Como experiencia práctica del uso del modelo ISO Extendido tenemos la realizada por las compañías participantes en el proyecto QUINT (Quality in Information Technology)[4] cuyo primer proyecto empezó en 1991, siendo su objetivo el desarrollar un modelo y una guía para las especificaciones de calidad del software, participando todas las partes involucradas en la negociación sobre los requerimientos.

El segundo proyecto QUINT expandió los resultados del primero. En él participaron seis compañías bajo la dirección de los institutos de investigación SERC, TNO/TPD y FPIQM.

16.5. OBJETIVOS DE LAS AUDITORÍAS DE CALIDAD

Una auditoría de Calidad tiene como objetivo el mostrar la situación real para aportar confianza y destacar las áreas que pueden afectar adversamente esa confianza.

Hay varias razones para realizar una auditoría:

- Establecer el estado de un proyecto.
- Verificar la capacidad de realizar o continuar un trabajo específico.
- Verificar qué elementos aplicables del programa o Plan de Aseguramiento de la Calidad han sido desarrollados y documentados.
- Verificar la adherencia de esos elementos con el programa o Plan de Aseguramiento de la Calidad.

El propósito y la actividad de la auditoría es recoger, examinar y analizar la información necesaria para tomar las decisiones de aprobación.

La auditoría debe tener capacidad para investigar la pericia técnica, el desarrollo del software o la capacidad del departamento de desarrollo, el esfuerzo disponible, el soporte del mantenimiento o la efectividad de la gestión.

En las auditorías debe acordarse el dirigirse a criterios específicos tales como la realización del código software.

Cuando se identifiquen los puntos débiles, los auditores deberán tomar una actitud positiva y utilizar sus conocimientos y experiencia para hacer recomendaciones constructivas. En realidad, una función del auditor es pactar la idoneidad de cualquier acción correctiva propuesta. Este papel, si es usado adecuadamente, es uno de los vínculos más valorados entre las partes.

[4] "QUINT Het specifieren van software-kwaliteit", Kluwer Bedrijfswetenschappen, Deventer, the Netherlands, ISBN 90 267 1808 X (1992).

16.6. PROCESOS DE CALIDAD

En el entorno económico actual, la característica más importante es la competitividad, lo que quiere decir que los precios a los que ofrezcamos nuestros productos a nuestros clientes deben ser iguales o más bajos que los de la competencia, pero con una calidad más alta. Para conseguirlo es necesario tener una estructura de costes adecuada y disponer de una estrategia de Calidad que afecte a todas las áreas de la entidad u organismo.

Para satisfacer los requisitos de calidad es necesario conocer las Necesidades del Cliente. Éstas vienen dadas por estos tres parámetros:

- Calidad de los productos y servicios.
- Plazo de entrega adecuado.
- Coste dentro de los límites fijados.

El establecimiento de acuerdos de Nivel de Servicio y el cumplimiento de sus requerimientos le dará un determinado grado de satisfacción, que deberemos saber medir sobre todo una vez pasado el período de estabilización del producto entregado.

Una de las principales características de los procesos de calidad es la repetitividad de los mismos. Todo proceso debe estar suficientemente definido como para que pueda ser repetido consiguiendo los mismos resultados cada vez que se realice el mismo proceso. La idea "Sigma" está unida a la variabilidad de un proceso.

Una vez alcanzada esta repetitividad de los procesos y teniendo elementos para medir los atributos de los productos obtenidos, trataremos de ir refinando el modelo del proceso para reducir los defectos entregados (definiendo defecto como cualquier variación de una característica establecida que origina el incumplimiento de las necesidades del cliente con la consiguiente insatisfacción del mismo).

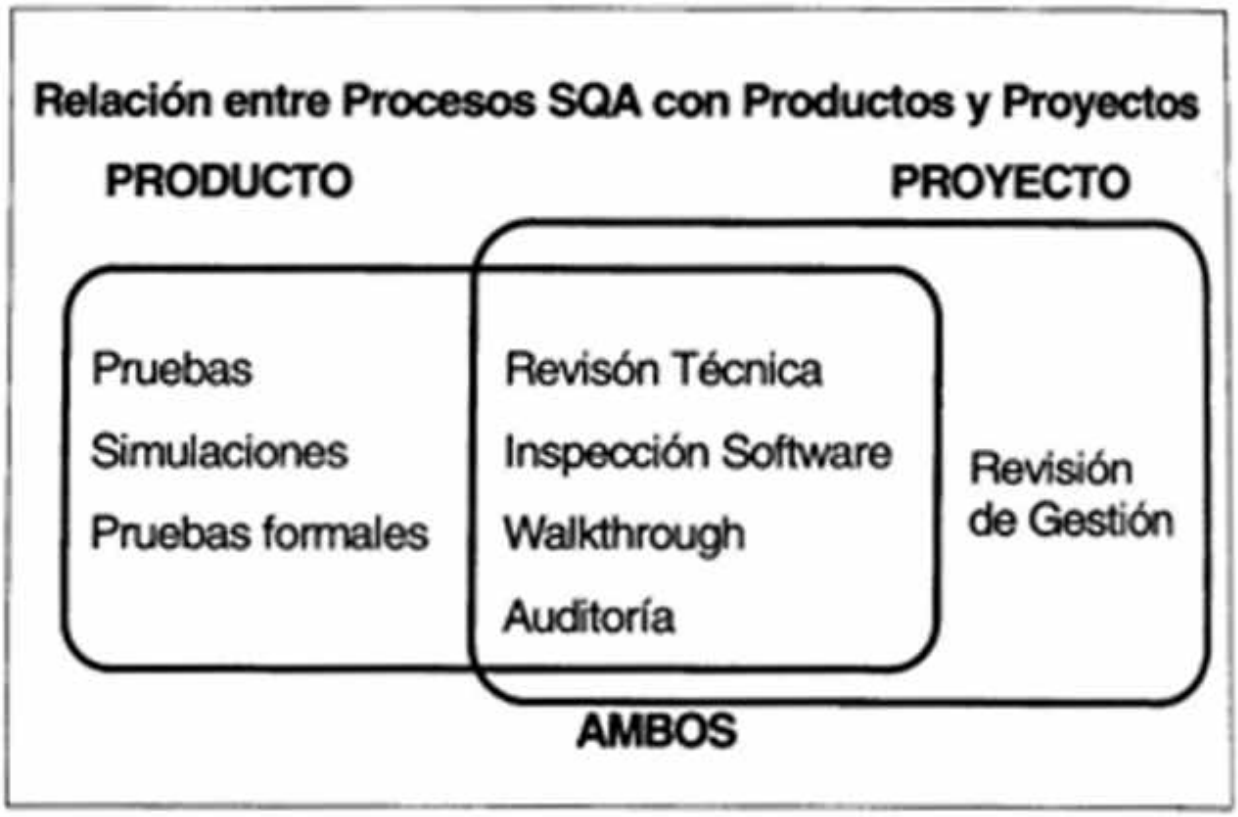
Como se ha indicado anteriormente, las revisiones y las auditorías pueden usarse para actividades de aseguramiento de la calidad, gestión de proyectos, gestión de la configuración o funciones de control singulares.

Según el estándar IEEE 1028, incluimos una tabla en la que se señalan los principales Procesos para conseguir Objetivos de Calidad.

Principales Procesos para conseguir Objetivos de Calidad

Objetivos	Principales Procesos que incluye
Evaluación	Revisiones de Gestión, Revisiones Técnicas
Verificación	Inspecciones, *Walkthrough*
Validación	Pruebas
Conformidad, Confirmación	Auditoría

También en la figura siguiente se refleja la relación entre procesos y productos dentro de la actividad de Aseguramiento de la Calidad.



El examen de los aspectos técnicos y de gestión se realiza en varias fases durante el ciclo de vida del proyecto. El resultado son controles para permitir mejorar los métodos y asegurar la calidad del software y la posibilidad de conjugar las restricciones de tiempo y coste. La evaluación de los elementos software se realiza durante la generación de esos elementos y a su término. Esto asegura que los elementos terminados expresan correctamente las especificaciones de su "línea base".

Cualquier proceso estándar tiene unas condiciones como prerrequisitos; éstas son necesarias, aunque no son suficientes en sí mismas para que el proceso quede completado. Para las revisiones las auditorías las condiciones son:

Prerrequisitos en los Procesos de Revisión

El objetivo de una Revisión de un elemento software es evaluar el software o el estado, del proyecto para identificar las discrepancias sobre los resultados planificados y recomendar mejoras cuando sea apropiado.

