Capítulo 3
Auditar y evaluar un sistema de información

1. Auditar es describir y calificar

Auditar un sistema de información consiste en comprenderlo en su globalidad y complejidad, identificando lo que constituye su fuerza, su debilidad y los riesgos de degradarlo. Para eso, tenemos que disponer de una herramienta que permita, por un lado, describir la situación sin omisiones y sin dejar nada en la sombra y, por otro lado, calificar lo existente para tener una visión crítica. La 2MSI nos aporta el soporte metodológico necesario:

– La matriz de 21 piezas nos permite organizar las investigaciones y no dejar nada al margen.

– Los tres criterios de supervisión, y sus nueve subcriterios, nos dan las herramientas para calificar el nivel de funcionamiento del SI.

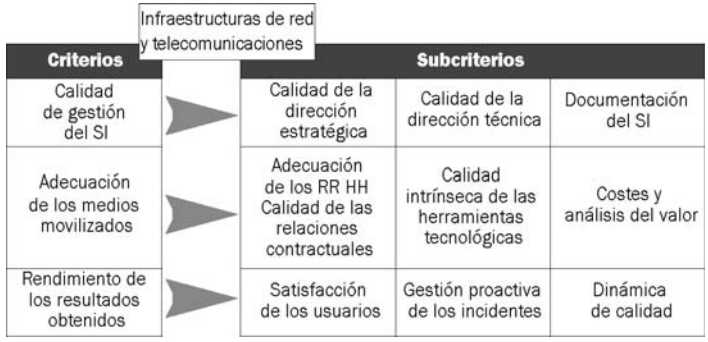
A continuación, suponemos que la auditoría se realiza en la totalidad del sistema de información tomado como objeto.

2. La matriz 2MSI estructura la metodología de la auditoría

La realización de la auditoría supone identificar y recopilar los datos necesarios para caracterizar el sistema de información de la organización. Para cada una de las piezas de la matriz 2MSI, se trata de realizar una dinámica de evaluación.

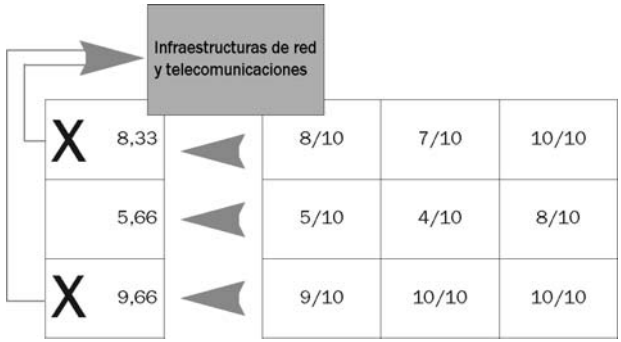
Así, si consideramos la pieza infraestructuras de red y telecomunicaciones, la primera en la parte superior izquierda de la matriz, habrá que aplicarle los tres criterios y nueve subcriterios anteriormente definidos, para establecer el estado del SI en este campo.

Análisis de la pieza infraestructuras de red y telecomunicaciones



Para calificar este estado, atribuimos una nota de 1 a 10 a cada uno de los tres subcriterios. La nota depende de su nivel de satisfacción. La media de los subcriterios permite obtener una valoración del criterio, que se considera satisfecho si obtiene al menos 8.

Valoración de la pieza infraestructuras de red y telecomunicaciones



Cada pieza (en este caso, la pieza infraestructuras de red y telecomunicaciones) se evalúa según la cantidad de criterios satisfechos y lleva un color:

- Pieza gris claro: tres criterios satisfechos. Quizás es necesario hacer mejoras, pero la política aplicada en este ámbito funcional es suficientemente madura para garantizar su parte dentro de la coherencia del SI.
- Pieza gris medio: dos criterios satisfechos. Hay una política activa, pero está incompleta. Acciones indispensables.
- Pieza gris oscuro: un único criterio satisfecho. La política aplicada es pobre y pone en peligro la coherencia del SI. Es conveniente iniciar inmediatamente un plan de acción.
- Pieza negra: ningún criterio satisfecho, lo que expresa una casi ausencia de política de gestión del SI en el campo interesado. Estamos en presencia de una zona de peligro absoluto.

En este ejemplo, dos criterios satisfechos, la pieza es de color gris medio.

Así, el método 2MSI permite una monitorización gráfica de la situación del SI. Proporciona, de manera muy visual, un informe de los campos prioritarios de acción.

