Tema 1

Administración del Sistema operativo y software de base. Funciones y responsabilidades. Control de cambios de los programas de una instalación.

Guion-resumen

Introducción

Actualmente es imposible imaginar una organización sin sistemas de información. Tampoco es fácil imaginar esos sistemas en forma de máquinas aisladas. Con casi total seguridad se encontrarán conectadas y además, de algún modo, podrán comunicarse con el exterior de la organización, mediante Internet.

Una **infraestructura de sistemas de información** podrá imaginarse como un número de usuarios utilizando diferentes programas y comunicándose unos con otros, compartiendo recursos -desde la impresora hasta la información- y todo ello de forma segura.

Por tanto, se deduce que únicamente con la presencia de la tecnología no es suficiente. Es necesaria una planificación de todos los elementos de la citada infraestructura para garantizar un óptimo rendimiento. Además, es preciso gestionar toda esa infraestructura. La **administración de sistemas** puede definirse como el conjunto de actividades orientadas a configurar y gestionar un conjunto de equipos informáticos en sus aspectos físico y lógico.

Los encargados de la administración de los sistemas informáticos han de prestar atención a numerosos aspectos que influirán en el desempeño de sus funciones: la tecnología, la planificación, los recursos -humanos y económicos-, la seguridad, el perfil de los usuarios y los aspectos legales.

El sistema operativo es la herramienta que permite el funcionamiento de los equipos informáticos. Sirve de interfaz entre el usuario y la máquina. La administración de sistemas no se limita al sistema operativo. Existe todo un conjunto de programas adicionales, que sirven para controlar e interactuar con dicho sistema: se trata del **software de base**, que proporcionará control sobre el hardware y facilitará soporte a otros programas.

En su afán de mejora continua, los fabricantes desarrollan sistemas operativos más sofisticados y complejos. Mucho software de base que solía adquirirse por separado ahora forma parte del sistema operativo por lo que, en ocasiones, es difícil establecer la frontera entre dicho sistema y el software de base. Sensores que controlan la temperatura de los componentes hardware, bibliotecas del sistema gráfico, controladores de dispositivos, gestores de arranque o hipervisores son ejemplos de este software de base que, cada vez más frecuentemente, es proporcionado por el sistema operativo.

Una de las circunstancias que puede hacer más difícil la administración de sistemas es la diversidad de plataformas tecnológicas que pueden encontrarse en una infraestructura, tanto en fabricantes o distribuciones como en versiones. Para reducir la complejidad, la administración tiende a centralizar su actividad, para ganar en homogeneidad, estandarización y control.

Otra modalidad que se ha implantado es la **administración remota**. Permite que muchas organizaciones no estén obligadas a contar con equipos de administradores en sus instalaciones y, a veces, ni siquiera en sus plantillas. La externalización, en inglés *outsourcing,* es una opción más de administración de infraestructuras tecnológicas.

Los sistemas de software cuentan con ciclos de vida, habitualmente largos, durante los cuales varían constantemente las condiciones iniciales así como el entorno de la organización. Se hace obligatorio mantener el software si se desea que los sistemas respondan a los requisitos para los que fueron implantados. Las distintas modificaciones provocan que el software deje de corresponderse con la arquitectura considerada para su desarrollo por lo que cada vez es más complejo entender el sistema. El **control de cambios** resolverá esa circunstancia y ayudará a mantener la integridad del producto software.

Uno de los aspectos que más preocupa a las organizaciones es la seguridad. Asistimos, sin duda, a un momento importante en los aspectos de seguridad de los sistemas de información. Todos los fabricantes están haciendo desde hace años un gran esfuerzo en mejorar los productos que lanzan al mercado. Desde el punto de vista de las organizaciones, sobre todo en las grandes, la gestión de la seguridad de los sistemas se ha convertido en uno de los factores que más recursos precisa. Existe una grandísima variedad de tipos de ataques. Entre ellos, los que consisten en programas que se hacen pasar por otros del sistema o que directamente los modifican para, cuando se ejecuten, cumplir su misión. El control de cambios en los programas de una instalación puede ayudar a detectar estos programas maliciosos antes de que sea demasiado tarde y de que el daño sea muy severo o, incluso, irreparable.

1. Administración del sistema operativo y software de base

La administración del sistema operativo y del software de base consiste en **configurar y gestionar** el sistema. Estas tareas las realiza la figura del **administrador del sistema**. Un administrador conoce el entorno y ofrece la visión técnica de los sistemas de información. Además, debe proporcionar respuesta y solución a las incidencias que se produzcan y que puedan afectar a la funcionalidad de dichos sistemas.