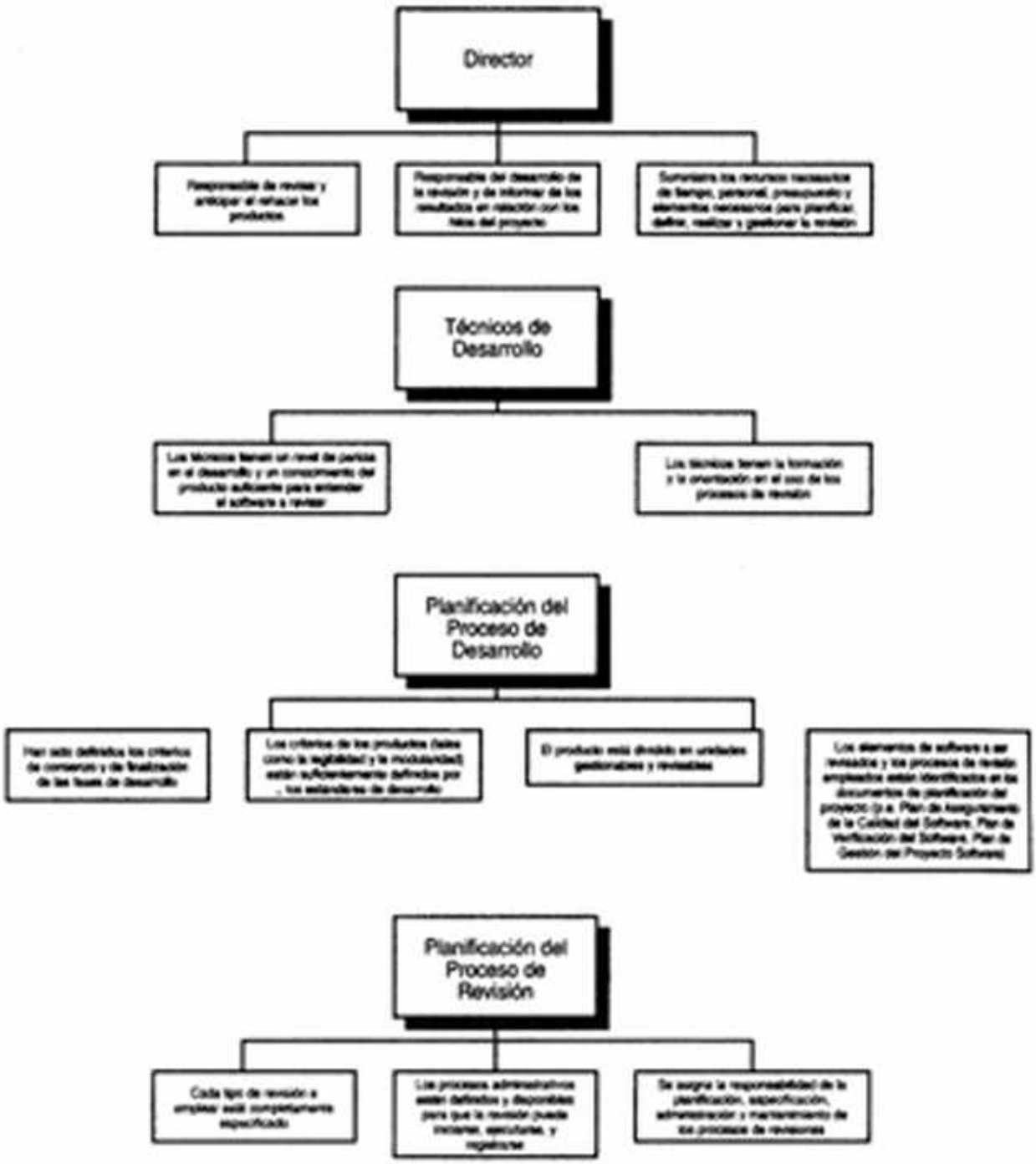
En la figura de la página siguiente se reflejan los prerrequisitos del Proceso de Revisión.

El objetivo de la auditoría del Software es suministrar una evaluación objetiva de los productos y los procesos para corroborar la conformidad con los estándares, las líneas guía, las especificaciones y los procedimientos. Los siguientes requerimientos son prerrequisitos para conseguir este objetivo:

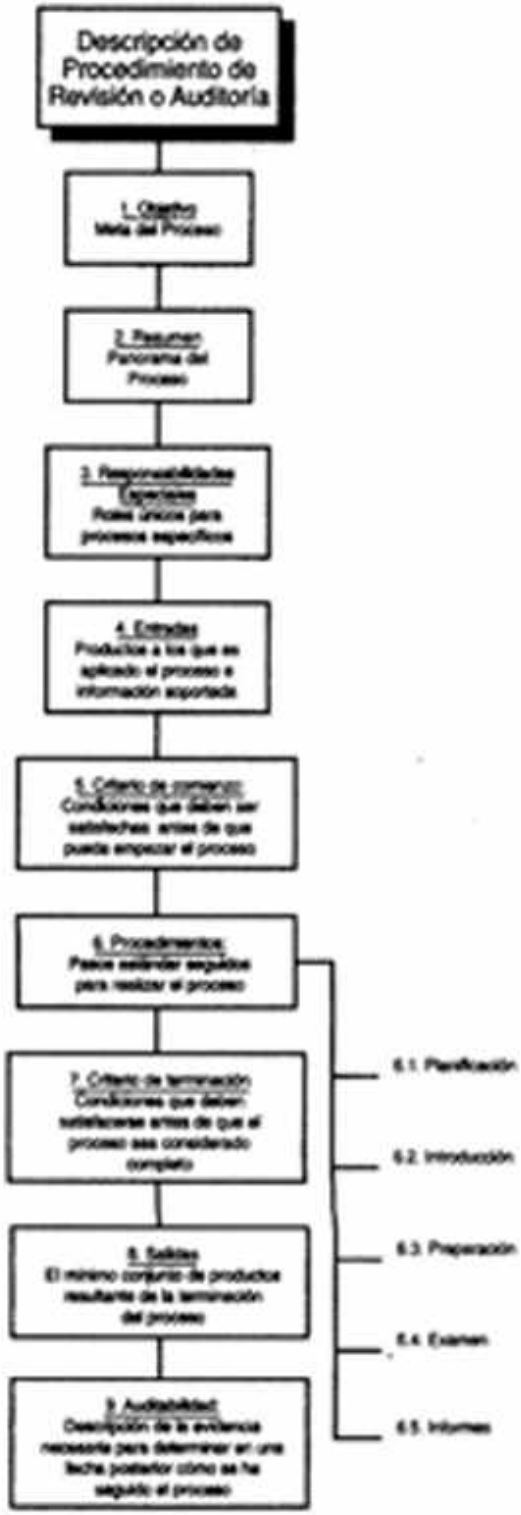
1. Objetivo de la auditoría, criterios existentes (por ejemplo, contratistas, requerimientos, planes, especificaciones, estándares) en relación con los elementos software y los procesos que puedan ser evaluados.

2. El personal de auditoría es seleccionado para promover los objetivos del grupo. Son independientes de cualquier responsabilidad directa para los productos y los procesos examinados y pueden provenir de una organización externa.

3. El personal de auditoría debe tener la suficiente autoridad que le permita una adecuada gestión con el fin de realizar la auditoría.



En la figura de la página siguiente se incluye una descripción esquemática del procedimiento a utilizar para planificar, preparar y realizar cualquier proceso de revisión o de auditoría, según el estándar IEEE 1028.



16.7. EL PROCESO DE AUDITORÍA DEL SOFTWARE

1. *Objetivo.* Según se ha indicado es proveer la confirmación de la conformidad de los productos y los procesos para certificar la adherencia con los estándares, líneas guía, especificaciones y procedimientos.

2. *Resumen.* La auditoría es realizada de acuerdo con los planes y procedimientos documentados. El plan de auditoría establece un procedimiento para dirigir la auditoría y para las acciones, de seguimiento sobre las recomendaciones de la auditoría.

Al realizar la auditoría, el personal de la auditoría evalúa los elementos software y los procesos para contrastarlos con los objetivos y criterios de la auditoría, tales como contratos, requerimientos, planes, especificaciones o procedimientos, líneas guía y estándares.

Los resultados de la auditoría son documentados y remitidos al director de la organización auditada, a la entidad iniciadora de la auditoría, y a cualquier organización externa identificada en el plan de auditoría. El informe incluye una lista de elementos no conformes u otros aspectos para las posteriores revisiones y acciones. Cuando sea estipulado en el plan de auditoría, las recomendaciones son informadas e incluidas en los resultados de la auditoría.

3. *Responsabilidades especiales.* Es responsabilidad del líder del equipo de auditoría el organizar y dirigir la auditoría y la coordinación de la preparación de los puntos del informe de auditoría. El líder del equipo deberá asegurar que el equipo de auditoría está preparado para llevar ésta, y que los procedimientos y los distintos puntos son realizados y reflejados en los informes de acuerdo con su alcance.

La entidad iniciadora de la auditoría es responsable para autorizar ésta. La dirección de la organización auditora asume la responsabilidad de la auditoría, y la asignación de los recursos necesarios para realizar dicha auditoría.

