta una figura que refleja las relaciones entre todos estos componentes:

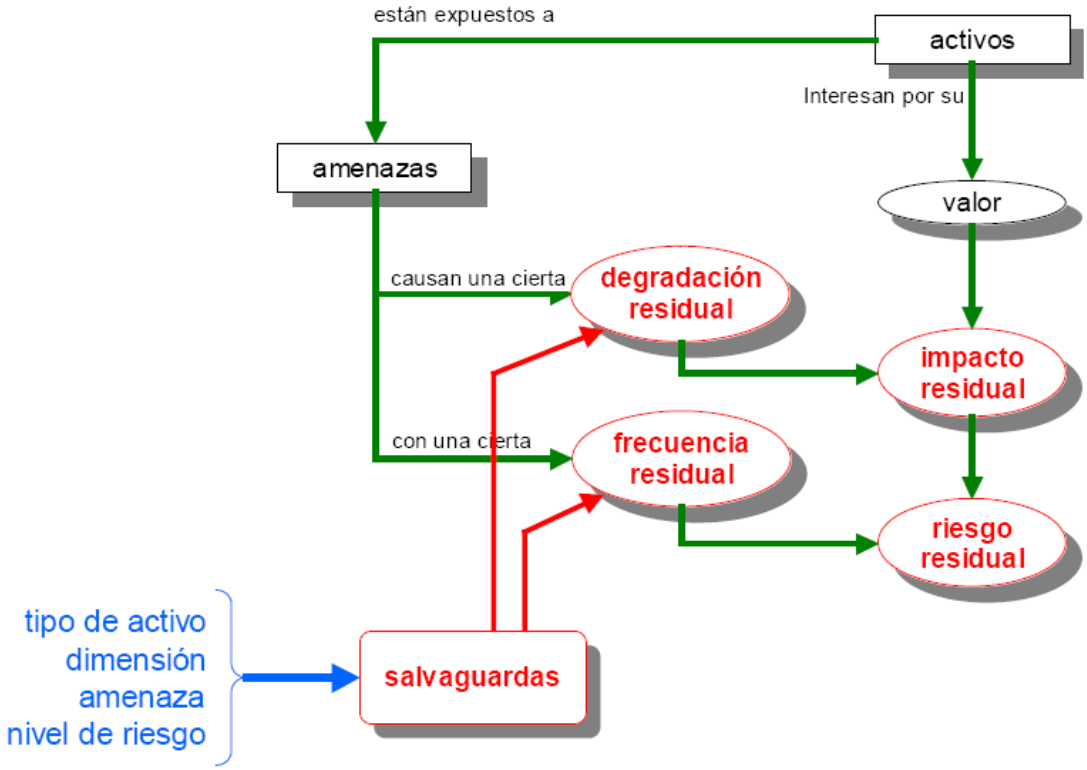


Figura 95.- **Conceptos de seguridad informática.**
(Fuente: Magerit 2.0)

Las **relaciones directas** entre las entidades representadas por los vectores de la figura anterior son:

- Relaciones directas del Activo:
  - Puede ser componente o dependiente de otro activo.
  - Puede tener vulnerabilidades respecto de diversas amenazas.

- Pueden estar afectado por impactos acumulables procedentes de diversas amenazas.
- Puede estar protegido por un mecanismo de salvaguarda.

- Relaciones directas de la Amenaza (si se materializa):
  - Puede ser componente o dependiente de otra amenaza.
  - Ha de explotar una vulnerabilidad para afectar a un activo.
  - Puede causar un impacto sobre el activo.

- Relaciones directas de la Vulnerabilidad:
  - Debe relacionarse con un activo.
  - Puede ser explotada por una amenaza para materializarse en agresión.
  - Puede ser afectada por una función o un servicio de salvaguarda.
  - Contribuye al riesgo.

- Relaciones directas del Impacto:
  - Debe relacionarse con un activo.
  - Puede causarlo la materialización de una amenaza.
  - Puede ser afectado por una función o un servicio de salvaguarda.
  - Contribuye al riesgo.

- Relaciones directas del Riesgo:
  - Se refiere a la vulnerabilidad de un activo respecto a una amenaza.

- Se refiere al impacto propiciado por la vulnerabilidad de un activo.
- Puede relacionarse con una función o un servicio de salvaguarda.

- Relaciones directas de la Salvaguarda:
  - Está relacionado con un riesgo.
  - Puede afectar al impacto de una amenaza.
  - Puede afectar a la vulnerabilidad de una amenaza.
  - Protege un activo.

Objetos a proteger

Se debe identificar cuáles son los objetos esenciales que se deben proteger en un SI. Estos son:

- Hardware

  Este objeto engloba a todos los elementos físicos del sistema.

- Software

  El software engloba a todos los programas lógicos que determinan cómo debe comportarse el hardware.

- Datos

  Los datos engloban la información que manipula tanto el hardware como el software.

Tipos de amenazas

A continuación se presenta el concepto de amenaza contra los objetos de un sistema de información, así como los tipos de amenazas más extendidos.

