

1. Objetivo

El programa que se adjunta como anexo (MFSC-2858.1) está diseñado para:

- Ayudar a obtener información sobre los sistemas de información de la entidad fiscalizada, que complemente la obtenida mediante el cuestionario MFSC-2857.1.
- Identificar actividades y objetivos de control relacionadas con los CGTI.
- Evaluar el diseño y eficacia de los CGTI de la entidad auditada.
- Documentar los procedimientos llevados a cabo, la evidencia obtenida y las conclusiones alcanzadas respecto a la eficacia e implementación de los CGTI.
- Identificar la existencia de deficiencias en esos controles que puedan derivar en riesgos significativos de auditoría.

2. Cuándo procede aplicar este procedimiento

El programa adjunto se cumplimentará cuando tras cumplimentar el procedimiento descrito en MFSC-2857 se concluya que es necesario ampliar el conocimiento sobre la situación de los CGTI.

Este procedimiento ha sido diseñado para ser completado por personal con conocimientos básicos sobre CGTI. En general se realizará por una persona de la Unidad de Auditoría de Sistemas de Información y Apoyo (UASI).

3. Estructura del formulario

Dada la amplitud de las áreas afectadas por las TI, los CGTI se agrupan en las siguientes áreas:

- A. Marco organizativo
- B. Gestión de cambios en aplicaciones y sistemas
- C. Operaciones de los sistemas de información
- D. Acceso a datos y programas
- E. Continuidad del servicio

Todas estas áreas de gestión de TI son críticas para configurar y mantener la integridad, confidencialidad, disponibilidad de la información financiera.

También hay un último apartado: F. Conclusión; que se cumplimentará conjuntamente por el auditor/técnico responsable y el jefe de la UASI.

4. Cómo completar el formulario

Los cuadros que recogen los *Objetivos y actividades CGTI* tienen las siguientes columnas:

a) Objetivos y actividades de control

Las actividades de control sobre cada objetivo son ejemplos genéricos de controles que una entidad debe tener implantados y no una relación completa de todas las actividades de control posibles. La entidad puede tener otras actividades de control para lograr el mismo objetivo. El auditor deberá modificar la tabla en cada sección para reflejar las actividades de control propias de la entidad, específicas para su casuística, que se han implantado para conseguir unos determinados objetivos de control en materia de TI.

Por tanto, las actividades de control no sean aplicables deberán eliminarse y se añadirán aquellas otras que sean pertinentes. El auditor solo necesita obtener el conocimiento necesario de las actividades de control de la entidad que permitan alcanzar cada objetivo de control. Por tanto, si existen varias actividades de control para un único objetivo, no es necesario obtener información sobre todas ellas.

b) Descripción de los CGTI

Esta columna debe utilizarse para describir los procedimientos y políticas de control que la entidad auditada ha implementado para lograr los objetivos de control.

c) Cambios respecto al año anterior

Esta columna se ha incluido por dos razones:

1. Para identificar aquellas actividades de control que no han cambiado significativamente desde el ejercicio anterior. Para estos controles, el auditor puede determinar que es posible confiar en el trabajo realizado en anteriores auditorías para evaluar la eficacia e implementación de los controles

en el año corriente, después de llevar a cabo los procedimientos necesarios para asegurar que la evidencia obtenida sobre los controles en ejercicios anteriores continúa siendo válida.

2. Para identificar aquellas actividades de control que han cambiado de forma significativa desde el ejercicio anterior. Para estos controles, el auditor deberá llevar a cabo procedimientos dirigidos a evaluar la implementación y la eficacia de los controles. Adicionalmente, el auditor debe determinar si el cambio afecta, elimina o crea riesgos de errores materiales que habían sido identificados a través de procedimientos de análisis de riesgos realizados y documentados anteriormente.

d) Procedimientos realizados/Referencia

El auditor debe documentar los procedimientos establecidos y las fuentes utilizadas para obtener la información sobre el control interno. Esta columna debe usarse para documentar estas materias o para detallar la referencia a los documentos en que se ha archivado esta información. El auditor puede elegir entre documentar estos procedimientos para cada objetivo de control o para cada actividad de control (es decir, para cada línea).

La documentación debe incluir, como mínimo, las siguientes materias:

- **Cuestionarios.** Se facilitará al responsable del departamento de TI el cuestionario general para la revisión de los controles generales de los sistemas de información (MFSC-2857.1 o MFSC-2859).
- **Entrevistas.** Incluyen las entrevistas individuales, descripción del puesto de trabajo y las respuestas a las preguntas formuladas (tener en cuenta que las entrevistas por sí solas, no son suficientes para evaluar el diseño y eficacia de un control relevante y determinar si este ha sido implementado).
- **Inspección de documentos.** Incluye la identificación de las características de los documentos analizados. Estas características pueden incluir, por ejemplo, el título del documento, cuando fue preparado y quien lo preparó.
- **Observaciones.** Identifican el proceso o materia que está siendo analizada, el personal clave y sus responsabilidades y cuando se llevó a cabo el trabajo.

e) Adecuadamente diseñado e implementado

Esta columna debe utilizarse para documentar la conclusión del auditor sobre si el control ha sido adecuadamente diseñado e implementado. Evaluar el diseño de un control implica considerar si el control, individualmente o en combinación con otros controles, es capaz de detectar, impedir y corregir efectivamente errores materiales. La implementación de un control significa que el control existe y que la entidad lo está aplicando.

Nota: La ausencia de un control o el inadecuado diseño de un control no implica que el sistema de control interno de la entidad no tenga un adecuado diseño. En muchos casos, pueden existir controles compensatorios para mitigar el riesgo causado por la ausencia o ineficacia de un control. Por ejemplo, una entidad de reducidas dimensiones puede dejar de aplicar la segregación de funciones sobre una tarea en particular, lo que, por sí mismo, puede ser una deficiencia de control. Sin embargo, la implicación directa de los responsables en el seguimiento y control de la tarea puede compensar eficazmente la falta de una adecuada segregación de funciones.

5. Conclusión del trabajo

Una vez cumplimentado el formulario, se concluirá conjuntamente por el auditor/técnico responsable y el jefe de la UASI, sobre

- Conclusiones generales sobre los controles revisados.
- Identificar y evidenciar las deficiencias de control detectadas y proponer controles compensatorios.
- Identificar y documentar riesgos concretos de errores materiales sobre los estados financieros.
- Necesidad de trabajo adicional.

6. Ubicación de la documentación

La información obtenida (el programa cumplimentado), las evidencias y las conclusiones sobre las mismas se documentarán en el proyecto de papeles de trabajo electrónicos creado para la fiscalización (TeamMate) dentro de un área creada para la revisión de los sistemas de información.