Aquellos cuyos productos y procesos son auditados suministrarán todos los materiales y recursos relevantes y corregirán o resolverán las deficiencias citadas por el equipo de auditoría.

4. *Entrada.* Se requieren las siguientes entradas para realizar la auditoría:

1. El propósito y alcance de la auditoría.
2. Criterios objetivos de la auditoría, tales como contratos, requerimientos, planes, especificaciones, procedimientos, líneas guía y estándares.
3. Los elementos software y los procesos a auditar y cualquier antecedente pertinente.
4. Información complementaria respecto a la organización responsable de los productos y los procesos a auditar (por ejemplo, organigramas de la organización).

5. *Criterio de comienzo.* La necesidad para que una auditoría se inicie debe ser por uno de los siguientes sucesos:

1. Se ha alcanzado un hito especial del proyecto. La auditoría es iniciada por planes previos (por ejemplo, el plan de aseguramiento de calidad, el plan de desarrollo del software).
2. Partes externas (por ejemplo, agencias reguladores o usuarios finales) demandando una auditoría en una fecha específica o en un hito del proyecto. Ésta puede ser por la realización de un requerimiento de un contrato o como prerrequisito a un acuerdo contractual.
3. Un elemento de la organización local (por ejemplo, el director del proyecto, la dirección funcional, ingeniería de sistemas, aseguramiento o control interno de la calidad) ha requerido la auditoría estableciendo una necesidad clara y específica.
4. Un hito especial del proyecto, fecha de calendario, u otro criterio ha sido alcanzado y dentro de la planificación de la organización de auditoría le corresponde la iniciación de una auditoría.

6. *Procedimientos:*

6.1. **Planificación.** La organización de auditoría debe desarrollar y documentar un plan de auditoría para cada auditoría. Este plan deberá apoyarse en el alcance de la auditoría identificando lo siguiente:

1. El proceso del proyecto a examinar (suministrado como entrada) y el tiempo de observación del equipo de auditoría.
2. Los requerimientos del software a examinar (suministrado como entrada) y su disponibilidad. Cuando se usa el muestreo, debe utilizarse una metodología estadística válida al respecto para establecer los criterios de selección y el tamaño de la muestra.
3. Los informes serán identificados (informes de resultados, y opcionalmente el informe de recomendaciones y definido su formato general). Si las recomendaciones son requeridas o excluidas, debe ser indicado explícitamente.
4. Distribución de informes.
5. Requerimientos de las actividades de seguimiento.
6. Requerimientos: actividades necesarias, elementos y procedimientos para cubrir el alcance de la auditoría.
7. Objetivos y criterios de auditoría: proveen las bases para determinar las coincidencias (suministradas como entrada).
8. Procedimientos de auditoría y listas de comprobación.
9. Personal de auditoría: número requerido, perfiles, experiencia y responsabilidades.
10. Organizaciones involucradas en la auditoría (por ejemplo, la organización cuyos productos y procesos están siendo auditados).
11. Fecha, hora, lugar, agenda y la audiencia a quien se dirige la sesión de introducción (opcional).

El líder del equipo de auditoría asegurará que su equipo está preparado e incluye los miembros con la experiencia y pericia necesaria.

La notificación de la auditoría a las organizaciones involucradas debe realizarse con una anterioridad razonable, excepto en el caso de las auditorías no anunciadas. La notificación deberá ser hecha por escrito y deberá incluir el alcance la identificación de los procesos y productos a auditar, así como la identificación de los auditores.

6.2. **Introducción.** Opcionalmente es recomendable hacer una reunión introductoria con la organización a auditar en el momento del arranque para examinar las fases de la auditoría. La reunión de introducción encabezada por el líder del equipo de auditoría, abordará lo siguiente:

1. Introducción sobre los acuerdos existentes (por ejemplo, alcance de la auditoría, planificación, contratos afectados).
2. Introducción de la producción y procesos a ser auditados.
3 Introducción del proceso de auditoría, sus objetivos y sus salidas.
4. Contribuciones esperadas de la organización auditada al proceso de auditoría (número de personas a entrevistar, facilidades para reuniones, etc.).
5. Planificación específica de la auditoría.

6.3. **Preparación.** Los siguientes puntos son requeridos para la preparación del equipo de auditoría:

1. Entender la organización: es esencial para identificar las funciones y las actividades realizadas por la organización auditada, así como para identificar las responsabilidades funcionales.
2. Entender los productos y los procesos: es prerrequisito para el equipo de auditoría conocer los procesos y los productos a auditar mediante lecturas e informes.
3. Entender los objetivos y criterios de la auditoría: es importante que el equipo de auditoría esté familiarizado con el objetivo de la auditoría y los criterios usados en ella.
4. Preparación para el informe de auditoría: es importante seleccionar el mecanismo administrativo de información que será usado durante la auditoría para ir confeccionando el informe siguiendo el diseño determinado en el plan de auditoría.
5. Detalle del plan de auditoría: seleccionar el método apropiado para cada paso en el programa de auditoría.

Adicionalmente el líder del equipo de auditoría deberá hacer los preparativos necesarios para:

1. Orientar a su equipo y formarlo si es necesario.
2. Preparar lo necesario para las entrevistas de la auditoría.
3. Preparar los materiales, documentos y herramientas necesarias según los procedimientos de auditoría.
4. Identificar los elementos software a auditar (por ejemplo, documentos, archivos informáticos, personal a entrevistar).
5. Planificar las entrevistas.

6.4. **Examen.** Los elementos que han sido seleccionados para auditarse deberán ser valorados en relación con el objetivo y criterios de la auditoría. Las evidencias deberán ser examinadas con la profundidad necesaria para determinar si esos elementos cumplen con los criterios especificados.

La auditoría será la adecuada para conseguir:

1. Revisar los procedimientos e instrucciones.
2. Examinar la estructura de descomposición de los trabajos.
5. Examinar las evidencias de la implantación y lo equilibrado del control.
4. Entrevistar al personal para averiguar el estado y el funcionamiento de los procesos y el estado de los productos.
5. Examinar cada documento.
6. Comprobar cada elemento.

6.5. **Informes.** A continuación del examen de auditoría, el equipo auditor deberá emitir un borrador del informe de auditoría a la organización auditada para su revisión y comentarios.

El equipo auditor podrá rehacer el informe de auditoría antes de que se tenga el resultado formal del informe. Estas adaptaciones se harán de acuerdo con la revisión del borrador del informe y resolverán cualquier mal entendido o ambigüedad mientras se mantiene la objetividad y exactitud. Esto también sirve para asegurar la fácil utilización del informe dándole consistencia en los detalles e incluyendo cualquier nueva información verificada. La práctica recomendada es involucrar a los representantes de la organización auditada en la revisión de los resultados de la auditoría.

Involucrando a la organización auditada se contribuye a mejorar la calidad del informe mediante la interacción y la posible aportación de cualquier evidencia adicional.

El grupo de auditoría organizará una conferencia posterior a la auditoría para revisar con los técnicos de la organización auditada las deficiencias, fallos y (si es aplicable) las recomendaciones. Los comentarios y los puntos abordados por la organización auditada, deberán ser resueltos.

El informe final de la auditoría debe ser preparado, aprobado y distribuido por el líder del equipo de auditoría a las organizaciones especificadas en el plan de auditoría.

6.6. **Criterio de terminación.** Una auditoría debe ser considerada terminada cuando:

1. Se ha examinado cada elemento dentro del alcance de la auditoría.
2. Los resultados han sido presentados a la organización auditada.
3. La respuesta al borrador de los resultados ha sido recibida y evaluada.
4. El resultado final ha sido formalmente presentado a la organización auditada y a la entidad iniciadora.
5. El informe final ha sido preparado y enviado a los receptores designados en el plan de auditoría.
6. El informe de recomendaciones, si el plan lo requiere, ha sido preparado y enviado a los receptores designados en el plan de auditoría.
7. Se han realizado todas las acciones de seguimiento incluidas en el alcance de la auditoría (o en el contrato).

6.7. **Salidas.** Como un marco estándar para los informes, el informe borrador de auditoría y el informe final de auditoría, deberán contener como mínimo, lo siguiente:

1. *Identificación de la auditoría.* Título del informe, organización auditada, organización auditora y fecha de la auditoría.

2. *Alcance.* Alcance de la auditoría, incluyendo la enumeración de los estándares, especificaciones, prácticas y procedimientos que constituyen su objetivo y el criterio contra el cual será dirigida la auditoría de los elementos software y de los procesos a auditar.

3. *Conclusiones.* Un resumen e interpretación de los resultados de la auditoría incluyendo los puntos clave de los aspectos no conformes.

4. *Sinopsis.* Un listado de todos los elementos software auditados, los procesos y los elementos asociados.

5. *Seguimiento.* El tipo y el cronograma de las actividades de seguimiento de la auditoría.

Adicionalmente, cuando lo estipule el plan de auditoría, las recomendaciones deberán enviarse a la organización auditada o a la entidad que inicie la auditoría. Las recomendaciones irán en un informe separado de los resultados.