En términos generales, una amenaza es una acción o evento que puede atentar contra la seguridad de los objetos de un sistema. Las amenazas son los eventos que pueden desencadenar un incidente en la organización, produciendo daños y pérdidas inmateriales en sus activos. Se pueden agrupar en clases y los atributos a tener en cuenta son: su código, nombre, frecuencia (habitualmente subjetiva). Principalmente se distinguen dos tipos básicos de amenazas:

• Amenazas no intencionadas.
• Amenazas intencionadas.

Donde las *amenazas no intencionadas* o *incidentes de seguridad* son provocadas por usuarios autorizados que, por negligencia o falta de conocimiento, no aplican las políticas de seguridad (más adelante se hablará de qué es una Política de Seguridad) establecidas para el correcto funcionamiento del sistema.

Sin embargo, las *amenazas intencionadas* o *ataques* son provocadas por usuarios no autorizados que acceden conscientemente de forma indebida a los objetos del sistema.

A su vez, los *ataques* se clasifican atendiendo a diferentes criterios. En función de si el objetivo final del ataque es vulnerar de forma directa o indirecta un determinado objeto, se definen las siguientes categorías:

• Ataques directos.
• Ataques indirectos.

Donde un *ataque directo* tiene como objetivo vulnerar un determinado objeto aunque para ello pueda ser necesario comprometer una serie de objetos intermedios. Sin embargo, un *ataque indirecto* tiene como objetivo extraer información de un objeto sin atacar al objeto en sí mismo.

Los ataques indirectos son especialmente conflictivos en las bases de datos, donde es posible hacer preguntas indirectas sobre un objeto y derivar información confidencial a partir de las respuestas obtenidas. Este caso particular de ataque indirecto se denomina *inferencia*.

Además, en función de si el ataque modifica o no el comportamiento normal del sistema, se definen las siguientes categorías:

• Ataques pasivos.
• Ataques activos.

Donde un *ataque pasivo* monitoriza el comportamiento normal de un sistema sin modificarlo, con el propósito de recopilar información. Este tipo de ataques resulta muy difícil de detectar, ya que no altera el funcionamiento normal del sistema.

Sin embargo, un *ataque activo* sí modifica el comportamiento normal del sistema en alguna medida. Como por ejemplo, insertando, modificando o eliminando mensajes en la red con el propósito de abusar deliberadamente del sistema. Este tipo de ataques son más fáciles de detectar que los ataques pasivos.

Efectos de una amenaza

Los efectos principales que una amenaza puede provocar sobre los objetos de un SI son los siguientes:

• *Interrupción*

Este efecto se produce cuando se interrumpe temporalmente o permanentemente la funcionalidad de un objeto.

• *Interceptación*

Se produce una interceptación cuando una entidad[161] no autorizada consigue acceso a un determinado objeto.

• *Modificación*

[161] Una entidad se define como un proceso o usuario del sistema.

Se produce una modificación cuando un objeto es interceptado y modificado, en parte o en su totalidad, por una entidad malintencionada. La *destrucción* de un objeto se considera un caso particular de modificación.

• *Fabricación o generación*

Se produce una fabricación cuando una entidad malintencionada añade información parcial a un objeto o introduce nuevos objetos en el sistema.

Agentes amenazantes

En este apartado se presentan los agentes amenazantes de los que debe protegerse un sistema de información. Esencialmente se distinguen los siguientes agentes:

• *Personas.*
• *Amenazas lógicas.*
• *Catástrofes.*

A continuación se presentan cada unos de los agentes amenazantes citados:

Personas

Existe una gran diversidad de personas que pueden constituir un riesgo para la seguridad de un sistema de información. A continuación se presentan las principales

categorías de atacantes de un sistema de información que James P. Anderson presentó en 1980 y aún hoy sirven de referencia:

• *Impostor*

Un impostor es un usuario de acceso no autorizado al sistema que vulnera el control de acceso para explotar una cuenta de usuario legítimo. Habitualmente este tipo de atacante es una persona ajena al sistema de información.

• *Malhechor*

Un malhechor es un usuario legítimo que accede a datos, software o recursos del sistema para los cuales no tiene permitido el acceso.

• *Usuario clandestino*

Un usuario clandestino es el que adquiere control del sistema con privilegios de supervisor y lo utiliza para evadir o eliminar los controles de acceso al sistema. Este tipo de atacante puede ser tanto un usuario legítimo como un usuario ajeno al sistema.

Amenazas lógicas

Además de los ataques en los que existe una actuación directa del intruso, también existe una gran variedad de amenazas lógicas automáticas, que intentan vulnerar la seguridad de los sistemas sin necesidad de supervisión humana. Las amenazas lógicas pueden clasificarse en dos categorías esenciales:

• *Malware.*

• *Errores de programación.*

A continuación se introduce cada una de las amenazas lógicas citadas:

Malware

No todos los problemas de seguridad proceden de errores o descuidos en la programación. Existe una amplia gama de amenazas lógicas creadas expresamente con intenciones maliciosas. A estos programas, cuyo propósito es atacar la seguridad de un sistema, se les denomina ***malware*** o ***mal****icious soft****ware***.