Existe la aceptación casi unánime de denominar **administrador** al perfil de usuario que realiza estas funciones, pero también podemos encontrar la denominación de **superusuario** y también la de ***root***, esta última ceñida a los sistemas operativos basados en Unix o Linux. Se trata de perfiles que cuentan con todos los permisos para operar en un sistema de información, con todo lo que esto puede implicar. Por ello, es muy conveniente trabajar en los sistemas con perfiles menos privilegiados, con la idea de minimizar las consecuencias ante posibles errores. Únicamente cuando fuese imprescindible se cambiaría al perfil de administrador para realizar las operaciones que así lo requiriesen.

De un administrador se exigen amplios conocimientos del sistema administrado, capacidad de toma de decisiones, filosofía de mejora continua, eficacia y responsabilidad.

Existen diversos caminos para llegar a convertirse en administrador de sistemas. Desde el camino autodidacta, muy presente en la profesión, que sigue posibilitando la existencia de grandes expertos en el conocimiento de la materia, pasando por el camino académico reglado y terminando en el camino de las certificaciones ofrecidas por los fabricantes, como por ejemplo MCSE (*Microsoft Certified Solutions Expert)* en el caso de los sistemas operativos Windows Server o LPIC (*Linux Professional Institute Certification*) en el caso de sistemas operativos basados en Linux.

Dependiendo de la naturaleza, del tamaño y de la complejidad de los sistemas de información de las organizaciones, la administración puede exigir una dedicación exclusiva. En organizaciones grandes y complejas existirá un mayor número de administradores que podrán agruparse en equipos y especializarse por sistemas operativos, servicios o disciplinas.

Otra modalidad de administración es la externalización. Existen organizaciones que, o bien no cuentan con los recursos humanos y técnicos precisos para la administración de sus sistemas, o bien no desean gestionarlos y prefieren ceder esa tarea a profesionales independientes o empresas del sector. En estos casos, se llega a acuerdos contractuales en los que se establecen las necesidades de la organización y se definen los niveles de atención, los **acuerdos de nivel de servicio** (en inglés, S*ervice Level Agreement, SLA*).

Un acuerdo de nivel de servicio debe recoger aspectos tales como el número de administradores que se necesitarán, sus funciones y responsabilidades, la disponibilidad horaria, los tiempos de respuesta o las penalizaciones en caso de incumplimiento.

2. Funciones y responsabilidades

Un departamento de sistemas de información no puede abstraerse de la filosofía de su organización que, al final, suele condicionar tanto los organigramas como las funciones y responsabilidades. No serán las mismas funciones en el caso de una PYME que en el de una multinacional que cuente con sus propios equipos de administradores o en el caso de una empresa que ofrece servicios de administración de manera externalizada.

2.1. Funciones

A grandes rasgos, podrían establecerse las siguientes funciones:

— **Administración de servidores**

La tarea consistirá en instalar, configurar, mantener y garantizar el servicio de una serie de equipos en la organización.

Controlará la instalación y desinstalación de software en esos equipos, pues es su más profundo conocedor, tanto de la necesidad como de la compatibilidad con el hardware y el resto de software.

Obtendrá y analizará estadísticas de uso –cargas de utilización de CPU, de memoria o de red-, horarios de conexión y duración de los accesos a los recursos o cualquier otro dato que pueda resultar de interés para ajustar los sistemas, dimensionarlos eficientemente, proponer mejoras y evitar problemas por sobrecargas.

Es competencia del administrador la realización de un estudio de viabilidad del software a instalar. Con cierta frecuencia se instala software innecesario que penaliza el rendimiento del sistema si no se elimina.

Además, si el software instalado no se mantiene o actualiza puede convertirse en un factor de riesgo ante ataques que exploten sus vulnerabilidades.

No puede olvidarse que es obligatorio realizar un control de licencias del software instalado para cumplir con la legalidad.

Además, el administrador responderá ante una posible contingencia para poder recuperar el sistema rápidamente.

— **Administración de la red**

No es fácil imaginar sistemas de información que funcionen de forma independiente (en inglés, servidores *stand-alone*). Asegurar la conectividad es imprescindible. La administración de los elementos que permiten esta conectividad requiere de la presencia de un administrador con conocimientos añadidos en tipologías, topologías, protocolos de red, etc.