6.8. **Auditabilidad.** Los materiales que documentan el proceso de auditoría deben ser mantenidos por la organización auditora durante un período estipulado después de la auditoría e incluyendo lo siguiente:

1. Todos los programas de trabajo, listas de comprobación, etc. con todos sus comentarios.
2. El equipo de técnicos.
3. Comentarios de las entrevistas así como de las observaciones.
4. Evidencias de pruebas de conformidad.
5. Copias de los elementos examinados con sus comentarios.
6. Informes borradores con las respuestas de la organización auditada.
7. Memorándum del seguimiento si es necesario.

16.8. AUDITORÍA DE SISTEMAS DE CALIDAD DE SOFTWARE

El propósito de la auditoría de un Sistema de Calidad, o un programa de evaluación de la calidad, es suministrar una valoración independiente sobre la conformidad de un Plan de Aseguramiento de la Calidad del Software.

Específicamente el objetivo es determinar, basándose en evidencias observables y verificables, que:

1. La documentación del programa de calidad del software establecida por la organización de desarrollo recoge como mínimo los elementos básicos del estándar ANSI/IEEE 730 u otro estándar apropiado.
2. La organización de desarrollo del software sigue el programa de calidad de software por ellos documentado.

El Plan de Aseguramiento de la Calidad del Software debe incorporar todos los objetivos y los criterios de actuación organizativos; estándares internos y procedimientos; procesos requeridos por la legislación, contratos u otras políticas; conformidad con el estándar ANSI/IEEE 730 u otro estándar apropiado para el aseguramiento de la calidad del software.

16.9. PROCESO DE ASEGURAMIENTO DE LA CALIDAD DESCRITO POR ISO 12207

Para realizar cualquier proceso de auditoría, es imprescindible conocer la actividad que se va auditar, por tanto, no debe extrañar al lector que vayamos intercalando descripciones de los procesos de calidad y los de desarrollo a lo largo del texto, en este caso lo que al respecto describe la norma ISO 12207.

La norma ISO/IEC 12207 "Information technology – Software life cycle processes" 1995, no podríamos dejar de citarla en este capítulo, ya que es una importante norma para el proceso de desarrollo del software y para los procesos de calidad.

Estructura de la norma ISO/IEC 12207

En la figura anterior se muestra la estructura de dicha norma en la que vemos los Procesos Primarios del Ciclo de Vida, los de Soporte y los Organizativos. El número que figura antes de cada proceso corresponde al apartado donde se describe el mismo en la norma.

De ella vamos a describir dos de los procesos más relacionados con nuestro tema, como son el Proceso de Aseguramiento de la Calidad y el Proceso de Auditoría, que consideramos que contribuyen a completar una perspectiva más amplia del tema que nos ocupa.

El apartado 6.3 relativo a los Procesos de Aseguramiento de la Calidad dice:

Los Procesos de Aseguramiento de la Calidad sirven para suministrar la seguridad de que durante el ciclo de vida del proyecto los productos y los procesos están de acuerdo con los requerimientos especificados y se adhieren a los planes establecidos. Al ser imparcial, el aseguramiento de la calidad necesita tener libertad organizativa y autoridad de las personas directamente responsables del desarrollo de los productos software o los que realizan los procesos en el proyecto. El aseguramiento de la calidad puede ser interno o externo, dependiendo de si la evidencia de la calidad de los productos o los procesos se va a demostrar a la dirección del suministrador o al cliente. El aseguramiento de la calidad puede hacer uso de los resultados de otros procesos de Soporte, tales como Verificación, Validación, Revisiones Conjuntas, Auditorías y Resolución de Problemas.

Este proceso de aseguramiento de la calidad se compone de las cuatro actividades que describimos a continuación:

16.9.1. Implementación del proceso

Esta actividad tiene las siguientes tareas:

- El proceso de aseguramiento de la calidad debe establecerse adaptado al proyecto. Los objetivos de este proceso de aseguramiento de la calidad serán asegurar que los productos software y los procesos utilizados para conseguir estos productos software cumplen con los requerimientos establecidos y se adaptan a los planes previstos.

- Los procesos de aseguramiento de la calidad deben ser coordinados con los procesos indicados de Verificación, Validación, Revisión Conjunta y Auditoría.

- El plan para dirigir los procesos, actividades y tareas de aseguramiento de la calidad debe ser desarrollado, documentado, implementado y mantenido durante el tiempo de duración del contrato. Este plan deberá incluir lo siguiente:

  a) Estándares de calidad, metodologías, procedimientos, y herramientas para realizar las actividades de aseguramiento de la calidad (o sus referencias a la documentación oficial de la organización).
  b) Procedimientos para la revisión y coordinación del contrato.
  c) Procedimientos para identificar, recoger, cumplimentar, mantener y acceder a los registros de calidad.
  d) Recursos, planes, y responsabilidades para dirigir las actividades de aseguramiento de calidad.
  e) Determinadas actividades y tareas de los procesos de soporte, tales como Verificación, Validación, Revisiones Conjuntas, Auditorías y Resolución de Problemas.

- Las actividades y tareas planificadas de aseguramiento de la calidad deben realizarse. Cuando son detectados problemas o no conformidades con los requerimientos contractuales, deben ser documentados y servir de entrada al Proceso de Resolución de Problemas. Deben prepararse y mantenerse los registros de estas actividades y tareas, su realización, los problemas y su resolución.

- Los registros de las actividades y tareas de aseguramiento de la calidad deben estar disponibles al cliente así como especificados en el contrato.

- Deberá cerciorarse de que las personas responsables de asegurar la concordancia con los requerimientos del contrato tienen la libertad

organizativa, los recursos y la autoridad para permitir evaluaciones objetivas e iniciar, efectuar, resolver y verificar la resolución de problemas.

16.9.2. Aseguramiento del producto

Esta actividad tiene las siguientes tareas:

- Deberá asegurar que aquellos planes requeridos por el contrato están documentados, cumplen con el contrato, son mutuamente consistentes, y están siendo ejecutados como se requiere.

- Deberá asegurar que aquellos productos software y su documentación cumplen con el contrato y están de acuerdo con los planes.

- En la preparación para el suministro de los productos software, deberá asegurarse de que satisfacen completamente los requerimientos contractuales y son aceptables para el cliente.

16.9.3. Aseguramiento del proceso

Esta actividad tiene las siguientes tareas:

- Deberá asegurar los procesos del ciclo de vida del software (suministro, desarrollo, operación, mantenimientos y soporte, incluyendo el aseguramiento de la calidad) empleados para que el proyecto esté de acuerdo con el contrato y se ajuste a los planes.

- Deberá asegurar que las prácticas internas de ingeniería de software, entorno de desarrollo y librerías están de acuerdo con el contrato.

- Deberá asegurar que los requerimientos aplicables del contrato principal son pasados al subcontratista, y que los productos software del subcontratista satisfacen los requerimientos del contrato principal.

- Deberá asegurar que al cliente y a las otras partes se les aporta el soporte y la cooperación requeridos de acuerdo con el contrato, las negociaciones y los planes.

- Deberá asegurar que los productos software y los procesos medidos están de acuerdo con los estándares y procedimientos establecidos.

- Deberá asegurar que el personal técnico asignado tiene el perfil y los conocimientos necesarios para conseguir cumplir los requerimientos del proyecto y que recibe la formación que pudiera necesitar.

16.9.4. Aseguramiento de la calidad de los sistemas

Esta actividad tiene la siguiente tarea:

- Las actividades adicionales de gestión de calidad deberán asegurar su concordancia con la cláusula de ISO 9001 según especifique el contrato.

16.10. PROCESO DE AUDITORÍA DESCRITO POR ISO 12207

El proceso de auditoría sirve para determinar la adherencia con los requerimientos, los planes y el contrato cuando es apropiado. Este proceso puede ser empleado por cualquiera de las dos partes, donde una de ellas (parte auditora) audita los productos software o las actividades de la otra parte (parte auditada).

Este proceso se compone de dos actividades:

16.10.1. Implementación del proceso

Esta actividad tiene las siguientes tareas:

- Las auditorías deben realizarse en determinados hitos, según lo especificado en los planes del proyecto.

- El personal auditor no debe tener ninguna responsabilidad directa en los productos software ni en las actividades que auditan.

- Todos los recursos requeridos para llevar la auditoría deben ser pactados por las partes, éstos incluyen personal de soporte, locales, hardware, software, herramientas y elementos complementarios.

- Las partes deberán ponerse de acuerdo en cada auditoría sobre: agenda; productos software (y resultados de las actividades) a revisar; alcance de la auditoría y procedimientos; y criterios de comienzo y de terminación de la auditoría.

- Los problemas detectados durante la auditoría deben ser registrados y tratados en el Proceso de Resolución de Problemas.