Sin embargo, en ocasiones resulta difícil determinar si un programa fue creado originalmente con intenciones maliciosas, o si simplemente se ha abusado de su legítima funcionalidad. Por tanto, dentro de la categoría de *malware*, también se puede incluir aquellos programas que no fueron creados con fines maliciosos pero que un uso indebido los convierte en una amenaza potencial.

Error de programación

En el concepto de amenaza lógica se engloba una amplia variedad de software que puede vulnerar un sistema de información, bien de forma intencionada, como es el caso del *malware*, o bien como resultado de un error de programación.

Si bien en los últimos diez años se ha depurado la seguridad de los nuevos desarrollos y se ha conseguido reducir los errores de programas y servicios existentes, los errores de programación siguen siendo una amenaza importante en la actualidad.

Catástrofes

Las catástrofes naturales, si bien pueden resultar devastadores, representan un riesgo menos probable para la seguridad de un sistema de información que las personas y las amenazas lógicas.

Tipos de seguridad

Como ya se ha comentado con anterioridad, la seguridad es un concepto amplio y difícil de abordar desde una única perspectiva. Por tanto, habitualmente la seguridad de los sistemas de información se divide en tres tipos:

- *Seguridad física.*
- *Seguridad lógica.*
- *Seguridad administrativa.*
- *Seguridad jurídica.*

La *seguridad física* tiene como objetivo proteger el sistema de información contra amenazas físicas naturales (terremotos, inundaciones, incendios) y humanas (robos, atentados).

Para alcanzar dicho objetivo, la seguridad física trata de establecer y mantener un entorno suficientemente seguro para la manipulación y almacenamiento de los objetos sensibles del sistema.

Por otra parte, la *seguridad lógica* tiene como objetivo proteger el software y los datos del sistema de información contar amenazas lógicas y personas con intenciones maliciosas.

Sin embargo, la *seguridad administrativa* tiene como objetivo proteger los objetos del sistema de información proporcionando mecanismos de seguridad que intentan minimizar los efectos de una potencial amenaza. Los mecanismos de seguridad administrativa más extendidos son: políticas de seguridad, políticas de personal, políticas de contratación, análisis de riesgos y planes de contingencia.

Finalmente, la *seguridad jurídica* tiene como objetivo fijar el marco jurídico adecuado para proteger los sistemas de información.

Mecanismos de seguridad

Para poder definir los mecanismos de seguridad adecuados para proteger un sistema de información es necesario realizar un análisis detallado de las potenciales amenazas a las que se expone el sistema. En base a dicho análisis se define una política de seguridad

adecuada, para cuya implementación se pueden utilizar diferentes mecanismos de seguridad.

Los mecanismos de seguridad se dividen en tres categorías:

• *Prevención.*

• *Detección.*

• *Recuperación.*

A continuación se estudia cada una de las categorías citadas.

Mecanismos de prevención

Los mecanismos de prevención se encargan de reforzar la seguridad del sistema evitando posibles ataques. Los mecanismos de prevención más utilizados son:

• *Mecanismos de autentificación*

Los mecanismos de autenticación permiten identificar las entidades legítimas del sistema.

• *Mecanismos de control de acceso*

Los mecanismos de control de acceso permiten controlar la forma en que las entidades acceden a los objetos del sistema.

• *Mecanismos de separación*

Los mecanismos de separación permiten definir y organizar los objetos en múltiples niveles de seguridad.

• *Mecanismos de seguridad en la comunicación*

Estos mecanismos tratan de preservar la integridad y la confidencialidad de los objetos que se transfieren entre varias máquinas.

Mecanismos de detección

Los mecanismos de detección se encargan de detectar los potenciales ataques del sistema mientras éstos se están produciendo. Habitualmente estos mecanismo proporcionando información necesaria para la inmediata detención de los ataques.

De entre los mecanismos de detección, en esta tesis se estudiará en detalle los IDS[162].

Mecanismos de recuperación

Los mecanismos de recuperación se encargan de restablecer el sistema vulnerado al estado anterior a la consumación del ataque.

[162] *Intrusion Detection System.*

Los mecanismos de recuperación más utilizados son las copias de seguridad. No obstante, dentro de ésta categoría se engloba el análisis forense que permite analizar el comportamiento monitorizado del intruso, para , tras un estudio detallado, conseguir identificar las vulnerabilidades explotadas en el sistema y establecer la medida correctiva más adecuada.

El coste de la seguridad

La seguridad informática se establece como un equilibrio entre la necesaria operatividad del sistema (correcto funcionamiento de los activos) frente a los diversos riesgos potenciales y las diferentes salvaguardas que permiten minimizar la probabilidad de aparición de incidentes o reducir sus efectos, es decir, minimizar el riesgo.

Las salvaguardas y su implantación implican un coste (directo e indirecto) para el funcionamiento del sistema, que permite y recomienda considerar a la seguridad informática como un problema de carácter económico, en el que se tratan de alcanzar unos objetivos o resultados determinados mediante la asignación eficiente de unos recursos que tienen su coste. La seguridad de un SI debe ser, por tanto, cuidadosamente planificada y presupuestada, determinándose los niveles aceptables de seguridad para la organización y su coste, así como los medios más idóneos para conseguirlos.