— **Administración de usuarios**

Los sistemas informáticos son una herramienta para una organización y para sus usuarios. Estos necesitarán acceso a los distintos servicios proporcionados por los servidores. Una eficiente gestión de usuarios resulta clave y es una de las partes más visibles en la tarea de un administrador.

Es posible que la tarea de creación de usuarios le sea encomendada a un administrador. Este proporcionará derechos y permisos sobre los distintos recursos de la organización, habitualmente en función de roles. Resultará más cómoda la agrupación de usuarios para facilitar su administración.

En muchas ocasiones, será necesario establecer cuotas para evitar el crecimiento desmesurado de las necesidades de almacenamiento o de ancho de banda de red, por ejemplo. Son situaciones que pueden tener alto impacto en un sistema y en la organización, pues un crecimiento incontrolado puede afectar al rendimiento, exigirá una mayor inversión en almacenamiento y provocará que el sistema de copias de seguridad consuma más recursos, tanto en tiempo como en espacio de disco.

En la administración de usuarios es vital la confidencialidad de las cuentas. No conviene guardar las contraseñas de los usuarios para recuperarlas en el caso de un olvido por parte de un usuario. El administrador establecerá mecanismos que le permitan establecer una nueva contraseña en una cuenta sin necesidad de conocer la antigua.

— **Administración de los datos**

En una sociedad como la actual, gran parte de los activos de una organización se encuentra en los datos que maneja. Garantizar el acceso, su seguridad y su integridad es prioritario. La administración de las bases de datos se ha convertido en un aspecto vital para las organizaciones.

— **Administración de la web**

  La web es la imagen que una organización muestra al mundo que accede a ella vía Internet. Aspectos como disponibilidad, rendimiento y seguridad son imprescindibles para su administrador.

— **Administración de la seguridad**

  Se trata de una función que se ha potenciado en los últimos años, sobre todo desde la exposición masiva de los sistemas de información gracias a Internet. Un administrador de seguridad es el responsable de la seguridad de un sistema y deberá garantizar la protección de los activos de la organización.

  Se trata de una disciplina muy amplia y compleja que abarca numerosos aspectos, por ejemplo el diseño de la asignación de permisos a los usuarios, la gestión de las copias de seguridad, la instalación de elementos de seguridad –software y hardware– que protejan la infraestructura y los datos, la seguridad física de la propia infraestructura, etc.

  Además, el administrador participará en el diseño, mantenimiento y aplicación de los planes de contingencia que permitirán recuperar una instalación o parte de ella en el caso de una pérdida de servicio.

Vistas las anteriores funciones desglosadas por tipos de servicio, sí podríamos relacionar una serie de funciones consideradas como transversales para los administradores de sistemas:

— Implementar y configurar los sistemas operativos.

— Instalar y configurar elementos hardware y software.

— Mantener los elementos que componen la infraestructura del sistema.

— Monitorizar la infraestructura.

— Documentar la situación y configuración de la infraestructura, así como los procedimientos para realizar ciertas operaciones.

— Afinar el rendimiento de los sistemas.

— Gestión de incidencias en los sistemas. El administrador es el encargado de solucionar cualquier error que aparezca en el sistema administrado y hacerlo de forma que suponga el menor impacto posible para el servicio y la organización. El administrador es el encargado de evaluar la situación, examinar las alternativas y proponer las acciones a adoptar.

— Administración proactiva: las tareas de prevención forman parte de las responsabilidades de los administradores. Puesto que son los mejores conocedores de un sistema, pueden adelantarse a la aparición de una incidencia en dicho sistema. El administrador identifi-

cará la criticidad del sistema que administra y tomará las medidas preventivas adecuadas.

Estas funciones pueden extenderse o acortarse, atendiendo a los factores de tipología y tamaño de organizaciones ya comentados. Además, aunque las funciones cuentan con unas tareas definidas que no son independientes, han de coordinarse. Así y todo, en no pocas ocasiones se producirá un solapamiento de funciones entre administradores de distintas disciplinas.

No obstante a todo lo anterior, la responsabilidad del administrador será la de asegurar el correcto funcionamiento de un sistema o de algún aspecto del mismo.

2.2. Responsabilidades

Es común, en el caso de organizaciones que cuentan con un departamento de tecnologías de información y comunicaciones (TIC), que las decisiones las tome un responsable previa consulta con los expertos técnicos –los administradores–. Estos asesoran al responsable para que adopte unas decisiones que afectarán a la infraestructura de la organización. Aspectos como qué sistema operativo implantar, qué software de base adquirir o el dimensionamiento del Centro de Proceso de Datos (CPD), representan decisiones claves, complejas y que comprometen económicamente a la organización.