- Después de completar la auditoría, los resultados de ésta deben ser documentados y entregados a la parte auditada, quien deberá acusar recibo a la parte auditora de cualquier problema detectado en la auditoría y en la resolución de problemas planificada.

- Las partes deberán ponerse de acuerdo sobre los resultados de la auditoría y sobre cualquier punto de acción, responsabilidades y criterios de cierre.

16.10.2. Auditoría

Esta actividad tiene la siguiente tarea:

La auditoría deberá ser dirigida para asegurar que:

a) Los productos software codificados (tal como un elemento software) reflejarán lo diseñado en la documentación.

b) Los requerimientos de la revisión de aceptación y de pruebas prescritos por la documentación son adecuados para la aceptación de los productos software.

c) Los datos de prueba cumplen con la especificación.

d) Los productos software fueron sucesivamente probados y alcanzaron sus especificaciones.

e) Los informes de pruebas son correctos y las discrepancias entre los resultados conseguidos y lo esperado han sido resueltas.

f) La documentación del usuario cumple con los estándares tal como se ha especificado.

g) Las actividades han sido llevadas de acuerdo con los requerimientos aplicables, los planes y el contrato.

h) El coste y el cronograma se ajustan a los planes establecidos.

16.11. CONCLUSIONES

Hemos pretendido hacer una semblanza de los aspectos que consideramos más importantes para hacer una Auditoría de Calidad, tratando de soportarlos en diversos estándares y normas que en la mayoría de los casos hemos insertado traduciéndolos directamente de las mismas para no adulterarlos con una posible subjetividad. Con

esto consideramos que nos puede permitir tener una visión más amplia a través de los distintos enfoques que dan dichas normas sobre las Auditorías de Calidad.

Aunque somos conscientes de que el abordar una auditoría sólo con este bagaje no es suficiente. Un buen auditor en Tecnologías de la Información necesita tener una amplia experiencia en las distintas funciones de dicha actividad, estar muy al día en las distintas metodologías, procesos y herramientas que se emplean, de forma que le sea fácil detectar los defectos en los planes, en los productos y en los procesos, así como estar capacitado para poder proponer recomendaciones.

Reconocemos que no es una tarea fácil, pero precisamente por ello es altamente gratificante el alcanzar un éxito que satisfaga los intereses, en muchas ocasiones contrapuestos, de las partes involucradas, consiguiendo de la entidad auditada el reconocimiento de la profesionalidad del auditor al conseguir detectar los problemas existentes y proponer soluciones, y de la parte que promovió la auditoría el conseguir que se pueda conocer en dónde residían los problemas que no permitían alcanzar los objetivos deseables.

Pero debemos recordar que esta actividad no es un arte, sino una técnica, y como tal debe seguirse un orden y un método en el que nada se da por supuesto si no existe una evidencia objetiva que lo acredita. En ese conjunto de evidencias se apoyaran nuestras conclusiones, y de nuestra experiencia y *know how* saldrán las recomendaciones a proponer.

16.12. LECTURAS RECOMENDADAS

Cohen, L. *Inspection Moderators Handbook.* Maynard, M. A: Digital Equipment Corporation. 1991.

Freedman D. P. y Weinberg G. M. *Handbook of Walkthroughs, Inspections, and Technical Reviews, 1990.*

IEIE 1028 "Standard for Software Reviews and Audits".

16.13. CUESTIONES DE REPASO

1. Elabore su propia definición de "calidad".

2. ¿Qué características de la calidad define la norma ISO 9126?

3. Objetivos de las auditorías de la calidad.

4. ¿Qué prerrequisitos se exigen a los técnicos de desarrollo en un proceso de revisión?

5. Resuma las principales fases del proceso de auditoría software.

6. ¿Cómo se incluyen los procesos de auditoría en la norma ISO/IEC 12207?

7. Diferencias entre aseguramiento del producto y aseguramiento del proceso.

8. Elementos a incluir en un plan para el aseguramiento de la calidad.

9. ¿Qué conocimientos se requieren para poder llevar a cabo con éxito una auditoría de la calidad?

10. ¿Cómo explicaría a un director de informática las ventajas de llevar a cabo una auditoría de la calidad?

CAPÍTULO 17

AUDITORÍA DE LA SEGURIDAD

Miguel Ángel Ramos González

17.1. INTRODUCCIÓN

Para muchos la seguridad sigue siendo el área principal a auditar, hasta el punto de que en algunas entidades se creó inicialmente la función de auditoría informática para revisar la seguridad, aunque después se hayan ido ampliando los objetivos.

Ya sabemos que puede haber seguridad sin auditoría, puede existir auditoría de otras áreas, y queda un espacio de encuentro: la auditoría de la seguridad (figura 17.1), y cuya área puede ser mayor o menor según la entidad y el momento.

Figura 17.1. Encuentro entre seguridad y auditoría

Lo cierto es que cada día es mayor la **importancia de la información,** especialmente relacionada con sistemas basados en el uso de tecnologías de la información y comunicaciones, por lo que el impacto de los fallos, los accesos no autorizados, la

revelación de la información, y otras incidencias, tienen un impacto mucho mayor que hace unos años: de ahí la necesidad de protecciones adecuadas que se evaluarán o recomendarán en la auditoría de seguridad.

(También es cierto que en muchos casos tan necesario o más que la protección de la información puede ser que las inversiones en sistemas y tecnologías de la información estén alineadas con las estrategias de la entidad, huyendo del enfoque de la tecnología por la tecnología.)

Las áreas que puede abarcar la Auditoría Informática las recogía el autor de este capítulo en su tesis doctoral en 1990, y en líneas generales vienen a coincidir con las expuestas en esta obra.

En realidad, debemos ir hablando más de **Auditoría en Sistemas de Información** que sólo de Auditoría Informática, y no se trata de un juego de palabras sino de una actualización acorde con el nuevo enfoque y las áreas que llega a cubrir, y lejos ya de la denominación en inglés que seguimos viendo en muchos libros y artículos actuales –algunos citados en la bibliografía– EDP Audit, auditoría en proceso electrónico de datos (Electronic Data Processing).

La nueva denominación abarca globalmente los sistemas de información: desde la planificación, el alineamiento con las estrategias de las entidades, hasta los sistemas de información y el aprovechamiento de las tecnologías de la información aportan ventajas competitivas a la entidad, la gestión de los recursos, e incluso la medida de **la rentabilidad** de todo ello, que es quizá el único punto que personalmente temo cuando se nos sugiere a la hora de establecer objetivos de la auditoría.

Algunas entidades tienen detallados sus costes en la contabilidad analítica, pero ¿cómo cuantificar en algunas semanas las ventajas y los beneficios –algunos intangibles y difícilmente cuantificables– si la propia entidad no ha podido hacerlo en toda su existencia?

Como se indica en la figura 17.2, adaptada de la obra de Emilio del Peso y el propio Miguel A. Ramos *Confidencialidad y Seguridad de la Información: La LORTAD y sus aplicaciones socioeconómicas*, la **auditoría viene a ser el control del control.** (Recordemos que LORTAD significa Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de carácter personal.)

Volviendo a la seguridad, aunque solemos oír varias expresiones como seguridad informática, seguridad de los sistemas y tecnologías de la información, **seguridad –o protección– de la información,** puestos a elegir, y sin llegar a descartar ninguna, nos quedaríamos con la última, ya que los datos y la información son los activos más estratégicos y valiosos relacionados con los sistemas y el uso de las tecnologías de la información.

Figura 17.2. Auditoría como control del control

La expresión seguridad informática, que es la más usada, puede llegar a relacionarse, sólo con los equipos y los entornos técnicos, como si la información en otros soportes y ambientes no requiriera protección, cuando son las propias operaciones de la entidad, el negocio en entidades con ánimo de lucro, lo que requiere protección.

Si no existen suficientes y adecuadas medidas de protección se puede perder información vital, o al menos no estar disponible en el momento requerido (pensemos en diagnósticos de pacientes muy graves o en control de vuelos), las decisiones tomadas pueden ser erróneas, o se pueden incumplir contratos e incluso la propia legislación, lo que puede traducirse en grandes multas en el caso de infracciones graves, o lo que es aún peor: la inmovilización de los archivos prevista en la LORTAD.

Debe evaluarse en la auditoría si los **modelos de seguridad** están en consonancia con las nuevas arquitecturas, las distintas plataformas y las posibilidades de las comunicaciones, porque no se puede auditar con conceptos, técnicas o recomendaciones de hace algunos años (que en realidad no son tantos).

En cuanto a la **justificación de la auditoría,** que no parece necesaria en una obra de este tipo, sólo decir que tanto la normativa como la auditoría son necesarias: una auditoría no basada en políticas de la entidad auditada (además de las normas para realizar la auditoría) sería subjetiva y hasta peligrosa (aunque en sistemas de información es una situación habitual, que no normal); y la existencia de normativa sin auditoría podría equivaler a la no-existencia de la Guardia Civil de Tráfico, lo que incrementaría los accidentes e iría convirtiendo la circulación en caótica y peligrosa.