Se trata, para ello, de encontrar un punto de equilibrio entre las técnicas y procedimientos a emplear y su coste, frente a los beneficios que a partir de estas medidas se pueden derivar. Es necesario tratar de cuantificar dos tipos de magnitudes:

- Por un lado, los daños que se pueden ocasionar en el sistema y una estimación de los costes derivados de dichos daños.
- Por otro, los costes de implantación y mantenimiento de las medidas apropiadas para su contención.

El presupuesto a invertir en seguridad dependerá de lo crítico de la información que maneje y de los recursos que pueda o quiera asignar la Dirección para su protección.

En la actualidad existen diversas organizaciones encargadas de estudiar y analizar el incremento anual de los delitos informáticos y las pérdidas económicas asociadas a éstos.

Algunas de las principales organizaciones especializadas en ayudar y formar a los profesionales de la seguridad de la información son: el CSI[163], la ISSA[164] o el MISTI[165].

En el informe "*2004 CDI/FBI Computer Crime and Security Survey*" elaborado por el CSI en colaboración con el FBI (*Federal Bureau of Investigation)* se proporcionaron una serie de valores. Estos valores se basaban en los resultados recopilados de 530 organizaciones americanas, entre las cuales se encuentran agencias gubernamentales,

[163] El CSI (*Computer Security Institute*) fue fundado en 1974. En la actualidad, el CSI proporciona seminarios educativos sobre cifrado, control de intrusiones, seguridad en Internet, entre otros. Esta organización esponsoriza dos conferencias y exposiciones anuales, "NetSec" en junio, y el "*CSI Annual Computer Security Conference and Exhibition*" en noviembre. Para más información consultar [RefWeb-17].

[164] La ISSA (*Information Systems Security Association*) fue fundada en 1982. ISSA es una organización internacional sin ánimo de lucro, orientada a la formación de profesionales y practicantes de la seguridad de la información. El principal objetivo de ISSA es promover normas de gestión, que aseguren confidencialidad, integridad y la disponibilidad de los recursos de una organización. Para más información consultar [RefWeb-19].

[165] El MISTI (*MIS Training Institute*) fue fundado en 1978. MISTI es la principal organización internacional orientada a la formación de profesionales en las área de auditoría y seguridad de la información. En la actualidad, el MISTI opera en cinco continentes, presenta seminarios y conferencias sobre auditorías internas, seguridad de la información, TCP/IP, aplicaciones de *e-commerce*, entre otros. Para más información consultar [RefWeb-18].

instituciones financieras, instituciones médicas y universidades. Los resultados publicados confirmaron por séptimo año consecutivo que la amenaza de los crímenes informáticos no disminuía y además, las pérdidas económicas derivadas de éstos seguían aumentado.

Dos años más tarde (en 2006) los datos que reflejaba el informe "*CDI/FBI Computer Crime and Security Survey"*[166] no eran alentadores:

"Los ataques por virus continúan siendo el origen de las mayores pérdidas económicas. Los accesos no autorizados son la segunda razón. Pérdidas económicas relacionadas con portátiles (o hardware móvil) y hurtos del a propiedad de la información (por ej. la propiedad intelectual) son la tercera y la cuarta causa respectivamente. Estas cuatro categorías conllevan el 74% del total de las pérdidas económicas".[167]

Alguna otra información que se arroja de dicho informe es la que sigue:

"El porcentaje de organizaciones que sufren intrusiones en sus equipos informáticos sube del 20 al 25%".

Como puede observarse, nada en estos últimos 4 años ha hecho cambiar estos datos.

[166] http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf.
[167] Traducción propia.

En cuanto a la Unión Europea, en base a los indicadores presentados en el estudio "*Métrica de la Sociedad de la Información*"[168] del año 2006, elaborado por el Ministerio de Ciencia y Tecnología y SEDISI[169], el 52% de los usuarios de Internet manifestaron haber experimentado problemas de seguridad durante el año 2005. En particular, en España, el 25% de los usuarios de Internet manifestaron haber sufrido algún problema de seguridad.

Función del coste de la seguridad

Si bien se ha aseverado que no existe ningún sistema absolutamente seguro, se puede medir la seguridad de cualquier sistema de información en una escala de valores continuos definidos en el intervalo del 0 al 1; donde el valor "0**"** representa un sistema completamente "inseguro", en el que cualquier atacante podría vulnerar dicho sistema fácilmente; y, el valor "1**"** representa un sistema "seguro", en el que un atacante necesitaría invertir una cantidad excesiva de tiempo, dinero y recursos para vulnerar dicho sistema.

El *coste de la seguridad* se define en función de una combinación de diversos costes parciales. Los costes parciales que se deben contemplar son:

• Coste del decremento del rendimiento del sistema.

• Coste del incremento de la complejidad en el sistema.

• Coste del decremento de la usabilidad del sistema.

• Coste del incremento de operación.

[168] Para más información sobre el estudio de "Métrica de la Sociedad de la Información" consultar [SED02], [SED03] y [Ref Web 23].
[169] Para más información sobre SEDISI, actualmente AETIC (Asociación de Empresas de Electrónica, Tecnologías de la Información y Telecomunicaciones de España) consultar [Ref Web 24].