Las organizaciones se adaptan continuamente a los cambios que se van sucediendo en distintos campos, entre ellos el tecnológico o el económico. La respuesta de estas organizaciones suele ser la **planificación estratégica**. Esta es la herramienta que permite ajustar el funcionamiento de una organización y que ha de ser capaz de integrar sus distintos departamentos bajo unos mismos objetivos utilizando un marco común de trabajo. Un plan estratégico puede definirse como un conjunto de propuestas realistas que servirán para fijar los objetivos futuros de la organización.

El responsable de informática, responsable de tecnologías de información y comunicaciones (o responsable TIC), director de tecnología o CIO (*Chief Information Officer*) es la figura que enlaza las necesidades de la organización y el trabajo que se realiza en el departamento de tecnologías de la información. Cuenta con información estratégica de la organización que traslada a su departamento para el cumplimiento de los planes establecidos por la dirección. En su departamento gestionará los recursos –humanos y técnicos–, para lograr el equilibrio necesario, dichos recursos y los objetivos de la organización.

Como cualquier otro departamento, el de informática ha de ceñirse a los planes estratégicos que marca la dirección. Cada departamento contará con su propia versión del plan que se vinculará al plan estratégico global. El responsable del departamento de informática garantizará la elaboración y velará por el cumplimiento del plan estratégico en su departamento. Otras responsabilidades del responsable de informática son:

— Detección de necesidades.

— Concreción de necesidades con los responsables de otros departamentos y con la dirección de la organización.

— Diseño e implantación de planes de actuación, proactiva y reactiva.

— Diseño e implantación de planes de actualización.

— Diseño e implantación del análisis de riesgos.

— Diseño e implantación del plan de seguridad.

— Diseño e implantación del plan de contingencia para actuar ante situaciones que comprometan la seguridad de los sistemas de información así como la propia información de la organización.

— Supervisión de los proyectos de software.

— Actuación ante situaciones de índole legal.

3. Control de cambios de los programas de una instalación

El cambio es un hecho habitual en el desarrollo del software. Los fabricantes y los usuarios adquieren un conocimiento que lleva a exigir mejoras, la tecnología avanza y permite aproximarse a un problema desde otro enfoque que obliga a modificar el software anterior. No hay que olvidar los motivos económicos, pues fuerzan a que el cambio esté garantizado en un momento dado del ciclo de vida de cualquier software.

Inicialmente el control de versiones se utilizó para gestionar los cambios en el código fuente del software. Con la explosión de los sistemas de información y del mundo digital, su utilización se ha extendido tanto a los grandes desarrollos de software como a cualquier disciplina que genere un flujo de información en formato digital.

3.1. El proceso de gestión de configuración del software

Una organización puede necesitar identificar y gestionar las distintas versiones del software que utiliza, así como de la documentación que se genera, garantizando una introducción eficiente de cambios. Aspectos como quién aprueba la asignación de los cambios, cómo se realizan dichos cambios antes de distribuir las nuevas versiones, cómo garantizar que los cambios fueron realizados correctamente o el método de notificar la realización de los mismos se recogen en la gestión de configuraciones del software. Esta disciplina se conoce como Ingeniería del Software o también como Arquitectura del Software.

Con el objetivo de garantizar la calidad del software, esta disciplina se aplica en todas las fases del proceso de ingeniería definiendo el producto de software como un agregado de componentes, tanto funcionales como estructurales.

La configuración de un software ha de ser controlada, pues es necesario conservar su integridad. Para ello, será preciso mantener actualizada la información, sobre todo el software existente en un sistema, y asegurar que la misma es clara y rigurosa a medida que se van sucediendo los cambios.

Este proceso puede hacerse de forma manual pero, dada la existencia de herramientas que automatizan las tareas y facilitan la administración de cada software desarrollado, no resulta muy aconsejable. Existen herramientas propietarias y de código abierto.

Actualmente es posible elegir entre dos grandes modelos:

— **Modelo cliente-servidor**. En este modelo se utiliza un repositorio central al que se accede desde un cliente ubicado en cada máquina.

  Ejemplos de herramientas propietarias son: CA SCM (Computer Associates), ClearCase (Rational Software, IBM), SourceAnywhere (Dynamsoft) o Visual SourceSafe (Microsoft).

  En el caso del código abierto existen las herramientas: Concurrent Versions Systems (CVS) y Subversion.