La realidad es que no se conocen datos completos y fiables sobre el nivel de protección de las entidades en España respecto a sistemas de información y vendrían bien algunas estadísticas.

En definitiva, como decía un cliente: "No pasan más cosas porque Dios es bueno", y podemos añadir, que no conocemos la mayor parte de las que pasan, porque ya se ocupan las entidades afectadas de que no se difundan.

Volviendo al **control,** los grandes grupos de controles son los siguientes, además de poderlos dividir en manuales y automáticos, o en generales y de aplicación:

- Controles **directivos,** que son los que establecen las bases, como las políticas, o la creación de comités relacionados o de funciones: de administración de seguridad o auditoría de sistemas de información interna.

- Controles **preventivos,** antes del hecho, como la identificación de visitas (seguridad física) o las contraseñas (seguridad lógica).

- Controles **de detección,** como determinadas revisiones de accesos producidos o la detección de incendios.

- Controles **correctivos,** para rectificar errores, negligencias o acciones intencionadas, como la recuperación de un archivo dañado a partir de una copia.

- Controles **de recuperación,** que facilitan la vuelta a la normalidad después de accidentes o contingencias, como puede ser un plan de continuidad adecuado.

Podemos hablar de **Objetivos de Control** respecto a la seguridad, que vienen a ser declaraciones sobre el resultado final deseado o propósito a ser alcanzado mediante las protecciones y los procedimientos de control, objetivos como los recogidos en la *publicación COBIT (Control Objectives for Information and Related Technologies)* de ISACA (Information Systems Audit and Control Association/Foundation).

Cada entidad ha de definir sus propios objetivos de control, en cuanto a seguridad y otras áreas, y crear y mantener un Sistema de Control Interno (funciones, procesos, actividades, dispositivos...) que puedan garantizar que se cumplen los objetivos de control.

Los auditores somos, en cierto modo, los **"ojos y oídos" de la Dirección,** que a menudo no puede, o no debe, o no sabe, cómo realizar las verificaciones o evaluaciones. (En cuanto a los ojos sigue existiendo en algunos sectores la figura clásica del veedor.)

En los informes se recomendará la implantación o refuerzo de controles, y en ocasiones incluso que se considere la supresión de algún control, si resulta redundante o ya no es necesario.

El **sistema de control interno** ha de basarse en las políticas, y se implanta con apoyo de herramientas, si bien encontramos a menudo en las auditorías que lo que existe es más bien la implantación parcial de controles de acceso lógico a través de paquetes o sistemas basada en el criterio de los técnicos, pero no sustentada en normativa, o bien habiendo partido ésta de los propios técnicos, sin aprobaciones de otro nivel.

La realidad es que el control interno no está generalizado en España fuera de los procesos que implican gastos, y especialmente pagos, pero existen otros riesgos tan importantes o más que las pérdidas monetarias directas, relacionados con la gestión adecuada de los recursos informáticos o con la propia protección de la información, que podrían suponer responsabilidades y pérdidas muy importantes para la entidad.

Cuando existe un sistema de control interno adecuado, los procesos de auditoría, especialmente si son periódicos, son revisiones necesarias pero más rápidas, con informes más breves; si el sistema de control interno es débil, la auditoría llevará más tiempo y esfuerzo, su coste será mayor, y las garantías de que se pongan en marcha las recomendaciones son mucho menores; en ocasiones la situación dista tanto de la ideal como la del paciente que se somete a un chequeo después de varios años sin control.

Finalmente, queremos indicar que por la lógica limitación de espacio no ha sido posible detallar más los puntos, ni incluir listas, que en todo caso sin estar referidas a ningún entorno y sector concreto y, por tanto, sin tener pesos, pueden dar resultados dudosos si quien las usa no sabe adaptarlas e interpretar sus resultados.

17.2. ÁREAS QUE PUEDE CUBRIR LA AUDITORÍA DE LA SEGURIDAD

Se incluyen las que con carácter general pueden formar parte de los objetivos de una revisión de la seguridad, si bien ésta puede abarcar sólo parte de ellas si así se ha determinado de antemano.

En una auditoría de otros aspectos –y, por tanto, en otros capítulos de esta misma obra– pueden también surgir revisiones solapadas con la seguridad; así, a la hora de revisar los desarrollos, normalmente se verá si se realizan en un entorno seguro y protegido, y lo mismo a la hora de revisar la explotación, o el área de técnica de sistemas, las redes, la informática de usuario final, las bases de datos... y en general cualquier área, salvo que expresamente se quiera pasar por alto la seguridad y

concentrarse en otros aspectos como pueden ser la gestión, costes, nivel de servicio, cumplimiento de procedimientos generales, calidad, o cualquier otro.

Volviendo a las áreas, las que se citan pueden ser objeto de la auditoría de seguridad, si bien en cada caso se habrán fijado los objetivos que más interesen, no considerando o por lo menos no con el mismo énfasis otros, si bien debiendo quedar claro y por escrito cuáles son esos objetivos, tanto cuando se trate de una auditoría interna como externa, en cuyo caso puede mediar un contrato o al menos una propuesta y carta de aceptación.

Las **áreas** generales citadas, algunas de las cuales se amplían después, son:

- Lo que hemos denominado controles directivos, es decir, los fundamentos de la seguridad: políticas, planes, funciones, existencia y funcionamiento de algún comité relacionado, objetivos de control, presupuesto, así como que existen sistemas y métodos de evaluación periódica de riesgos.

- El desarrollo de las políticas: procedimientos, posibles estándares, normas y guías, sin ser suficiente que existan estas últimas.

- Que para los grupos anteriores se ha considerado el marco jurídico aplicable, aspecto tratado en otros capítulos de esta obra, así como las regulaciones o los requerimientos aplicables a cada entidad: del Banco de España en el caso de las entidades financieras, del sector del seguro, los de la Comunidad Autónoma correspondiente, tal vez de su Ayuntamiento, o de la casa matriz las multinacionales o que formen parte de un grupo. Otro aspecto es el cumplimiento de los contratos.

- Amenazas físicas externas: inundaciones, incendios, explosiones, corte de líneas o de suministros, terremotos, terrorismo, huelgas...

- Control de accesos adecuado, tanto físicos como los denominados lógicos, para que cada usuario pueda acceder a los recursos a que esté autorizado y realizar sólo las funciones permitidas: lectura, variación, ejecución, borrado, copia... y quedando las pistas necesarias para control y auditoría, tanto de accesos producidos al menos a los recursos más críticos como los intentos en determinados casos.

- Protección de datos: lo que fije la LOPD en cuanto a los datos de carácter personal bajo tratamiento automatizado, y otros controles en cuanto a los datos en general, según la clasificación que exista, la designación de *propietarios* y los riesgos a que estén sometidos.

- Comunicaciones y redes: topología y tipo de comunicaciones, posible uso de cifrado, protecciones ante virus, éstas también en sistemas aislados aunque el impacto será menor que en una red.

- El entorno de Producción, entendiendo como tal Explotación más Técnica de Sistemas, y con especial énfasis en el cumplimiento de contratos en lo que se refiera a protecciones, tanto respecto a terceros cuando se trata de una entidad que presta servicios, como el servicio recibido de otros, y de forma especial en el caso de la subcontratación total o *outsourcing*.

- El desarrollo de aplicaciones en un entorno seguro, y que se incorporen controles en los productos desarrollados y que éstos resulten auditables.

- La continuidad de las operaciones.

No se trata de áreas no relacionadas, sino que **casi todas tienen puntos de enlace y partes comunes:** comunicaciones con control de accesos, cifrado con comunicaciones y soportes, datos con soportes y con comunicaciones, explotación con varias de ellas, y así en otros casos.

17.3. EVALUACIÓN DE RIESGOS

Se trata de identificar los riesgos, cuantificar su **probabilidad** e **impacto,** y analizar medidas que los eliminen –lo que generalmente no es posible– o que disminuyan la probabilidad de que ocurran los hechos o mitiguen el impacto.

Para evaluar riesgos hay que considerar, entre otros factores, el tipo de información almacenada, procesada y transmitida, la criticidad de las aplicaciones, la tecnología usada, el marco legal aplicable, el sector de la entidad, la entidad misma y el momento.

Para ello los auditores disponemos de listas, que normalmente incluimos en hojas de cálculo, o bien usamos paquetes, y tal vez en el futuro sistemas exentos. El problema sigue siendo la adaptación de los puntos a cada caso, y asignar el **peso** que puede tener cada uno de los puntos.

Desde la perspectiva de la auditoría de la seguridad es necesario revisar si se han considerado las **amenazas,** o bien evaluarlas si es el objetivo, y de todo tipo: errores y negligencias en general, desastres naturales, fallos de instalaciones, o bien fraudes o delitos, y que pueden traducirse en daños a: personas, datos, programas, redes, instalaciones, u otros activos, y llegar a suponer un peor servicio a usuarios internos y externos éstos normalmente clientes, imagen degradada u otros difícilmente

cuantificables, e incluso pérdida irreversible de datos, y hasta el fin de la actividad de la entidad en los casos más graves.