• Coste del incremento del mantenimiento.

• Costes intangibles de imagen y prestigio.

Estos costes están estrechamente relacionados entre si. Por ejemplo, es posible incrementar el grado de seguridad de un sistema, eliminando parte de la funcionalidad del sistema y agregando el coste asociado por el decremento de la usabilidad.

El coste total de la seguridad de un sistema está directamente relacionado con el grado de seguridad proporcionado. Es más, en la mayoría de los sistemas de información el coste de la seguridad crece de forma exponencial a medida que el grado de seguridad se aproxima al 100%.

En la figura 101 se muestra una aproximación de la función del coste de la seguridad de un sistema de información:

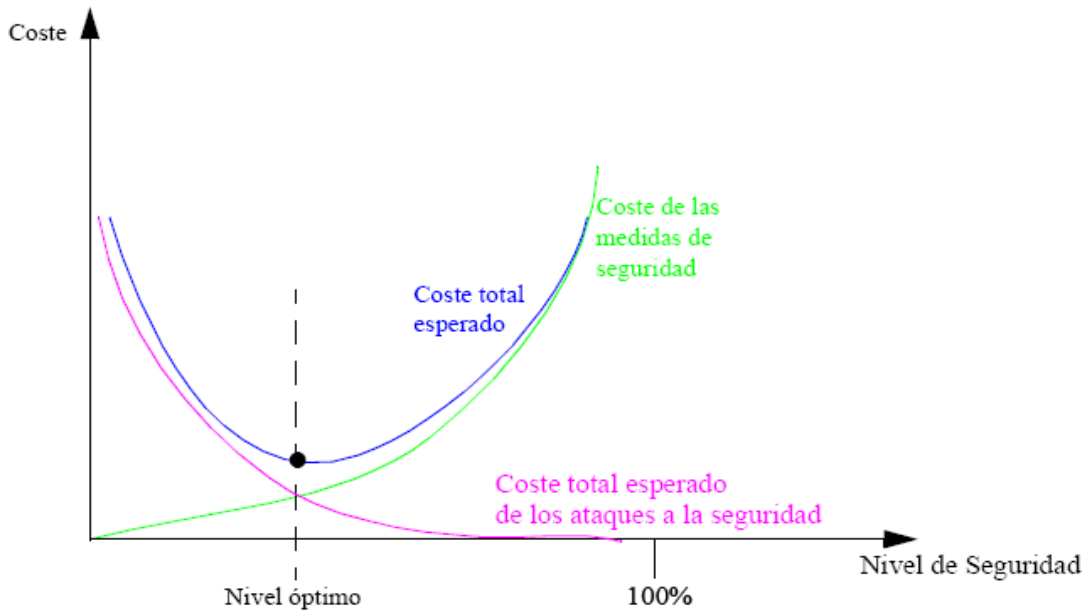


Figura 96.- **Coste de la seguridad.**

En esta aproximación, el coste total esperado de los ataques a la seguridad se calcula en función del coste de un único ataque de seguridad multiplicado por la frecuencia de ataques. Éste es un coste difícil de estimar.

Finalmente, el nivel óptimo de seguridad se define como el punto de corte entre el coste de los mecanismos de seguridad y el coste total esperado de los ataques a la seguridad, proyectado sobre la curva del coste total esperado.

ANEXO 3. Ciclos de Vida

Ciclo de vida en V

Propuesto por Alan Davis, tiene las mismas fases que el ciclo de vida en cascada tradicional, pero tiene en consideración el nivel de abstracción de cada una.

Una fase además de utilizarse como entrada para la siguiente, sirve para validar o verificar otras fases posteriores. Su estructura está representada en la figura 102.

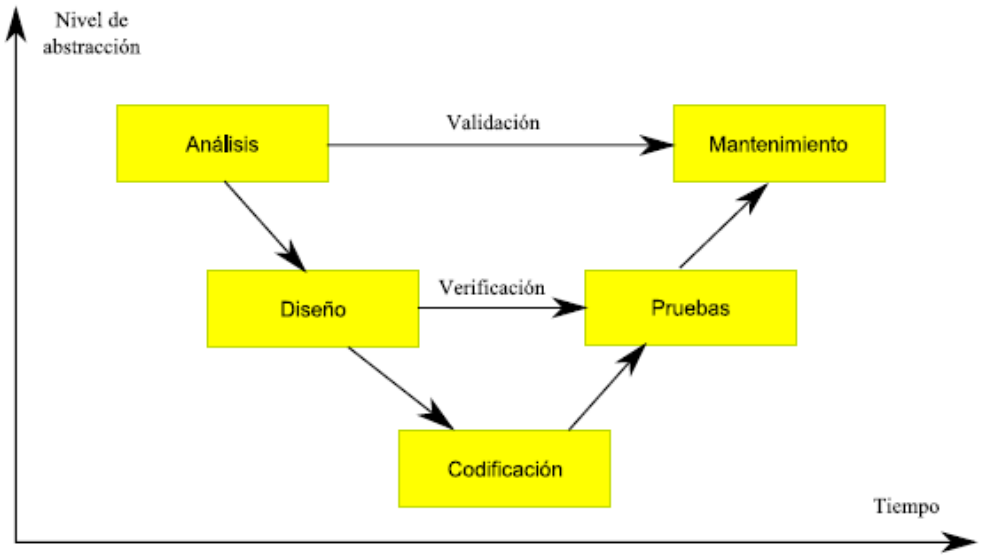


Figura 97.- **Ciclo de vida en V.**

Ciclo de vida tipo *sashimi*

Según el modelo en cascada puro una fase sólo puede empezar cuando ha terminado la anterior. En este caso, sin embargo, se permite un solapamiento entre fases. Por ejemplo, sin tener terminado del todo el diseño se comienza a implementar.