Ejemplo de monitorización coloreada tras la auditoría del SI por una pyme de servicios

Infraestructuras de redes y telecomunicaciones	Supervisión y operación de red. Gestión operadores de red y telecomunicaciones	Integridad, seguridad y PRA red y telecomunicaciones
Servidores (Alojamiento y OS)	Supervisión y operación de servidores	Integridad, seguridad y PRA de datos y configuraciones
Dispositivos (PC, tableta y smartphone)	Soporte y operación de dispositivos, Helpdesk	Seguridad dispositivos
Edición e impresión	Soporte y operación de flotas de edición e impresión, Helpdesk	Seguridad Confidencialidad Costes
Usuarios (directorios, correo y ofimática)	Gestión de derechos, correo y ofimática	Seguridad y PRA directorios, correo y acceso
Aplicaciones de negocio	Supervisión y operación aplicaciones de negocio. Relaciones de editores	Seguridad, integridad y PRA aplicaciones de negocios
Riesgos	Supervisión de riesgos. Evaluación de impactos	Aseguradoras, asesoría legal. Gestión de crisis

En el ejemplo que aparece aquí arriba, se observa que la política de gestión del SI comporta dos zonas negras (seguridad de los entornos de usuarios y seguridad de los entornos de negocio), dos zonas en alerta (seguridad de los entornos de servidores y gestión de los entornos de usuarios) y seis zonas debilitadas (gestión de los activos de red, soporte de los usuarios, seguridad de las herramientas personales, gestión de las relaciones de editores, supervisión de riesgos y gestión de impactos en materia de riesgos). Esta monitorización coloreada permite identificar inmediatamente los ámbitos donde se deben iniciar acciones prioritarias.

3. La matriz 2MSI organiza la información necesaria para la realización de la auditoría

Una vez definido el método, la cuestión principal que se plantea el auditor es inventariar la materia que necesita para calificar lo que tiene que auditar. Dentro de esta perspectiva, nos apoyamos en los nueve subcriterios de valoración para organizar este inventario, respondiendo para cada uno de ellos a dos preguntas: ¿qué debo observar o recoger? ¿Qué método voy a usar para recoger y tratar esta información?

A continuación, retomamos un ejemplo de inventario elaborado para auditar el SI de uno de nuestros clientes, Spicojeu, como un importante establecimiento público industrial y comercial:

Calificar la calidad de la dirección estratégica

Elementos a observar o recoger	Métodos de recogida y tratamiento
Organigrama y definición de las responsabilidades.	Observación. Entrevistas. Estudio de descripciones de puestos de trabajo. Si es necesario, reconstitución de las descripciones de puestos de trabajo.
Herramienta de gestión de proyectos: informes de comités de dirección, cuadros de indicadores, herramientas de creación de informes, posición de la dirección estratégica en los procedimientos.	Observación. Entrevistas. Estudio de los documentos.
Competencia del interviniente delegado de la dirección estratégica. Posición en la organización.	Observación. Entrevistas. Estudio de los CV. Entrevistas con la dirección superior.

Calificar la calidad de la dirección técnica

Elementos a observar o recoger	Métodos de recogida y tratamiento
Organigrama y definición de las responsabilidades.	Observación. Entrevistas. Estudio de las descripciones de puestos de trabajo. Si es necesario, reconstitución de las descripciones de puestos de trabajo. O estudio de los contratos de prestaciones o de infogerencia.
Herramientas de gestión de proyectos: informes de comités de dirección, cuadros de indicadores, herramientas de creación de informes y posición de la dirección técnica en los procedimientos. Herramientas de gestión de procedimiento.	Observación. Entrevistas. Estudio de los documentos. Estudio de los procedimientos y de los métodos de intervención operativa.
Competencia de las direcciones técnicas. Posición en la organización.	Observación. Entrevistas. Estudio de los CV. Entrevistas con la dirección superior. Entrevistas con los directores estratégicos.

Calificar la política de documentación del SI

Elementos a observar o recoger	Métodos de recogida y tratamiento
Herramientas de gestión de la documentación básica: instrucciones, manuales, licencias, programas y códigos. Base de conocimientos. Método de protección y de clasificación.	Verificación durante la auditoría *in situ*. Análisis de los documentos entregados. Verificación mediante sondeo aleatorio.
Herramientas de gestión de la documentación operativa del SI: inventarios, textos descriptivos, planos e informes de intervención. Base de conocimientos. Método de protección y de clasificación.	Verificación durante la auditoría *in situ*. Análisis de los documentos entregados. Verificación mediante sondeo aleatorio.
Herramientas de gestión de la documentación de estructuración operativa del SI: fichas de procedimiento, listas de verificación, plan de gestión de los riesgos y plan de recuperación de actividad.	Verificación durante la auditoría *in situ*. Análisis de los documentos entregados. Verificación mediante sondeo aleatorio.