Para ello es necesario evaluar las vulnerabilidades que existen, ya que la cadena de protección se podrá romper con mayor probabilidad por los eslabones más débiles, que serán los que preferentemente intentarán usar quienes quieran acceder de forma no autorizada.

Debemos pensar que las medidas deben considerarse como **inversiones en seguridad,** aunque en algunos casos se nos ha dicho que no es fácil reflejarlas como activos contables ni saber cuál es su **rentabilidad;** podemos estar de acuerdo, pero ¿cuál es la rentabilidad de blindar la puerta de acceso a nuestro domicilio o la de instalar un antirrobo en nuestro automóvil? Esa rentabilidad la podemos determinar si los dispositivos o controles han servido para evitar la agresión, y a veces habrá constituido simplemente una medida disuasorio, sobre todo en seguridad lógica, y no llegaremos a conocer su efecto positivo.

En todo caso debemos transmitir a los auditados que, además, la seguridad tiene un impacto favorable en la imagen de las entidades (aunque esto sólo no suela justificar las inversiones), y tanto para clientes y posibles como para los empleados. Unos y otros pueden sentirse más protegidos, así como sus activos.

La protección no ha de basarse sólo en dispositivos y medios físicos, sino en formación e información adecuada al personal, empezando por la mentalización a los directivos para que, en cascada, afecte a todos los niveles de la pirámide organizativa.

El **factor humano** es el principal a considerar, salvo en algunas situaciones de protección física muy automatizados, ya que es muy crítico: si las personas no quieren colaborar de poco sirven los medios y dispositivos aunque sean caros y sofisticados.

Además, es conveniente que haya cláusulas adecuadas en los contratos, sean de trabajo o de otro tipo, especialmente para quienes están en funciones más críticas.

Es necesaria una separación de funciones: es peligroso que una misma persona realice una transacción, la autorice, y revise después los resultados (un diario de operaciones, por ejemplo), porque podría planificar un fraude o encubrir cualquier anomalía, y sobre todo equivocarse y no detectarse; por ello deben intervenir funciones/personas diferentes y existir controles suficientes.

En un proceso de auditoría, por tanto, se evaluarán todos estos aspectos y otros, por ejemplo si la seguridad es realmente una preocupación corporativa no es suficiente que exista presupuesto para ello; si las personas a diferentes niveles están mentalizadas, pues es necesaria una **cultura de la seguridad;** y si hay un comité que

fije o apruebe los objetivos correspondientes y en qué medida se alcanzan, qué modelo de seguridad se quiere implantar o se ha implantado, qué políticas y procedimientos existen: su idoneidad y grado de cumplimiento, así como la forma en que se realiza el desarrollo de aplicaciones, si el proceso se lleva a cabo igualmente en un entorno seguro con separación de programas y separación en cuanto a datos, si los seguros cubren los riesgos residuales, y si está prevista la continuidad de las operaciones en el caso de incidencias.

Una vez identificados y medidos los **riesgos,** lo mejor sería poder **eliminarlos,** pero ya hemos indicado que normalmente lo más que conseguimos es **disminuir** la probabilidad de que algo se produzca o bien su impacto: con sistemas de detección, de extinción, mediante revisiones periódicas, copiando archivos críticos, exigiendo una contraseña u otros controles según los casos.

Algunos manuales hablan de **transferir los riesgos,** por ejemplo contratando un seguro pero debemos recordar que si se pierden los datos la entidad aseguradora abonara el importe estipulado –si no puede acogerse a alguna cláusula en letra pequeña– pero la entidad seguirá sin recuperar los datos.

Otra posibilidad es **asumir los riesgos,** pero debe hacerse a un nivel adecuado en la entidad, y considerando que puede ser mucho mayor el coste de la inseguridad que el de la seguridad, lo que a veces sólo se sabe cuando ha ocurrido algo. ¿Cuál es el riesgo máximo admisible que puede permitirse una entidad? Alguna vez se nos ha hecho la pregunta, y depende de lo crítica que sea para la entidad la información así **como** disponer de ella, e incluso puede depender del momento: es un tema tan crítico que no puede generalizarse.

Algunos de los riesgos se han podido asumir de forma temporal, por estar en proceso de cambio las plataformas, las aplicaciones o las instalaciones, o por no existir presupuesto ante las grandes inversiones necesarias; en todos los casos debe constar por escrito que se asumen y quién lo hace, y ha de ser alguien con potestad para hacerlo, ya que a menudo son técnicos intermedios quienes asumen la responsabilidad sin poder hacerlo, o bien los directivos señalan a los técnicos cuando ocurre algo sin querer asumir ninguna responsabilidad.

Si la entidad auditada está en medio de un proceso de implantación de la seguridad, la evaluación se centrará en los objetivos, los planes, qué proyectos hay en curso y los medios usados o previstos.

La evaluación de riesgos puede ser global: todos los sistemas de información, centros y plataformas, que puede equivaler a un chequeo médico general de un individuo, y que es habitual la primera vez que se realiza, o bien cuando se ha producido el nombramiento de algún responsable relacionado, o cuando una entidad compra otra, pero puede producirse también una evaluación parcial de riesgos, tanto

por áreas como por centros, departamentos, redes o aplicaciones, así como previa a un proyecto, como puede ser una aplicación a iniciar.

A menudo en la auditoría externa se trata de saber si la entidad, a través de funciones como administración de la seguridad, auditoría interna, u otras si las anteriores no existieran, ha evaluado de forma adecuada los riesgos, si los informes han llegado a los destinatarios correspondientes y si se están tomando las medidas pertinentes, así como si el proceso se realiza con la frecuencia necesaria y no ha constituido un hecho aislado.

En estos casos se debe considerar la **metodología** que se sigue para evaluar los riesgos más que las **herramientas,** aunque sin dejar de analizar éstas, y si se han considerado todos los riesgos –al menos los más importantes– y si se han medido bien, ya que sobre todo cuando la evaluación se hace de forma interna por técnicos del área de sistemas de información, suelen minimizar los riesgos porque llevan años conviviendo con ellos o simplemente los desconocen.

La seguridad no es, un tema meramente técnico, aunque sean muy técnicas algunas de las medidas que haya que implantar.

Es necesaria la designación de **propietarios** de los activos, sobre todo los datos (por delegación de los titulares), y que son quienes pueden realizar la clasificación y autorizar las reglas de acceso; un buen propietario se interesará por los riesgos que puedan existir, por lo que promoverá o exigirá la realización de auditorías y querrá conocer, en términos no técnicos, la sustancia de los informes.

Al hablar de seguridad siempre se habla de sus tres dimensiones clásicas: confidencialidad, integridad y disponibilidad de la información, y algunos controles van más dirigidos a tratar de garantizar alguna de estas características.

La **confidencialidad:** se cumple cuando sólo las personas autorizadas (en un sentido amplio podríamos referirnos también a sistemas) pueden conocer los datos o la información correspondiente.

Podemos preguntarnos ¿qué ocurriría si un soporte magnético con los datos de los clientes o empleados de una entidad fuera cedido a terceros?, ¿cuál podría ser su uso final?, ¿habría una cadena de cesiones o ventas incontroladas de esos datos?

La LORTAD y la LOPD han influido positivamente en concienciarnos respecto a la confidencialidad.

La **integridad:** consiste en que sólo los usuarios autorizados puedan variar (modificar o borrar) los datos. Deben quedar pistas para control posterior y para auditoría.

Pensemos que alguien introdujera variaciones de forma que perdiéramos la información de determinadas deudas a cobrar (o que sin perderla tuviéramos que recurrir a la información en papel), o que modificara de forma aleatoria parte de los domicilios de algunos clientes.

Algunas de estas acciones se podrían tardar en detectar, y tal vez las diferentes copias de seguridad hechas a lo largo del tiempo estarían "viciadas" (corruptas decimos a veces), lo que haría difícil la reconstrucción.

La **disponibilidad:** se alcanza si las personas autorizadas pueden acceder a tiempo a la información a la que estén autorizadas.

El disponer de la información después del momento necesario puede equivaler a la falta de disponibilidad. Otro tema es disponer de la información a tiempo sin que ésta sea correcta, e incluso sin saberse, lo que puede originar la toma de decisiones, erróneas.

Más grave aún puede ser la ausencia de disponibilidad absoluta por haberse producido algún desastre. En ese caso, a medida que pasa el tiempo el impacto será mayor, hasta llegar a suponer la falta de continuidad de la entidad como ha pasado en muchos de los casos producidos (más de un 80% según las estadísticas).

Debe existir además **autenticidad:** que los datos o información sean auténticos, introducidos o comunicados por usuarios auténticos y con las autorizaciones necesarias.