El nombre *sashimi* deriva del estilo de presentación en rodajas de pescado crudo en Japón.

Una ventaja de este modelo es que no necesita generar tanta documentación como el ciclo de vida en cascada puro, debido a la continuidad del mismo personal entre fases.

Los problemas planteados son:

- Es aún más difícil controlar el progreso del proyecto debido a que los finales de fase ya no son un punto de referencia claro.

- Al hacer cosas en paralelo, si hay problemas de comunicación pueden surgir inconsistencias.

La fase de "concepto" consiste en definir los objetivos del proyecto, beneficios, tipo de tecnología y tipo de ciclo de vida. El diseño arquitectónico es el de alto nivel, el detallado el de bajo nivel.

En la figura 103 se ha representado la estructura del ciclo de vida *sashimi*.

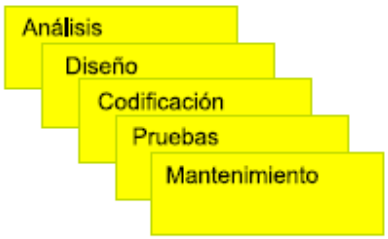


Figura 98.- **Ciclo de vida *sashimi*.**

Ciclo de vida en cascada con subproyectos

Si una vez que se ha llegado al diseño arquitectónico, se comprueba que el sistema se divide en varios subsistemas independientes entre sí, sería razonable suponer que a partir de ese punto, cada uno se puede desarrollar por separado y en consecuencia en paralelo con los demás. Cada uno tendrá seguramente fechas de terminación distintas. Una vez que han terminado todos se integran y se prueba el sistema en su conjunto.

La ventaja es que se puede tener a más gente trabajando en paralelo de forma eficiente.

El riesgo es que existan interdependencias entre los subproyectos.

Ciclo de vida en cascada incremental

En este caso se va creando el sistema añadiendo pequeñas funcionalidades. Cada uno de los pequeños incrementos es comparable a las modificaciones que ocurren dentro de la fase de mantenimiento.

La ventaja de este método es que no es necesario tener todos los requisitos desde el principio.

El inconveniente es que los errores en la detección de requisitos se encuentran tarde.

Hay dos partes en este tipo de ciclo de vida que lo hacen similar al ciclo de vida tipo *sashimi*. Por un lado están el análisis y el diseño global. Por otro lado están los pequeños incrementos que se llevan a cabo en las fases de diseño detallado, codificación y mantenimiento.