— **Modelo distribuido**. Con el modelo distribuido se trabaja directamente en un repositorio local. En fases posteriores se comparten los cambios entre repositorios.

  Como ejemplos de herramientas propietarias están: BitKeeper y Plastic SCM (de Codice Software).

  En código abierto existen las herramientas: Mercurial, Git, Bazaar, Codeville y LibreSource.

3.2. Tareas de gestión

Normalmente, un proceso de gestión de configuración de software consistirá en cuatro tareas: identificación, control de cambios, auditoría de la configuración y gestión de informes.

3.2.1. Identificación

En la tarea de identificación se establecen los estándares de documentación así como un esquema de identificación de los documentos necesarios. Tiene tres objetivos:

— Establecer un **formato**. Para ello habrá que definir la estructura de la documentación.

— Establecer una **metodología** para las revisiones y para el añadido de los cambios a medida que se produzcan.

— Facilitar el **control de los cambios**. Será necesario identificar quién, qué, cuándo, cómo, por qué, etc., se actualiza o se modifica.

La configuración de un software se mantiene durante todo su ciclo de vida. Pueden proporcionarse bibliotecas y ayudas de referencia como soporte a las configuraciones generadas.

El control de la documentación suele admitir tres enfoques:

— Se mantienen como parte de una biblioteca de documentación de ingeniería todos los documentos relacionados con el software y con los diferentes elementos de cada configuración.

— Se establece para todas las configuraciones de software una librería de software especial.

— Se establece una librería de software online, que contará con facilidades de recuperación de documentación accedida de forma remota.

Sea cual fuese el enfoque, conviene establecer un **sistema de referencia**. En la tabla siguiente se muestra un posible sistema:

CDC-001-P-0-1/16	Plan (P) del proyecto 1 de la empresa CDC. Es el documento original. Entró en el proceso de control de cambios en enero (mes 1) de 2016
CDC-001-R-1-2/16	Es la revisión (R) número 1 al plan del proyecto 1. Entró en el proceso de control de cambios en febrero (mes 2) de 2016
CDC-007-R-3-3/16	Es la revisión (R) número 3 al plan del proyecto 7. Entró en el proceso de control de cambios en marzo (mes 3) de 2016

En el ejemplo, cada documento es referenciado por un identificador único (XXX-YYY-Z-RL-NNN) que contiene:

— Identificador único de proyecto, XXX-YYY.

— Identificador del elemento de la configuración, Z. En este ejemplo puede adoptar los valores P (plan) y R (revisión).

— Número de nivel de revisión, en inglés *Revision Level*, RL. En el ejemplo 0, 1 y 3.

— Códigos de atributo, NNN. En el ejemplo 1/16, 2/16 y 3/16.

3.2.2. Control de cambios

Esta tarea evaluará y registrará todos los cambios que se realicen en la configuración del software. Pueden establecerse tres tipos de control:

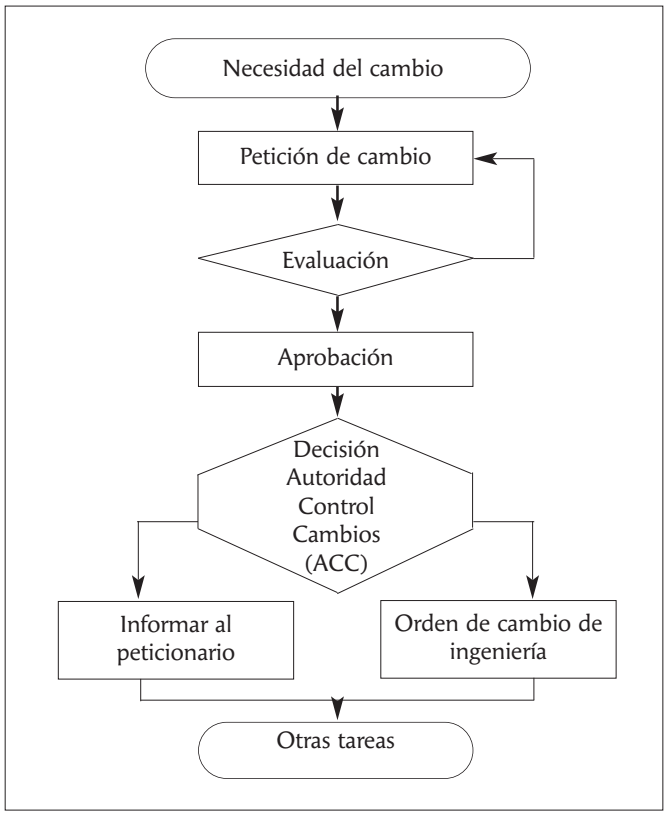
— **Individual**. Se establece antes de aprobarse un nuevo elemento. El administrador responsable modifica la documentación cuando así es requerido. Suele llevarse un control informal de las revisiones que no se incluyen en el documento. El control individual se caracteriza por cambios frecuentes y es aplicado durante las etapas más importantes del desarrollo del documento.