17.4. FASES DE LA AUDITORÍA DE SEGURIDAD

Con carácter general pueden ser:

- Concreción de los objetivos y delimitación del alcance y profundidad de la auditoría, así como del período cubierto en su caso, por ejemplo revisión de accesos del último trimestre; si no se especifica, los auditores deberán citar en el informe el período revisado, porque podría aparecer alguna anomalía anterior, incluso de hace mucho tiempo, y llegarse a considerar una debilidad de la auditoría.

- Análisis de posibles fuentes y recopilación de información: en el caso de los internos este proceso puede no existir.

- Determinación del plan de trabajo y de los recursos y plazos en caso necesario, así como de comunicación a la entidad.
- Adaptación de cuestionarios, y a veces consideración de herramientas o perfiles de especialistas necesarios, sobre todo en la auditoría externa.
- Realización de entrevistas y pruebas.
- Análisis de resultados y valoración de riesgos.
- Presentación y discusión del informe provisional.
- Informe definitivo.

17.5. AUDITORÍA DE LA SEGURIDAD FÍSICA

Se evaluarán las protecciones físicas de datos, programas, instalaciones, equipos, redes y soportes, y por supuesto habrá que considerar a las personas: que estén protegidas y existan medidas de evacuación, alarmas, salidas alternativas, así como que no estén expuestas a riesgos superiores a los considerados admisibles en la entidad e incluso en el sector, por ejemplo por convenio o normativa específica; y si bien todos estos aspectos suelen ser comunes con las medidas generales de la entidad, en una auditoría de sistemas de información nos preocupamos especialmente por quienes están en el área o de los daños que puedan afectar a los usuarios de los sistemas si entra dentro dé la auditoría.

Las **amenazas** pueden ser muy diversas: sabotaje, vandalismo, terrorismo, accidentes de distinto tipo, incendios, inundaciones, averías importantes, derrumbamientos, explosiones, así como otros que afectan a las personas y pueden impactar el funcionamiento de los centros, tales como errores, negligencias, huelgas, epidemias o intoxicaciones.

(Hay algo más que no recogemos en los informes, pero convencidos de que se trata de una amenaza real sí lo comentamos verbalmente a veces en la presentación del informe o en cursos a sabiendas de que produce comentarios: la lotería; si toca en un área un premio importante, juegan todos el mismo número, y no existen sustitutos o no hay una documentación adecuada –pensemos en un grupo que mantiene una aplicación– se puede originar un problema importante, y la prevención no es fácil porque no se puede impedir el hecho.)

Desde la perspectiva de las **protecciones físicas** algunos aspectos a considerar son:

- Ubicación del centro de procesos, de los servidores locales, y en general de cualquier elemento a proteger, como puedan ser los propios terminales, especialmente en zonas de paso, de acceso público, o próximos a ventanas en plantas bajas. Protección de computadores portátiles, incluso fuera de las oficinas: aeropuertos, automóviles, restaurantes...

- Estructura, diseño, construcción y distribución de los edificios y de sus plantas.

- Riesgos a los que están expuestos, tanto por agentes externos, casuales o no, como por accesos físicos no controlados.

- Amenazas de fuego (materiales empleados); riesgos por agua: por accidentes atmosféricos o por averías en las conducciones; problemas en el suministro eléctrico, tanto por caídas como por perturbaciones.

- Controles tanto preventivos como de detección relacionados con los puntos anteriores, así como de acceso basándose en la clasificación de áreas según usuarios, incluso según día de la semana y horario.

- Además del acceso, en determinados edificios o áreas debe controlarse el contenido de carteras, paquetes, bolsos o cajas, ya que podrían contener explosivos, así como lo que se quiere sacar del edificio, para evitar sustituciones o sustracción de equipos, componentes, soportes magnéticos, documentación u otros activos.

  El control deberá afectar a las visitas, proveedores, contratados, clientes... y en casos más estrictos igualmente a los empleados; los ex empleados se deberán considerar visitas en todo caso.

- Protección de los soportes magnéticos en cuanto a acceso, almacenamiento y posible transporte, además de otras protecciones no físicas, todo bajo un sistema de inventario, así como protección de documentos impresos y de cualquier tipo de documentación clasificada.

  Es fácil y barato obtener copias magnéticas periódicas de datos y de programas frente al perjuicio que nos puede causar el no haberlo hecho; es mucho más difícil o caro, o no es posible, obtener copias con igual valor de otros objetos o activos como obras de arte.

Todos los puntos anteriores pueden, además, estar cubiertos por seguros.

17.6. AUDITORÍA DE LA SEGURIDAD LÓGICA

Es necesario verificar que cada usuario sólo pueda acceder a los recursos a los que le autorice el propietario, aunque sea de forma genérica, según su función, y con las posibilidades que el propietario haya fijado: lectura, modificación, borrado, ejecución... trasladando a los sistemas lo que representaríamos en una **matriz de accesos** en la que figuraran los **sujetos:** grupos de usuarios o sistemas, los **objetos** que puedan ser accedidos con mayor o menor **granularidad:** un disco, una aplicación, una base de datos, una librería de programas, un tipo de transacción, un programa, un tipo de campo... y para completar la tripleta, las posibilidades que se le otorgan: lectura, modificación, borrado, ejecución...

Desde el punto de vista de la auditoría es necesario revisar cómo se identifican y sobre todo autentican los usuarios, cómo han sido autorizados y por quién, y qué ocurre cuando se producen transgresiones o intentos: quién se entera y cuándo y qué se hace.

En cuanto a autenticación, hasta tanto no se abaraten más y generalicen los sistemas basados en la **biométrica,** el método más usado es la **contraseña,** cuyas características serán acordes con las normas y estándares de la entidad, que podrían contemplar diferencias para según qué sistemas en función de la criticidad de los recursos accedidos.

Algunos de los aspectos a evaluar respecto a las **contraseñas** pueden ser:

- Quién asigna la contraseña: inicial y sucesivas.
- Longitud mínima y composición de caracteres.
- Vigencia, incluso puede haberlas de un solo uso o dependientes de una función tiempo.
- Control para no asignar las "x" últimas.
- Número de intentos que se permiten al usuario, e investigación posterior de los fallidos: pueden ser errores del usuario o intentos de suplantación.
- Si las contraseñas están cifradas y bajo qué sistema, y sobre todo que no aparezcan en claro en las pantallas, listados, mensajes de comunicaciones o corrientes de trabajos (JCL en algunos sistemas).
- Protección o cambio de las contraseñas iniciales que llegan en los sistemas, y que a menudo aparecen en los propios manuales.

- Controles existentes para evitar y detectar caballos de Troya: en este contexto se trata de un programa residente en un *PC* que emulando un terminal simule el contenido de la pantalla que recoge la identificación y contraseña del usuario, grabe la contraseña y devuelva control al sistema verdadero después de algún mensaje simulado de error que normalmente no despertará las sospechas del usuario.

- La no-cesión, y el uso individual y responsable de cada usuario, a partir de la normativa.

Siempre se ha dicho que la contraseña ha de ser difícilmente imaginable por ajenos y fácilmente recordable por el propio usuario, y este último aspecto se pone en peligro cuando un mismo usuario ha de identificarse ante distintos sistemas, para lo que puede asignar una misma contraseña, lo que supone una vulnerabilidad si la protección es desigual, por ser habitual que en pequeños sistemas o aplicaciones aisladas las contraseñas no están cifradas o lo estén bajo sistemas vulnerables; si opta por asignar varias contraseñas puede que necesite anotarlas.

La solución más adecuada por ahora puede consistir en utilizar **sistemas de identificación únicos *(single sign-on)*** que faciliten la administración y el acceso, permitiéndolo o no a según qué usuarios/sistemas/funciones, o bien adoptar cualquier otro tipo de solución que, con garantías suficientes, pueda propagar la contraseña entre sistemas.

En la auditoría debemos verificar que el proceso de altas de usuarios se realiza según la normativa en vigor, y que las autorizaciones requeridas son adecuadas, así como la gestión posterior como variaciones y bajas, y que los usuarios activos siguen vigentes, y si se revisa cuáles son inactivos y por qué, por ejemplo contrastando periódicamente con la base de datos de empleados y contratados. Debiera estar previsto bloquear a un usuario que no accediera en un período determinado, ¿35 días?

Otra posible debilidad que debe considerarse en la auditoría es si pueden crearse **situaciones de bloqueo** porque sólo exista un administrador, que puede estar ausente de forma no prevista, por ejemplo por haber sufrido un accidente, e impedir la creación nuevos usuarios en un sistema de administración centralizada y única; en más de una ocasión, según de qué entorno se trate hemos recomendado la existencia de algún usuario no asignado con perfil especial y contraseña protegida que pueda utilizar alguien con autoridad en caso de emergencia: todas sus operaciones deberán quedar registradas para control y auditoría.