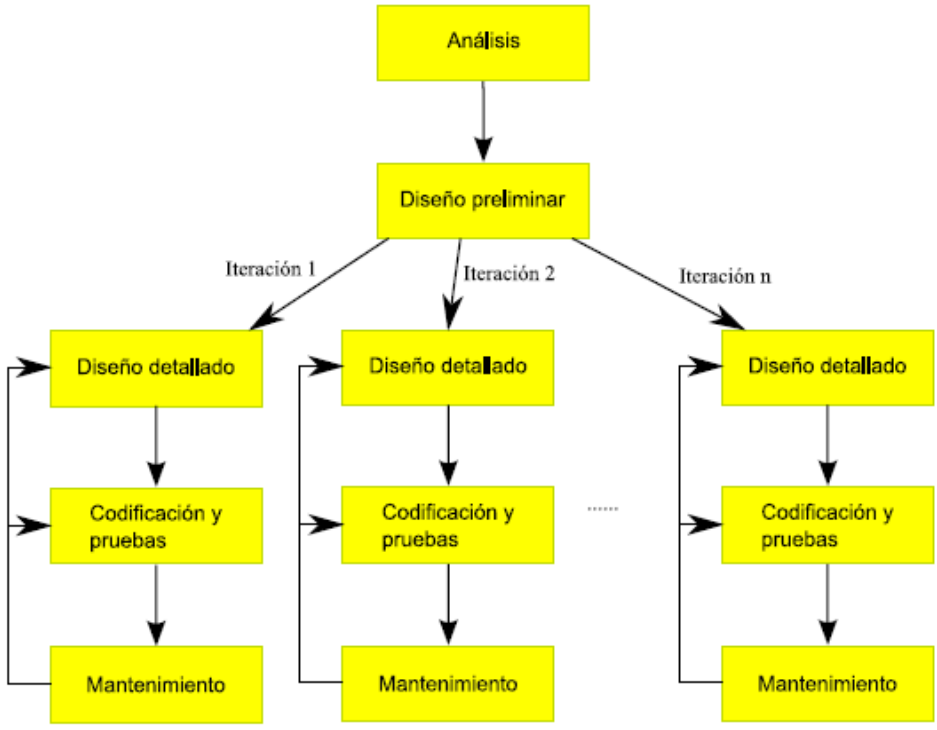


Figura 99.- **Ciclo de vida en cascada incremental.**

Ciclo de vida en cascada con reducción de riesgos

Como se ha comentado anteriormente, uno de los problemas del ciclo de vida en cascada es que si se entienden mal los requisitos esto sólo se descubrirá cuando se entregue el producto. Para evitar este problema se puede hacer un desarrollo iterativo durante las fases de análisis y diseño global. Esto consistiría en:

1. Preguntar al usuario.
2. Hacer el diseño global que se desprende del punto 1.
3. Hacer un prototipo de interfaz de usuario, hacer entrevistas con los usuarios enseñándoles el prototipo y volver con ello al punto 1 para identificar más requisitos o corregir malentendidos.

El resto es igual al ciclo de vida en cascada.

ANEXO 4. Normativa ISO/IEC 27002:2005.

DOMINIOS, OBJETIVOS DE CONTROL Y CONTROLES

A5. Política de seguridad

5.1. Política de seguridad de la información

5.1.1. Documento de política de seguridad de la información

5.1.2. Revisión de la política de seguridad de la información

A6. Aspectos organizativos para la seguridad

6.1. Organización interna

6.1.1. Compromiso de la Dirección con la seguridad de la información

6.1.2. Coordinación de la seguridad de la información

6.1.3. Asignación de responsabilidades relativas a la seguridad de la información

6.1.4. Proceso de autorización de recursos para el procesado de la información

6.1.5. Acuerdos de confidencialidad

6.1.6. Contacto con las autoridades

6.1.7. Contacto con grupos de especial interés

6.1.8. Revisión independiente de la seguridad de la información

6.2. Terceros

6.2.1. Identificación de los riesgos derivados del acceso de terceros

6.2.2. Tratamiento de la seguridad en la relación con los clientes

6.2.3. Tratamiento de la seguridad en contratos con terceros

A7. Clasificación y control de activos

7.1. Responsabilidad sobre los activos

7.1.1. Inventario de activos

7.1.2. Propiedad de los activos

7.1.3. Uso aceptable de los activos

7.2. Clasificación de la información

7.2.1. Directrices de clasificación

7.2.2. Etiquetado y manipulado de la información

A8. Seguridad ligada al personal

8.1. Antes del empleo

8.1.1. Funciones y responsabilidades

8.1.2. Investigación de antecedentes

8.1.3. Términos y condiciones de contratación

8.2. Durante el empleo

8.2.1. Responsabilidades de la dirección

8.2.2. Concienciación, formación y capacitación en seguridad de la información

8.2.3. Proceso disciplinario

8.3. Cese del empleo o cambio de puesto de trabajo

8.3.1. Responsabilidad del cese o cambio

8.3.2. Devolución de activos

8.3.3. Retirada de los derechos de acceso

A9. Seguridad física y del entorno

9.1. Áreas seguras

9.1.1. Perímetro de seguridad física

9.1.2. Controles físicos de entrada

9.1.3. Seguridad de oficinas, despachos e instalaciones

9.1.4. Protección contra las amenazas externas y de origen ambiental

9.1.5. Trabajo en áreas seguras

9.1.6. Áreas de acceso público y de carga y descarga

9.2. Seguridad de los equipos

9.2.1. Emplazamiento y protección de equipos

9.2.2. Instalaciones de suministro

9.2.3. Seguridad de cableado

9.2.4. Mantenimiento de los equipos

9.2.5. Seguridad de los equipos fuera de las instalaciones

9.2.6. Reutilización o retirada segura de equipos

9.2.7. Retirada de materiales propiedad de la empresa

A10. Gestión de comunicaciones y operaciones

10.1. Responsabilidades y procedimientos de operación

10.1.1. Documentación de los procedimientos de operación

10.1.2. Gestión de cambios

10.1.3. Segregación de tareas

10.1.4. Separación de los recursos de desarrollo, prueba y operación

10.2. Gestión de la provisión de servicios por terceros

10.2.1. Provisión de servicios

10.2.2. Supervisión y revisión de los servicios prestados por terceros

10.2.3. Gestión de cambios en los servicios prestados por terceros

10.3. Planificación y aceptación del sistema

10.3.1. Gestión de capacidades

10.3.2. Aceptación del sistema

10.4. Protección contra código malicioso y descargable

10.4.1. Controles contra el código malicioso

10.4.2. Controles contra el código descargado en el cliente

10.5. Copias de seguridad

10.5.1. Copias de seguridad de la información

10.6. Gestión de la seguridad de las redes

10.6.1. Controles de red

10.6.2. Seguridad de los servicios de red

10.7. Manipulación de los soportes

10.7.1. Gestión de soportes extraíbles

10.7.2. Retirada de soportes

10.7.3. Procedimientos de manipulación de la información

10.7.4. Seguridad de la documentación del sistema

10.8. Intercambio de información

10.8.1. Políticas y procedimientos de intercambio de información

10.8.2. Acuerdos de intercambio

10.8.3. Soportes físicos en tránsito

10.8.4. Mensajería electrónica

10.8.5. Sistemas de información empresariales

10.9. Servicios de comercio electrónico

10.9.1. Comercio electrónico

10.9.2. Transacciones en línea

10.9.3. Información puesta a disposición pública

10.10. Supervisión

10.9.4. Registro de auditorías

10.9.5. Supervisión del uso del sistema

10.9.6. Protección de la información de los registros

10.9.7. Registros de administración y operación

10.9.8. Registro de fallos

10.9.9. Sincronización del reloj

A11. Control de accesos

11.1. Requisitos de negocio para el control de acceso

11.1.1. Política de control de acceso

11.2. Gestión de acceso de usuario

11.2.1. Registro de usuario

11.2.2. Gestión de privilegios

11.2.3. Gestión de contraseñas de usuario

11.2.4. Revisión de los derechos de acceso de usuario

11.3. Responsabilidades de usuario

11.3.1. Uso de contraseña

11.3.2. Equipo de usuario desatendido

11.3.3. Política de puesto de trabajo despejado y pantalla limpia

11.4. Control de acceso a la red

11.4.1. Política de uso de los servicios de red

11.4.2. Autenticación de usuario para conexiones externas

11.4.3. Identificación de equipos en las redes

11.4.4. Diagnóstico remoto y protección de los puertos de configuración

11.4.5. Segregación de las redes

11.4.6. Control de la conexión de la red

11.4.7. Control de encaminamiento de red

11.5. Control de acceso al sistema operativo

11.5.1. Procedimientos seguros de inicio de sesión

11.5.2. Identificación y autenticación de usuario

11.5.3. Sistema de gestión de contraseñas

11.5.4. Uso de los recursos del sistema

11.5.5. Desconexión automática de sesión

11.5.6. Limitación del tiempo de conexión

11.6. Control de acceso a las aplicaciones y a la información

11.6.1. Restricción del acceso a la información

11.6.2. Aislamiento de sistemas sensibles

11.7. Ordenadores portátiles y teletrabajo

11.7.1. Ordenadores portátiles y comunicaciones móviles

11.7.2. Teletrabajo

A12. Desarrollo y mantenimiento de sistemas

12.1. Requisitos de seguridad de los sistemas de información

12.1.1. Análisis y especificación de los requisitos de seguridad

12.2. Tratamiento correcto de las aplicaciones

12.2.1. Validación de los datos de entrada

12.2.2. Control de procesamiento interno

12.2.3. Integridad de los mensajes

12.2.4. Validación de los datos de salida

12.3. Controles criptográficos

12.3.1. Política de uso de los controles criptográficos

12.3.2. Gestión de claves

12.4. Seguridad de los archivos de sistema

12.4.1. Control del software en explotación

12.4.2. Protección de los datos de prueba del sistema

12.4.3. Control de acceso al código fuente de los programas

12.5. Seguridad en los procesos de desarrollo y soporte

12.5.1. Procedimientos de control de cambios

12.5.2. Revisión técnica de aplicaciones tras efectuar cambios en el sistema operativo

12.5.3. Restricciones a los cambios en los paquetes de software

12.5.4. Fugas de información

12.5.5. Externalización del desarrollo de software

12.6. Gestión de la vulnerabilidad técnica

12.6.1. Control de las vulnerabilidades técnicas

A13. Gestión de incidentes de seguridad de la información

13.1. Notificación de eventos y puntos débiles de la seguridad de la información

13.1.1. Notificación de los eventos de seguridad de la información

13.1.2. Notificación de puntos débiles de la seguridad

13.2. Gestión de incidentes de seguridad de la información y mejoras

13.2.1. Responsabilidades y procedimientos

13.2.2. Aprendizaje de los incidentes de seguridad de la información

13.2.3. Recopilación de evidencias

A14. Gestión de continuidad de negocio

14.1. Aspectos de seguridad de la información en la gestión de la continuidad del negocio

14.1.1. Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.

14.1.2. Continuidad del negocio y evaluación de riesgos

14.1.3. Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información

14.1.4. Marco de referencia para la reevaluación de planes de continuidad

14.1.5. Pruebas, mantenimiento y reevaluación de planes de continuidad

A15. Cumplimiento

15.1. Cumplimiento de los requisitos legales

15.1.1. Identificación de la legislación aplicable

15.1.2. Derechos de propiedad intelectual (DPI)

15.1.3. Protección de los documentos de la organización

15.1.4. Protección de datos y privacidad de la información personal

15.1.5. Prevención del uso indebido de los recursos de tratamiento de la información

15.1.6. Regulación de los controles criptográficos

15.2. Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico

15.2.1. Cumplimiento de las políticas y normas de seguridad

15.2.2. Comprobación del cumplimiento técnico

15.3. Consideraciones de las auditorías de los sistemas de información

15.3.1. Controles de auditoría de los sistemas de información

15.3.2. Protección de las herramientas de auditoría de los sistemas de información