— **De gestión**. Suele implicar un procedimiento de revisión y de aprobación para cada modificación propuesta en la configuración. De la misma forma que en el control individual, el de gestión sucede durante todo el proceso de desarrollo y se utiliza después de haber sido aprobado un elemento de la configuración del software. Este nivel se caracteriza por contar con menos cambios que el individual. Cada cambio se registra y es visible para la gestión.

— **Formal**. Se realiza durante el mantenimiento del ciclo de vida del software, pues este ya está implantado. Cada tarea de mantenimiento ha de evaluarse antes de ser aprobada cualquier modificación. Esta evaluación es realizada por el denominado comité de control de cambios quien, además, aprueba o no las modificaciones solicitadas.

  En determinadas circunstancias es necesario establecer arreglos rápidos (en inglés *quick-fix*), por ejemplo ante la existencia de un error considerable en el elemento software que es obligatorio solventar en un tiempo breve. Este procedimiento es adecuado para proporcionar resultados significativos en situaciones de emergencia, pero no es conveniente para otros niveles de control de cambios.

El **flujo del proceso de la gestión de control del software** puede verse en el siguiente gráfico:



Una petición de cambio pide una modificación para corregir una deficiencia o un error, para adaptarse a un nuevo sistema operativo o a una nueva infraestructura y se somete al análisis de la organización. Una vez que los aspectos técnicos y de gestión se hayan resuelto, se generará un informe de cambios para su evaluación por el comité de control de cambios. De esta evaluación se obtiene una aprobación o un rechazo y es notificado al solicitante. Para cada modificación aprobada se generará una orden de cambio en la que se detallarán los criterios de revisión, el cambio realizado, las restricciones a respetar y las auditorías.

El comité de control de cambios podría considerarse como un órgano de gobierno para los asuntos relacionados con la gestión de configuración del software. Suele estar formado por componentes de los departamentos que solicitan los cambios y por los desarrolladores.

En pequeños proyectos, el comité tendrá una composición reducida, con apenas un representante de cada departamento. Sin embargo, en grandes proyectos suele existir una separación que afrontará aspectos relacionados con el hardware, el sistema y el software por separado. Las tareas habituales de este comité son:

— Análisis del impacto de las modificaciones en el sistema.

— Categorización y priorización de las modificaciones.

— Intervención ante posibles conflictos entre departamentos a la hora de realizar una modificación.

— Garantizar que las propiedades de mantenimiento de registro y contabilización se cumplan.

3.2.3. Auditoría de la configuración

Con la auditoría de la configuración se garantiza que el cambio se realizó de forma correcta. Habitualmente, será necesario realizar varias comprobaciones:

— Comprobación de la realización de la modificación así como de la incorporación de modificaciones adicionales.

— Comprobación de la revisión técnica formal.

— Comprobación de la adecuación de los estándares de ingeniería del software.

— Comprobación de la modificación en los elementos de configuración del software: fechas, autores, etc.

— Comprobación de la actualización adecuada de los elementos de configuración del software.

— Comprobación del seguimiento de la gestión de configuración del software para señalarlos, registrarlos y divulgarlos.

3.2.4. Generación de informes

Los informes son la documentación de todo el proceso que permitirá ampliar el conocimiento y mejorar el propio proceso. Se trata de responder a las siguientes preguntas:

— ¿Qué ocurrió?

— ¿Quién lo hizo?

— ¿Cuándo ocurrió?

— ¿Qué aspectos fueron afectados?

— ¿Cómo se solucionó?

La existencia de esta documentación permitirá compartir conocimientos y preservar la experiencia acumulada. En un momento dado, podrá aprovecharse esta documentación para realizar procedimientos similares o para operaciones de marcha atrás realizadas, incluso, por personas diferentes a las que generaron la documentación, convirtiéndose en un gran activo para la organización.

El flujo de información del proceso de generación de los informes de estado de la configuración (IEC) puede verse en el siguiente gráfico: