# La Auditoría Interna en los Sistemas de Información

"LOS DESAYUNOS DE MAZARS"

MAZARS

# « Los Desayunos de Mazars »: Objetivos

- **MAZARS** ha puesto en marcha una serie de Desayunos de Trabajo con el objetivo de …

  - **Reunir a profesionales** de diferentes empresas con responsabilidades en **Auditoría Interna, Control Interno y Gestión de Riesgos,** a fin de crear un **espacio de reflexión común** sobre cómo abordar la **Auditoría y el Control Interno** a nivel general y, en particular, **de los Sistemas de Información**

  - **Ofrecer la posibilidad de buscar, conjuntamente, soluciones concretas** a las cuestiones que se dan en el día a día y **ayudar** a los asistentes **en la toma de decisiones** en su ámbito de responsabilidad empresarial

  - **Dar acceso a especialistas de Mazars**, colaboradores externos y comentar **temas novedosos** y **casos reales** en los que ha participado **Mazars**

# Cada sesión, un contacto permanente

## Un intercambio continuo

- Las dudas o temas de interés, que les preocupan podrán ser enviados a la dirección Auditoria.IT@Mazars.es, y serán objeto de una *"FAQ"*, dentro de cada Boletín.
- Nuestro equipo queda a vuestra disposición para cualquier tema que queráis abordar en una sesión o dentro de un boletín.

## Resultados

- **Un desayuno cada tres meses…**
- **… y un boletín también cada tres meses.**

# La Auditoría Interna en los Sistemas de Información

## ORDEN DEL DÍA

MAZARS

# AGENDA DEL DÍA

- 9:15 Presentación de MAZARS
- 9:30 CCI - 99: Cumplimiento del Control Interno basado en SAS 99
  - Introducción a SAS 99
  - Controles de: Frecuencia, Patrones Numéricos, Materialidad, Horario y Descripción
  - Ejemplos con hojas Excel
- 10:30 Café
- 11:00 Auditoría interna de procesos automatizados
  - Introducción a CobiT
  - Controles de Aplicación
  - Guías de Auditoría
- 11:45 Últimas novedades
- 12:00 Conclusiones y próximos desayunos

# La Auditoría Interna en los Sistemas de Información

MAZARS, UNA ORGANIZACIÓN INTERNACIONAL INTEGRADA

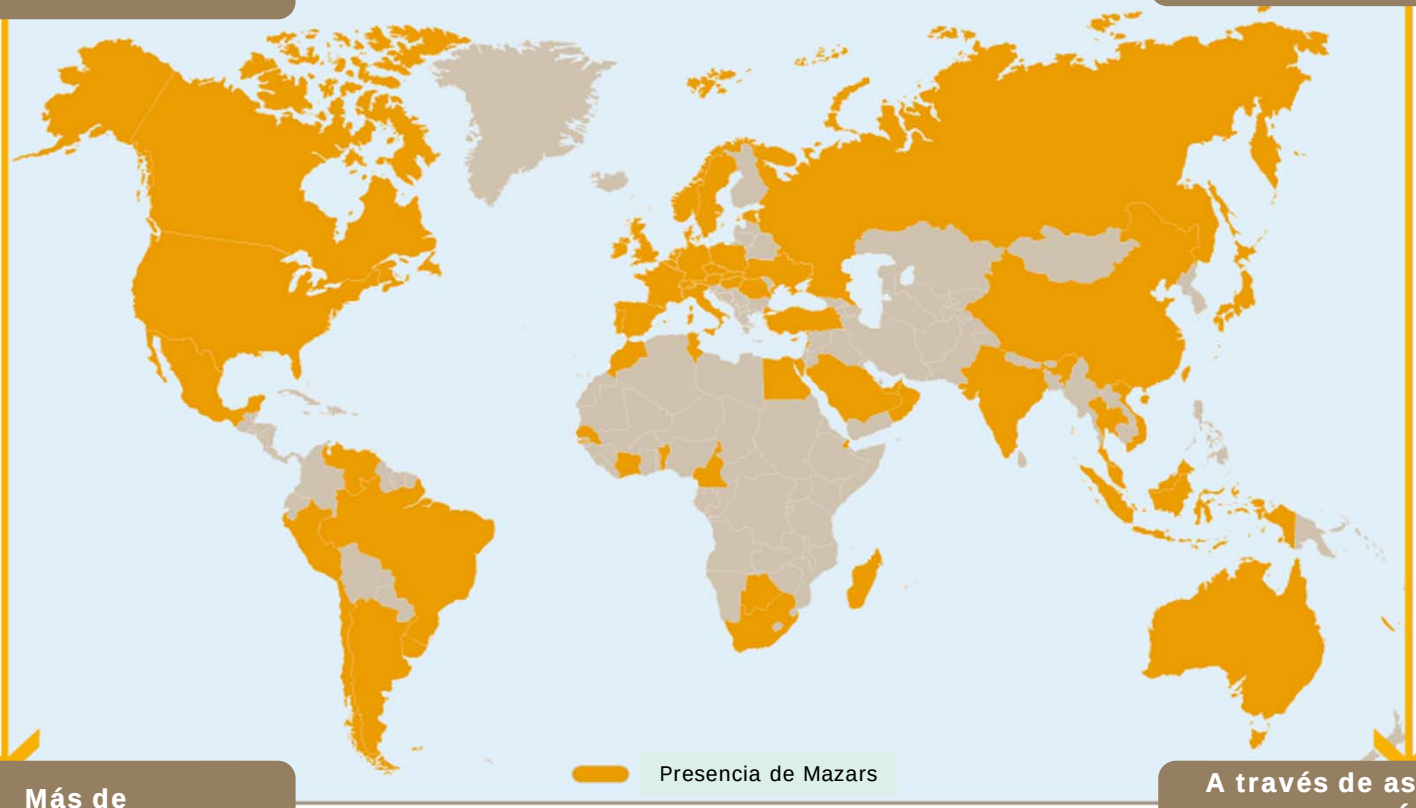
MAZARS

# Una organización internacional integrada

## Clasificada del 5º al 10º puesto en el ranking de firmas de auditoría en los países donde está presente

**Una organización integrada en 56 países**

**Capacidad de asistir a nuestros clientes en otros 22 países**




**Más de 12.500 profesionales**

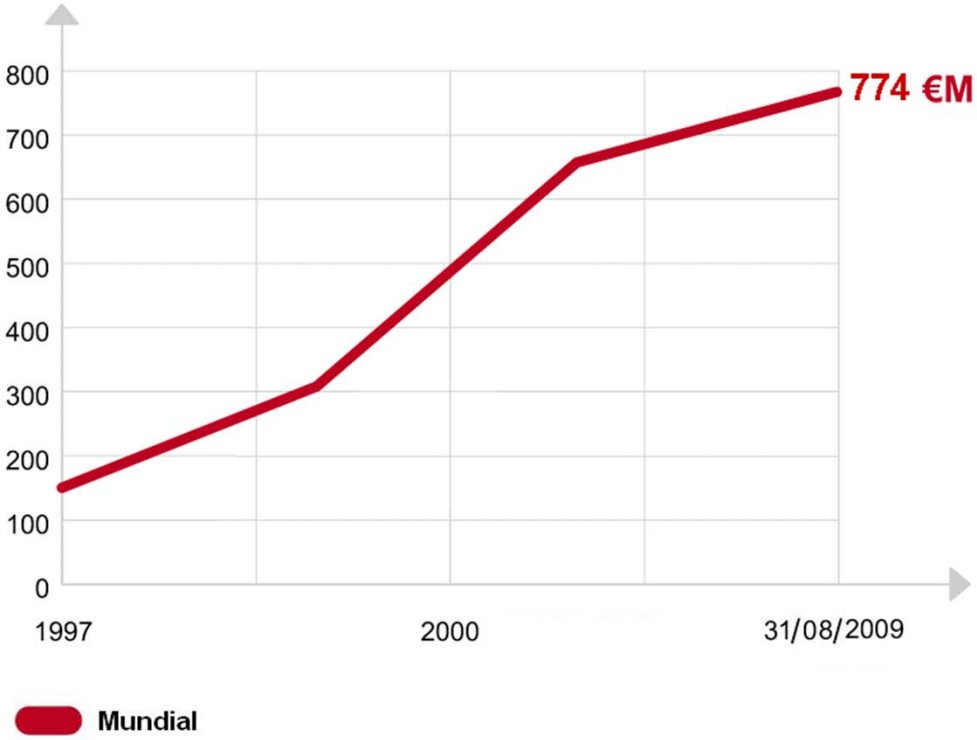
**A través de asociaciones con más de 25.000 profesionales**



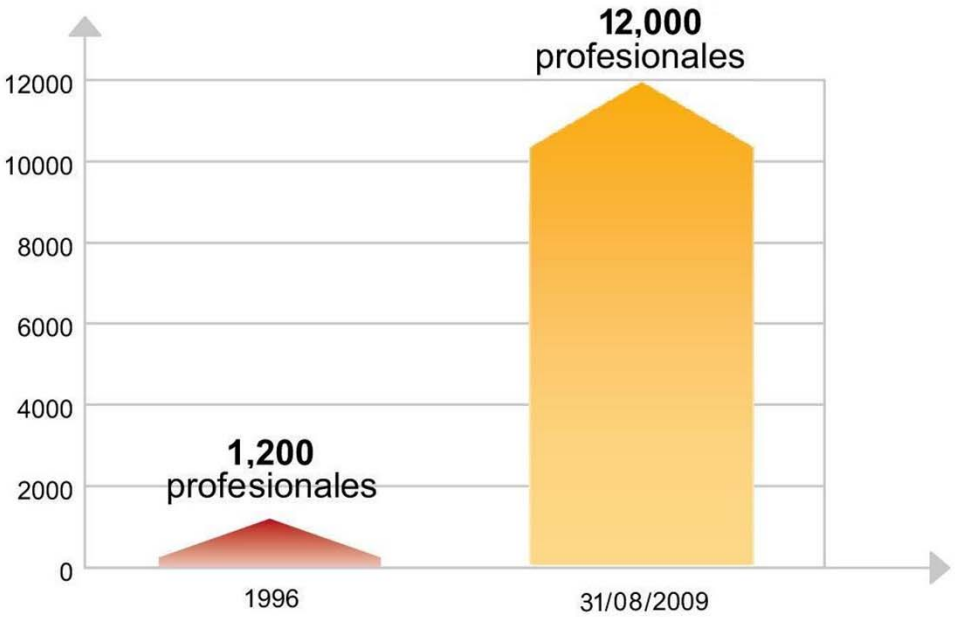
MAZARS

# Una organización internacional integrada

## … nuestra prioridad: la **calidad**




## … para asegurar la **continuidad**

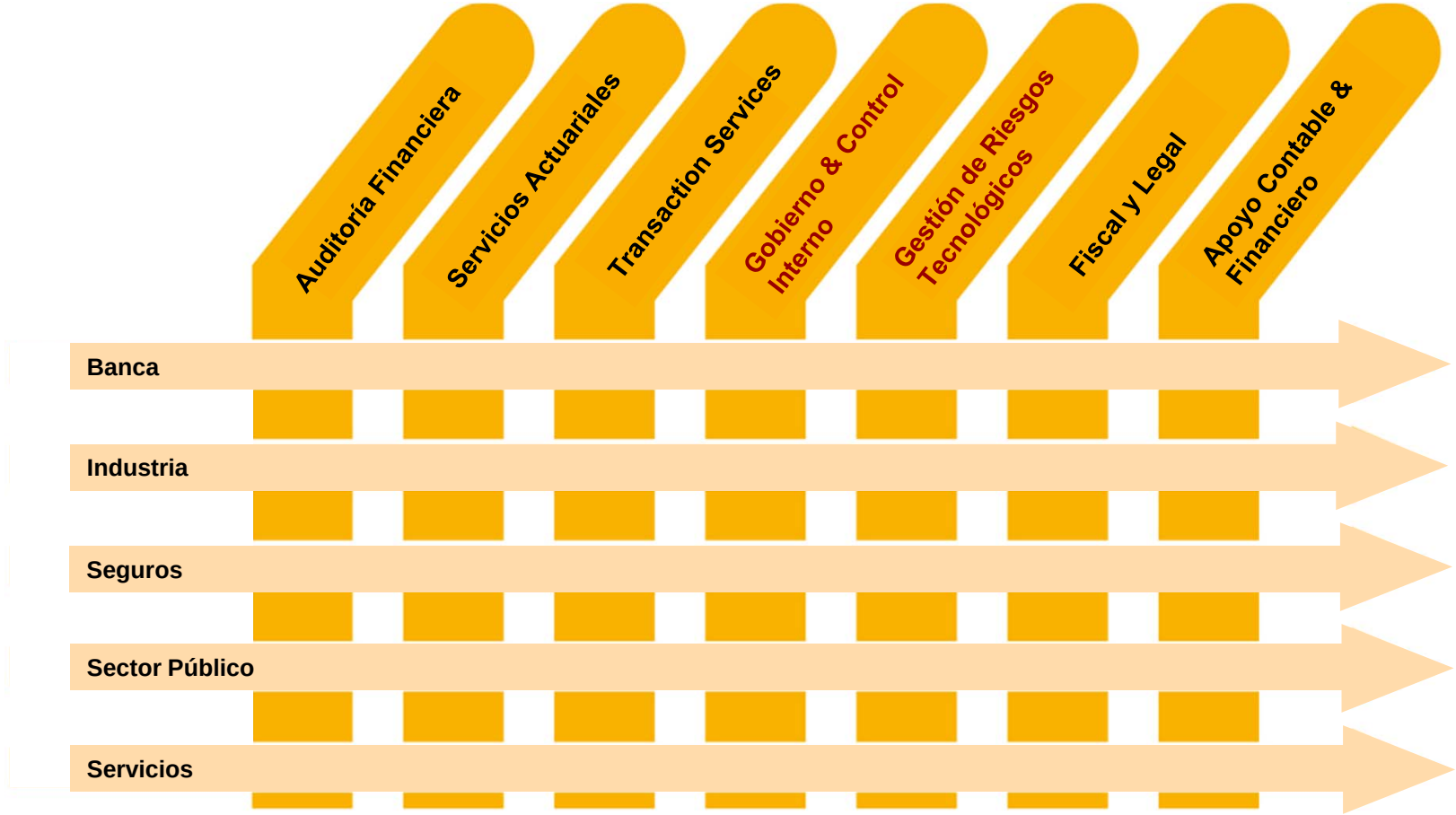





MAZARS

# Organización matricial entre líneas de servicio y sectores de clientes

## … para cumplir con las **necesidades** de nuestros **clientes**

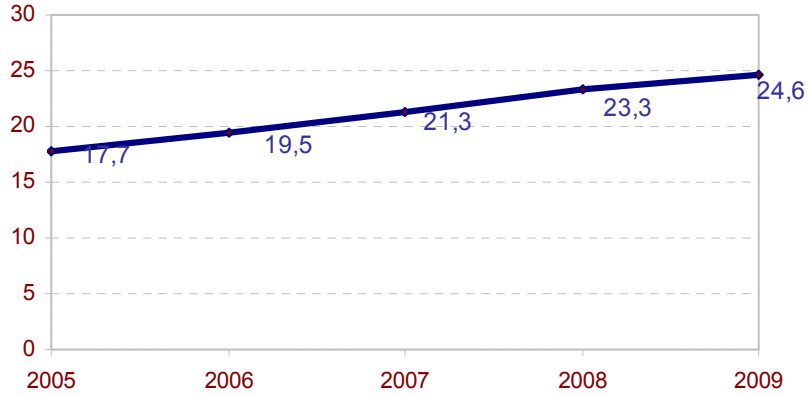




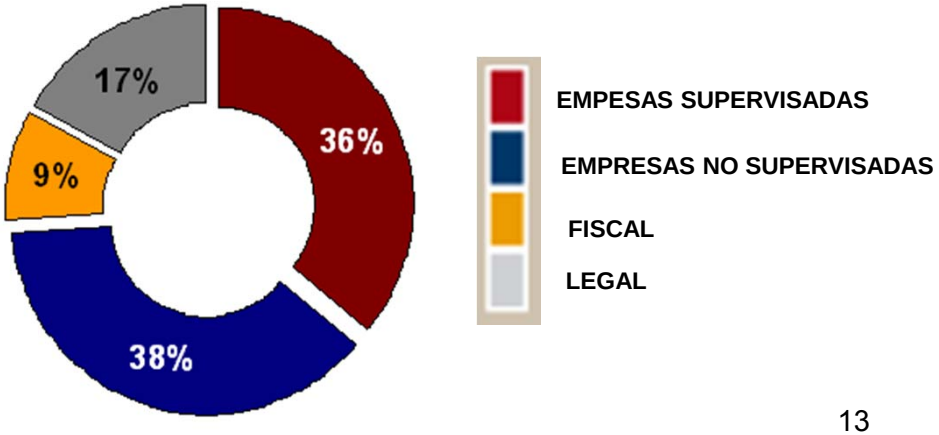

MAZARS

# Mazars España en cifras

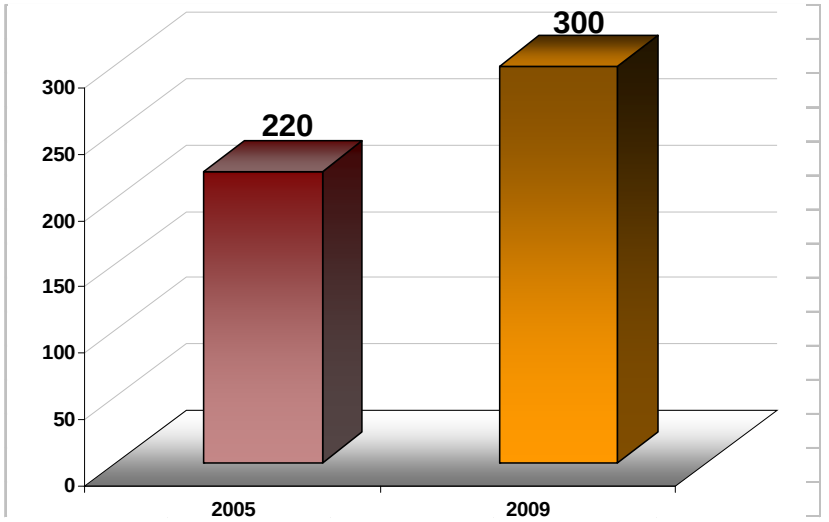

## Evolución de la cifra de negocios (M€)




## Cifra de negocios por ICL




## Número de profesionales






MAZARS


# INTRODUCCIÓN A LA AUDITORÍA INTERNA DE PROCESOS AUTOMATIZADOS

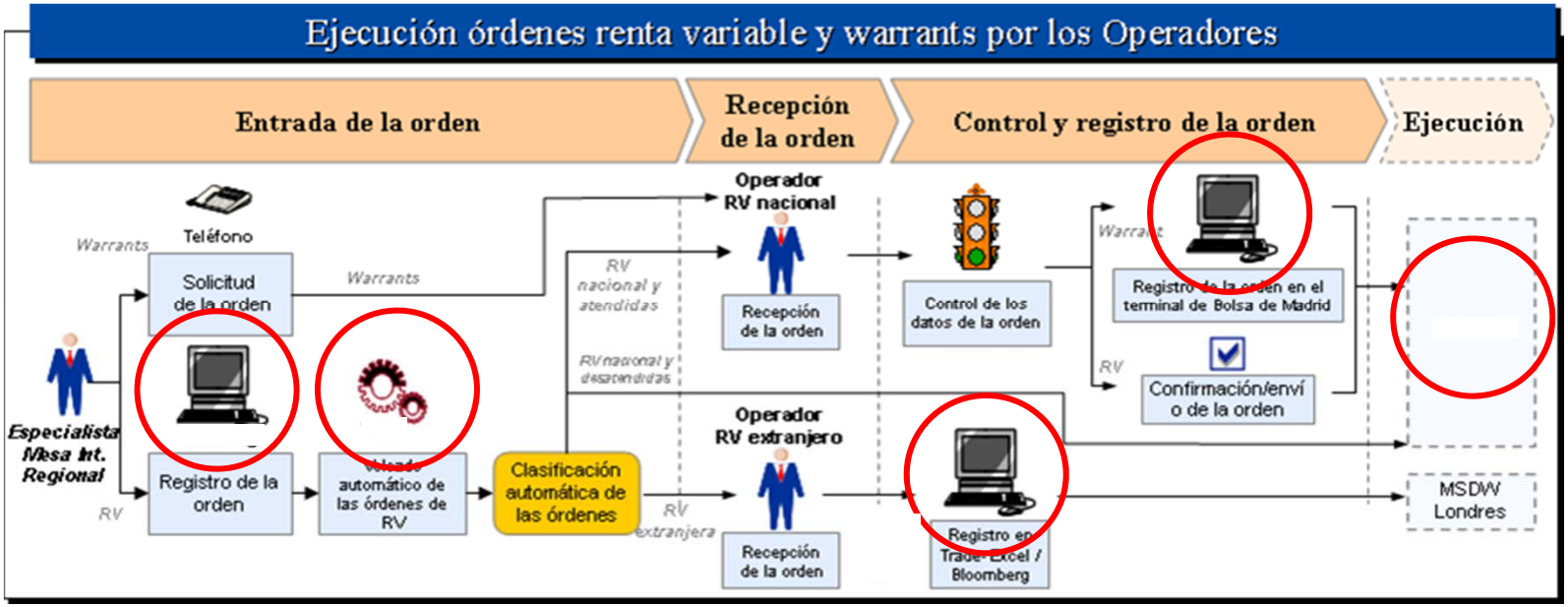
MAZARS

## Auditoría integrada de los procesos de negocio

Los equipos integrados por auditores internos y auditores de información disminuyen el riesgo de auditoría, frente a las revisiones independientes.

De esta forma la auditoría cubre la revisión de todo el proceso, con independencia de si finalmente los controles son automatizados o manuales, y verificando conjuntamente **la adecuación y eficacia de los controles en respuesta a los riesgos del gobierno, operaciones y sistemas de información de la organización**, respecto:

- La fiabilidad e integridad de la información financiera y operativa,
- La eficacia y eficiencia de las operaciones, ….






MAZARS

# La Auditoría Interna en los Sistemas de Información

## CCI-99: CUMPLIMIENTO DEL CONTROL INTERNO BASADO EN SAS 99

MAZARS

# CCI-99: CUMPLIMIENTO DEL CONTROL INTERNO BASADO EN SAS 99

- **¿Qué es CCI-99?**
- Plan de Trabajo
- Controles efectuados
  - Controles de Frecuencia
  - Controles de Patrones Numéricos
  - Controles de Materialidad
  - Controles de Horario
  - Controles de Descripción
- Estimación de Recursos

# Consideraciones previas

## Un problema creciente y de gran actualidad

El fraude y la gestión del riesgo de fraude han tomado una relevancia muy significativa como consecuencia de las diversas regulaciones que en uno u otro modo hacen mención a las prácticas internas para la prevención y detección del fraude. Normativas como la Ley Sarbanes-Oxley, la FCPA, Basilea II, COSO y otras de naturaleza similar tanto a nivel internacional como local (Prevención Blanqueo).

Esta presión regulatoria, combinada por los diferentes escándalos está haciendo reaccionar a las organizaciones en el establecimiento de políticas para la identificación, prevención y detección de actividades fraudulentas.

Es conveniente destacar que el contexto de crisis económica actual está favoreciendo la detección de fraude, ya sea porque los excesos cometidos en un contexto de bonanza, y que hizo que no fueran evidentes, ahora con la caída de actividad se hacen más visibles, o bien, porque las sociedades han endurecido el control, o una conjunción de ambos.

# Consideraciones previas

## ¿Qué entendemos por fraude?

Por fraude entendemos un acto voluntario por el que una persona o grupo de personas, consejeros, directivos o empleados y/o terceras partes, emplean algún tipo de engaño para obtener un beneficio o ventaja injusta o ilegal, **con perjuicio** para la empresa.

El fraude al que se enfrentan las empresas con más frecuencia es el interno, que involucra a sus directivos y/o empleados, y que puede dañar tanto sus activos como su imagen pública. Los fraudes más comunes en las empresas se pueden agrupar en las tres categorías siguientes:

| Apropiación de activos | Manipulación de la información financiera | Corrupción |
|---|---|---|
| Sustracción de activos de la empresa o el uso de los mismos para obtener un beneficio propio (cash/non cash) | Presentación de cifras no ajustadas a la realidad o de informaciones incompletas | Aquellos casos en los que reciben o pagan tratos de favor para la adjudicación de un producto o servicio. (Sobornos, Comisiones, uso de inform. privilegiada) |

# Consideraciones previas

## ¿Cuál es el perfil del defraudador?

Cuando analizamos los resultados de los controles orientados a detectar o mitigar el riesgo de fraude hay mitos que debemos desterrar, como son:

- La mayoría de las personas no son capaces de cometerlo
- El fraude es inmaterial o bien el control interno lo reduce a cifras inmateriales
- Es un coste más de la actividad

… entre otros.

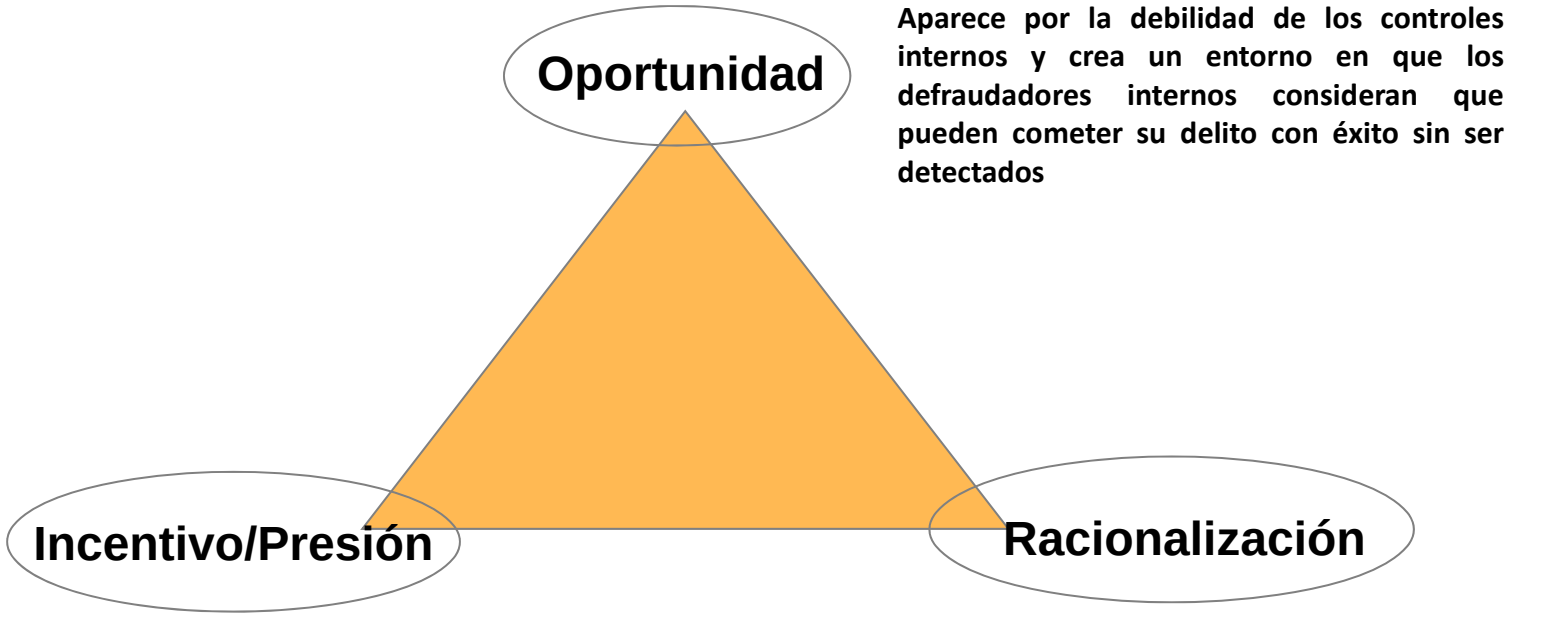
La realidad nos demuestra que el fraude existe en todas las organizaciones y a todos los niveles y que el control interno tiene limitaciones en cuanto a su prevención (colusión, errores, coste/beneficio). Por lo tanto, el escepticismo profesional es una máxima en el análisis del fraude (la honestidad pasada no garantiza la futura).

Al respecto, un dato interesante es que la variedad de estudios existentes, aunque ninguno se centra específicamente en el perfil latino que nos caracteriza, muestra a un defraudador típico como:

- Cargo directivo con más de 3 años antigüedad en la empresa
- Se trata de un varón y que actúa sólo
- Una edad comprendida entre 35 y 55 años

# Consideraciones previas

## ¿Por qué se cometen fraudes?




Destacar que el contexto actual se está incrementando la presión sobre los empleados de las compañías (reducción bonus, congelaciones salariales, Eres temporales, presión orientar cifras), factor que incrementa el incentivo para que se produzcan fraudes.

# Consideraciones previas

## ¿Qué están haciendo las sociedades?

| Prevención | Detección | Respuesta |
|---|---|---|
| ▸ Evaluación de los riesgos de fraude y de la ética profesional<br>▸ Controles y programas antifraude (Código conducta, políticas, procedimientos)<br>▸ Comunicación y formación<br>▸ Revisión de las prácticas de contratación de personal y selección de clientes y proveedores<br>▸ Supervisión de la dirección | ▸ Mecanismos anónimos de comunicación de fraude<br>▸ Pruebas de prevención de fraude y cumplimiento de controles<br>▸ Verificación de la seguridad informática<br>▸ **Análisis electrónicos de datos** | ▸ Protocolos de investigación interna<br>▸ Aseguramiento de las pruebas para posteriores procedimientos judiciales.<br>▸ Pautas de actuación RRHH y medidas de resolución<br>▸ Protocolos de revelación de información al mercado |

No existen estándares detallados y universales que definan con precisión los elementos de una política antifraude, así como estudios que permitan comparar las prácticas y controles antifraude de una empresa con los de sus competidores.

Se exige un análisis particular y adaptado a las necesidades específicas de cada empresa.

# Consideraciones previas

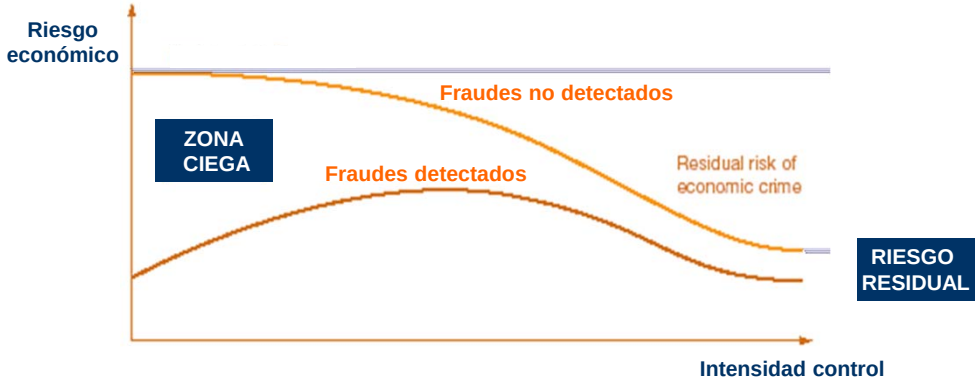
## ¿Qué se obtiene del análisis de datos?

Como hemos dicho uno de los controles que están efectuando las compañías es el análisis electrónico de datos, que como veremos a continuación, consiste en la interrogación de una forma estructurada de ficheros que contienen datos financieros con unos controles automáticos previamente definidos.

Al respecto es conveniente destacar que en este tipo de análisis los factores de riesgo de fraude no necesariamente indican la existencia de fraude; sin embargo, a menudo el fraude se presenta en alguno de estos indicios.

No obstante obtenemos otros resultados de la aplicación de análisis de datos como son:

- Identificación de debilidades de control interno
- Ineficiencias administrativas
- Implicación de la dirección
- Disuasión del fraude




Los planes anuales de auditoría interna, deberían incluir al menos pruebas de detección, si estas no están puestas en marcha por la propia organización. En este contexto presentamos a continuación una herramienta que puede resultar de gran utilidad para la detección de los indicios de fraude.

# ¿Qué es CCI – 99?

**CCI – 99: es un servicio de Análisis de Datos que procesa la información contable de una entidad en base a unos controles establecidos.**

- **Propone una batería de controles basados en SAS – 99.**
- **Servicio flexible, aplicable al entorno de Control Interno específico de cada organización.**

## Objetivos principales

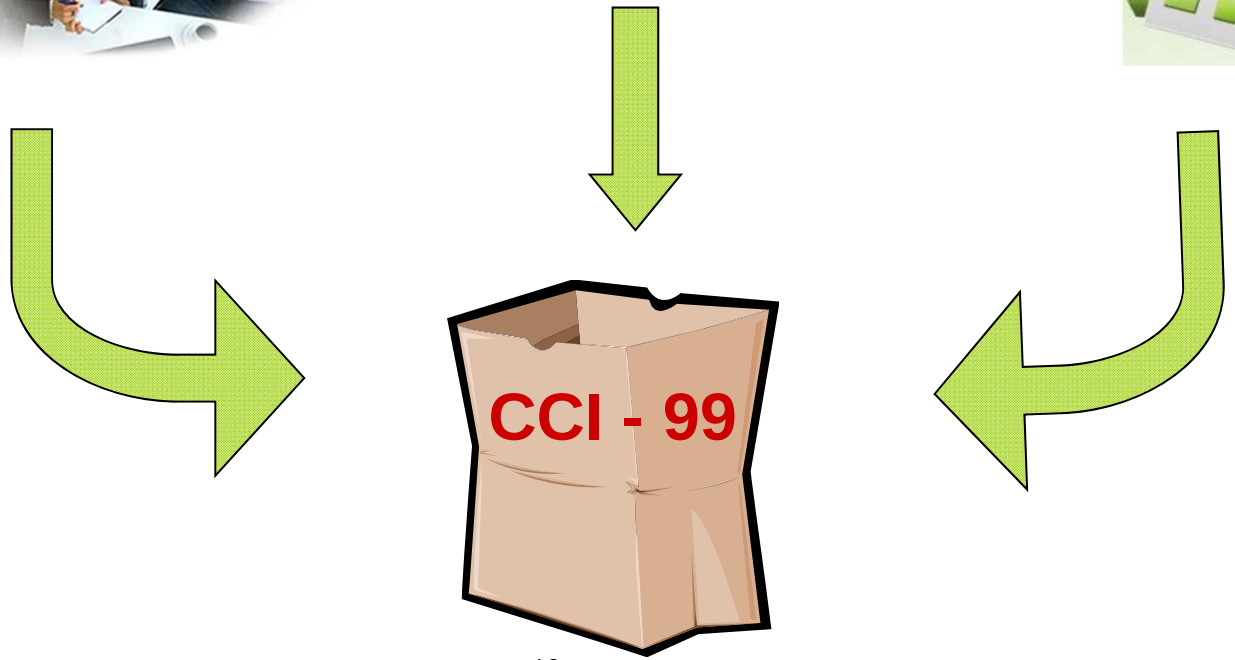
- ✓ Obtener conclusiones, a partir del **análisis de datos**, que colaboren con la organización en la **evaluación periódica del estado del Control Interno**.
- ✓ Minimizar la carga de trabajo de la organización gracias **al uso de controles automatizados**.
- ✓ Ofrecer un sistema capaz de analizar datos almacenados en **formatos heterogéneos.**
- ✓ **Identificar fraudes** potenciales presentes en la operativa diaria de la organización.
- ✓ Evaluar un conjunto de controles basados en un **estándar internacional (SAS 99).**

# ¿Qué es CCI – 99?

## Metodología


## Estándar

## Aplicaciones

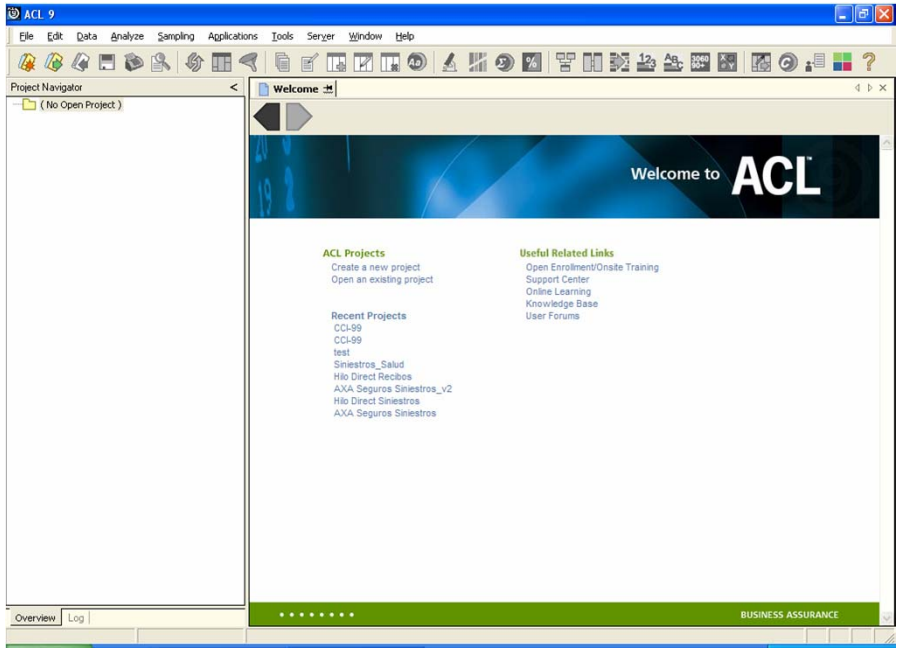



MAZARS

**El Análisis de Datos es una técnica de auditoría asistida por ordenador (CAAT) que aplica controles automáticos.**

- **Permite detectar anomalías en los datos de un sistema de información, provocadas por un usuario o por un sistema informático.**
- **Permite identificar riesgos en la operativa diaria.**
- **Implementado a través de la herramienta ACL.**

- ***Audit Command Language***
- *Herramienta para el análisis y tratamiento masivo de datos.*
- *No tiene límite de volumen de datos manejados.*
- *No altera los datos de origen manejados (acceso de solo lectura).*
- *Facilidades de reporte de resultados.*



# Statement on Auditing Standards (SAS) 99

**Statement on Auditing Standards No. 99 (SAS 99): "Consideración del Fraude en una Auditoría de Estados Financieros".**

- **Declaración de normas de auditoría emitidas por el Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA), en octubre de 2002.**
- **Seguridad razonable de que los estados financieros no contienen errores importantes, causados por error o fraude.**

## Aspectos principales de la declaración

- ☑ Descripción y características del fraude
- ☑ Escepticismo profesional
- ☑ Compromiso respecto a riesgos de fraude
- ☑ Información necesaria para identificar fraude
- ☑ Identificación de los riesgos que pudieran resultar en fraude
- ☑ Evaluación de los riesgos identificados
- ☑ Respuesta a los resultados de la evaluación
- ☑ Evaluación de la evidencia de auditoría
- ☑ Reporte del fraude a la dirección
- ☑ Documentación del fraude por parte del auditor

# SAS 99. Aspectos principales

## Descripción y características del Fraude

- Diferencia entre error y fraude: el fraude es intencionado (dificultad de demostrar la intención)
- Tipos de fraude: información financiera falsa y apropiación indebida (desfalco)
- Condiciones presentes en el fraude: móvil; oportunidad y actitud ("Triángulo de Fraude")

## Escepticismo profesional y riesgo de fraude

- Independiente del pasado "honesto" de la entidad
- Actitud escéptica del auditor frente a la gerencia

## Compromiso respecto al riesgo de fraude

- Identificación de posibles puntos críticos por parte del equipo auditor
- Conocimiento de la cultura y tipo de negocio de la organización.

# SAS 99. Aspectos principales

## Información necesaria para identificar fraude

- Averiguaciones propuestas para la gerencia, comité de auditoría, auditoría interna, empleados, etc.
- Propuesta de procedimientos de análisis para la auditoría.
- Propuesta de oportunidades de riesgo.

## Identificación de los riesgos que pueden resultar en fraude

- Considerar el “Triángulo de Fraude”
- Considerar en el riesgo el tipo de fraude, dimensión e impacto

## Evaluación de los riesgos identificados considerando aplicaciones y controles

- Conocimiento del Control Interno
- Evaluación de los resultados esperados de programas y controles

# SAS 99. Aspectos principales

## Respuesta a los resultados de la evaluación de riesgos

- Recomendaciones de mejora frente a los riesgos identificados
- Incremento del seguimiento y la fiabilidad de los controles
- Inventarios, análisis de libros diarios, identificación activos críticos, etc.

## Evaluación de la evidencia de auditoría

- Obtención de la evidencia in-situ
- Identificación de registros contables que pueden identificar fraude
- Consideración de fraude con “baja” repercusión contable
- Consideraciones de integridad y validez de las evidencias

## Reporte del fraude a la dirección

- Considerar el nivel adecuado, habitualmente el comité de auditoría
- Considerar las implicaciones internas

## Documentación del fraude por parte del auditor

- Incluir descripciones detalladas con actores y roles
- Procedimiento de documentación y aporte de evidencias
- Evidencias claras e irrefutables

# CCI-99: CUMPLIMIENTO DEL CONTROL INTERNO BASADO EN SAS 99

- ¿Qué es CCI-99?
- **Plan de Trabajo**
- Controles efectuados
  - Controles de Frecuencia
  - Controles de Patrones Numéricos
  - Controles de Materialidad
  - Controles de Horario
  - Controles de Descripción
- Estimación de Recursos

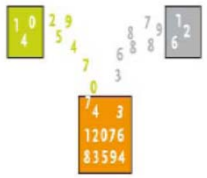
# Plan de Trabajo de CCI - 99

**Extracción de datos**

1

**Adecuación de formato**

2

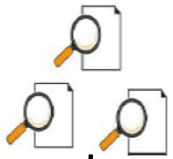


**Análisis de datos**

3

**Investigaciones complementarias**

4



**Presentación de conclusiones y resultados**

5



MAZARS

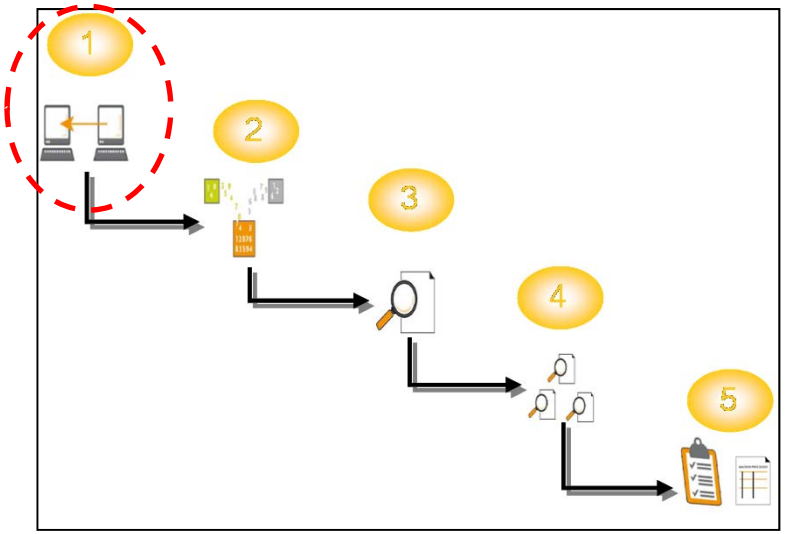
# Plan de Trabajo de CCI – 99. Extracción de datos

## *OBJETIVOS*

Obtener la **información financiera relevante** de la Entidad para su procesamiento y posterior análisis en la herramienta.

## *ACTIVIDADES*

- Interacción con la Entidad para la identificación de la información financiera relevante para su análisis.
- Extracción de la información financiera de los sistemas de la entidad.
- Agrupación de la información en forma de conjunto de transacciones contables.
- Volcado de la información a un dispositivo accesible por el equipo de Mazars.



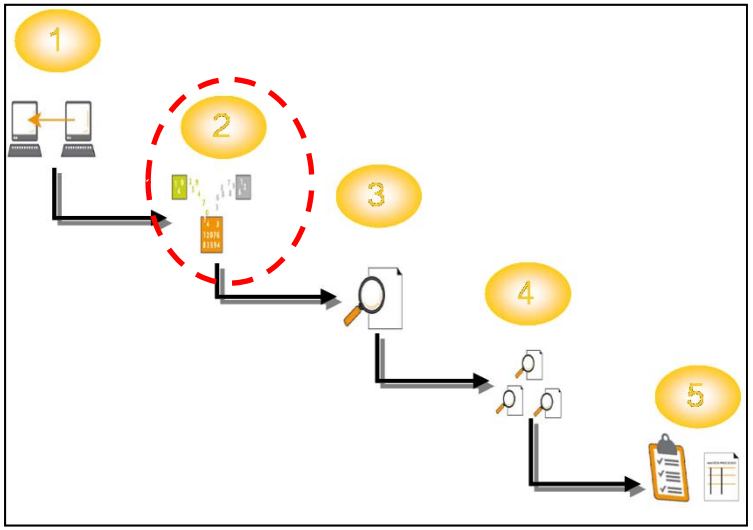

## *RESULTADOS*

- Conjunto de transacciones financieras, almacenadas en formato digital, accesible por el equipo de Mazars.

# Plan de Trabajo de CCI – 99. Adecuación de formato

## *OBJETIVOS*

Adaptar la información financiera procedente de la Entidad a un **formato legible por la herramienta** de análisis de CCI-99, manteniendo la integridad de los datos.




## *ACTIVIDADES*

- Conversión de la información financiera recibida a tablas legibles por la herramienta ACL.
- Obtención de una **tabla única de transacciones** que agrupe la totalidad de la información recibida de la entidad, manteniendo la integridad de los datos.
- Adaptación de la tabla única al formato establecido para las queries definidas de ACL.

## *RESULTADOS*

- **Tabla única** de transacciones que contenga la **totalidad de la información** financiera de la entidad, **adaptada al formato** de la herramienta.

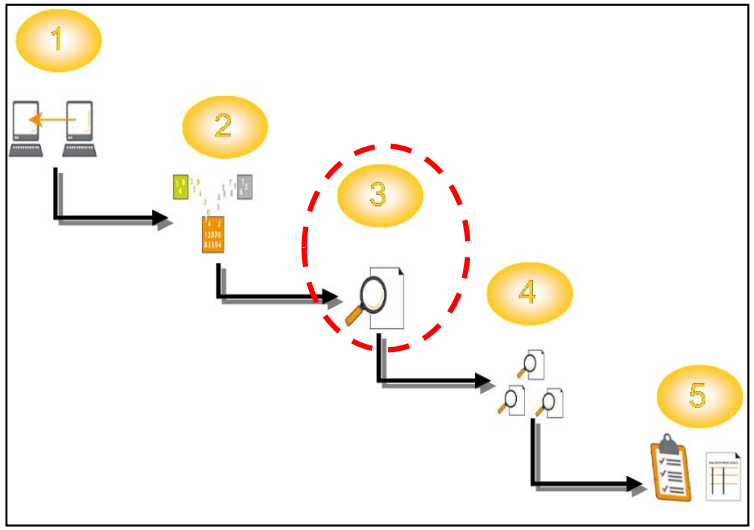
# Plan de Trabajo de CCI – 99. Análisis de datos

## *OBJETIVOS*

Efectuar la **batería de controles,** acordados con la Entidad sobre la información financiera recabada en los pasos anteriores.

## *ACTIVIDADES*

- Interacción con la Entidad para la obtención de los **parámetros de configuración** necesarios para ejecutar los controles acordados.
- Configuración de ACL para que ejecute los controles acordados.
- **Ejecución de los "scripts"** de ACL que implementan cada uno de los controles, introduciendo los parámetros de configuración obtenidos de la Entidad.
- Adaptación del formato de las hojas Excel de resultado generadas por la herramienta.




## *RESULTADOS*

- **Parámetros de configuración** necesarios para la ejecución de la totalidad de los controles.
- **Hojas Excel** de resultado de cada uno de los controles.

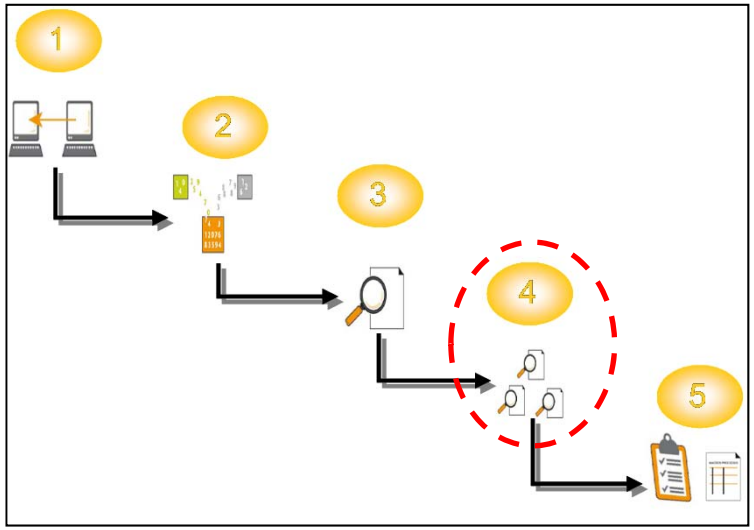
# Plan de Trabajo de CCI – 99. Investigaciones complementarias

## *OBJETIVOS*

Efectuar el **análisis y controles adicionales** que la Entidad pueda considerar necesarios.

## *ACTIVIDADES*

- Interacción con la Entidad para la obtención de los **controles adicionales** que se desean efectuar sobre la información financiera.
- Obtención de los posibles **parámetros de configuración** necesarios para la ejecución de los controles adicionales.
- **Implementación y ejecución de los controles** adicionales en ACL
- **Obtención de las hojas Excel** y adaptación de la funcionalidad a los controles efectuados.
- Adaptación del formato de las hojas Excel de resultado generadas por la herramienta.




## *RESULTADOS*

- **Parámetros de configuración** necesarios para la ejecución de los controles adicionales.
- **Hojas Excel** de resultado de los controles adicionales

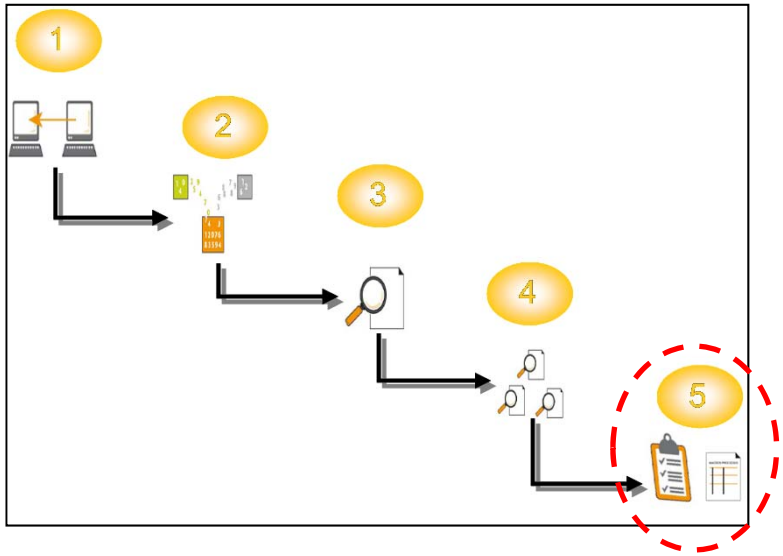


MAZARS

# Plan de Trabajo de CCI – 99. Conclusiones y resultados

## *OBJETIVOS*

Realizar un análisis general de los resultados obtenido tras la ejecución de los controles




## *ACTIVIDADES*

- **Evaluar los resultados** obtenidos a partir de las hojas Excel.
- Generar un **Resumen Ejecutivo** con los principales aspectos destacados de los resultados de cada uno de los controles.
- Agrupar y enviar a la Entidad el conjunto de **hojas Excel obtenidas junto con el Resumen Ejecutivo,** que facilite el posterior análisis por parte de la Entidad.

## *RESULTADOS*

- **Resumen Ejecutivo** de los aspectos destacados de los resultados.
- **Hojas Excel** de resultado del conjunto de controles efectuados.

# CCI-99: CUMPLIMIENTO DEL CONTROL INTERNO BASADO EN SAS 99

- ¿Qué es CCI-99?
- Plan de Trabajo
- **Controles efectuados**
  - Controles de Frecuencia
  - Controles de Patrones Numéricos
  - Controles de Materialidad
  - Controles de Horario
  - Controles de Descripción
- Estimación de Recursos

# Controles efectuados en CCI - 99. Descripción de las categorías

## Controles de Frecuencia

- Destinados a analizar frecuencias de transacciones realizadas por cada uno de los usuarios e identificar anomalías al respecto.

## Controles de Patrones Numéricos

- Destinados a analizar las cuantías de las transacciones, identificando cifras o tendencias poco frecuentes en una operativa normal de la organización.

## Controles de Materialidad

- Destinados a analizar las cantidades acumuladas manejadas en las transacciones, tanto para transacciones concretas como para acumulados por cuentas contables o usuarios.

## Controles de Horario

- Destinados a analizar la fecha y hora de ejecución de las transacciones, identificando aquellas efectuadas en momentos inusuales respecto a la operativa del negocio.

## Controles de Descripción

- Destinados a analizar las descripciones introducidas para las transacciones, identificando transacciones con descripciones inusuales.

# Controles de Frecuencia. ¿Qué controles para qué riesgos?

| Naturaleza de la operación contable | Control de CCI – 99 | Riesgos asociados |
|---|---|---|
| ▪Cuentas contables poco utilizadas | ▪Identificar el número de entradas por cuenta contable | ▪Cuentas contables con un volumen anormal de transacciones según su naturaleza |
| ▪Usuarios con un número bajo de entradas | ▪Identificar cuentas de usuario con poca actividad (que hayan registrado pocas entradas) | ▪Cuentas de usuario creadas con fines fraudulentos<br>▪Incidencias administrativas<br>▪Debilidades en el Control Interno |
| ▪Usuarios con un alto número de anulaciones o entradas correctoras | ▪Identificar usuarios que realizan demasiadas correcciones para el desempeño habitual de su actividad.<br>▪Identificar comportamientos extraños. | ▪Posibles acciones fraudulentas<br>▪Error de los usuarios en la operativa |

# Controles de Patrones Numéricos. ¿Qué controles para qué riesgos?

| Naturaleza de la operación contable | Control de CCI – 99 | Riesgos asociados |
|---|---|---|
| ▪Existencia de cifras redondas (millares) | ▪Identificar entradas cuyas cantidades sean cifras redondas. | ▪Transacciones que no corresponden a un concepto de la operativa diaria<br>▪Fraude o error |
| ▪Análisis de Benford | ▪Aplicación de la ley de Benford sobre los primeros dígitos del campo importe para identificar patrones sospechosos.<br>▪El criterio establecido es el de analizar los dos primeros dígitos. | ▪Operaciones con importes recurrentes. Pueden estar motivadas por conductas fraudulentas |
| ▪Transacciones, con importes repetidos, por Cuenta Contable | ▪Identificación de entradas con la misma cantidad en la misma cuenta contable. | ▪Identificación de posibles pagos duplicados<br>▪Importes recurrentes por motivos de fraude |
| ▪Transacciones, con importes repetidos, por Usuario | ▪Identificación de entradas con la misma cantidad para el mismo usuario | ▪Identificación de posibles pagos duplicados<br>▪Importes recurrentes por motivos de fraude |

# Controles de Materialidad. ¿Qué controles para qué riesgos?

| Naturaleza de la operación contable | Control de CCI – 99 | Riesgos asociados |
|---|---|---|
| ▪Volumen de transacciones por importe y usuario | ▪Identificar entradas cuyas cantidades sean cifras que, en valor absoluto, superen cierto umbral.<br>▪Considerar los umbrales aplicables a cada tipo de cuenta. | ▪Identificación de operaciones no permitidas<br>▪Fraude o error |
| ▪Ocurrencia de cada importe | ▪Detectar acumulaciones de transacciones en ciertos rangos de importe | ▪Evitar proceso autorización/apoderamiento<br>▪Patrones de fraude |
| ▪Entradas mayores para cada cuenta | ▪Existencia de cantidades superiores a cierto umbral | ▪Evitar operaciones no autorizadas |

# Controles de Horario. ¿Qué controles para qué riesgos?

| Naturaleza de la operación contable | Control de CCI – 99 | Riesgos asociados |
|---|---|---|
| ▪Usuarios con transacciones realizadas en fines de semana | ▪Identificación de entradas efectuadas en fines de semana | ▪Identificación de transacciones no autorizadas<br>▪Fraude |
| ▪Transacciones fuera del periodo de cierre | ▪Identificar transacciones de devengo de cuentas que se hayan ejecutado en días fuera del periodo de cierre. | ▪Presentación fraudulenta de la información financiera |

# Controles de Descripción. ¿Qué controles para qué riesgos?

| Naturaleza de la operación contable | Control de CCI – 99 | Riesgos asociados |
|---|---|---|
| ▪Campos de descripción en blanco | ▪Identificar entradas cuyo concepto no ha sido definido | ▪Identificación de entradas fraudulentas o erróneas. |
| ▪Descripciones inusuales | ▪Identificación de entradas cuyo concepto tiene contenido inusual.<br>▪El criterio de identificación se realizará en base a determinadas palabras clave. | ▪Identificación de entradas fraudulentas o erróneas. |

# CCI-99: CUMPLIMIENTO DEL CONTROL INTERNO BASADO EN SAS 99

- ¿Qué es CCI-99?
- Plan de Trabajo
- Controles efectuados
  - Controles de Frecuencia
  - Controles de Patrones Numéricos
  - Controles de Materialidad
  - Controles de Horario
  - Controles de Descripción
- **Estimación de Recursos**

# Estimación Recursos

## Dependiente de varios factores:

- Accesibilidad y formato de los datos
- Disponibilidad del personal de la entidad
- Definición de controles “Ad-hoc”

| Fase Plan de Trabajo | Responsable | Estimación Jornadas |
|---|---|---|
| Extracción de datos | Entidad | 1 |
| Adecuación de formato | Mazars | 1-2 |
| Análisis de datos | Mazars & Entidad | 1-2 |
| Investigaciones complementarias | Entidad & Mazars | (0-2) |
| Conclusiones y resultados | Mazars | 1 |
| **TOTAL** | | **1 semana aprox.** |

**Promoción por 2.000€ para los asistentes a los Desayunos de Mazars**



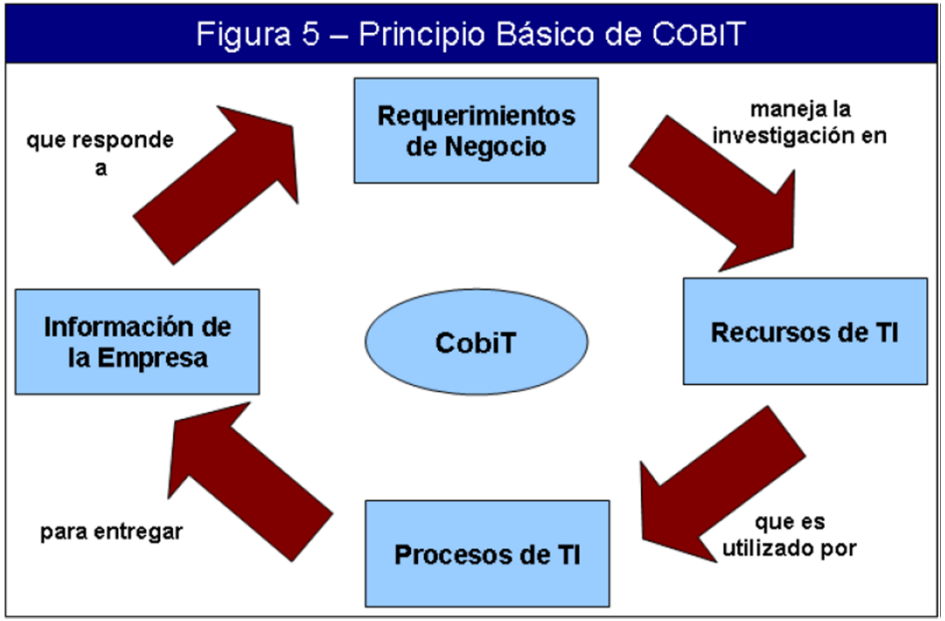
MAZARS


# MARCO DE REFERENCIA COBIT

MAZARS

# Objetivos de Control para la Información y la Tecnología relacionada

| | |
|---|---|
| **C** | **Control** |
| **OB** | **OBjectives** |
| **I** | **for Information** |
| **T** | **and Related Technology** |




**Misión de CobiT:** Investigar, desarrollar, publicar y promover un conjunto de objetivos de control para Tecnología de Información, que sea Internacional y esté actualizado para uso cotidiano de Gerentes, Auditores y Usuarios.

**Regla de Oro en CobiT:** Para proveer la Información que requiere la Organización para lograr sus objetivos, los recursos de TI deben ser administrados por un conjunto de procesos, agrupados de forma adecuada y ejecutados acorde a prácticas normalmente aceptadas.

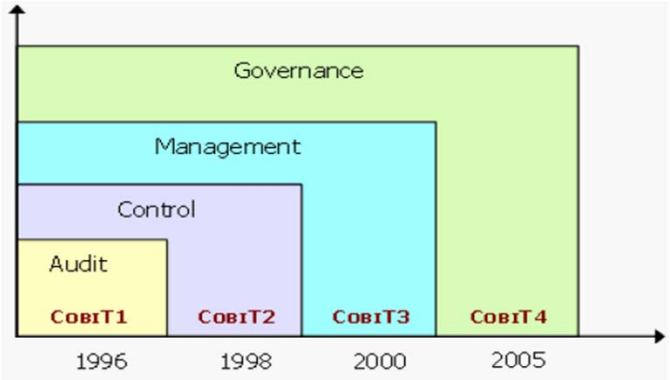
**Enfocado en el Negocio, orientado a Proceso, basado en Controles y dirigido por Medidas**

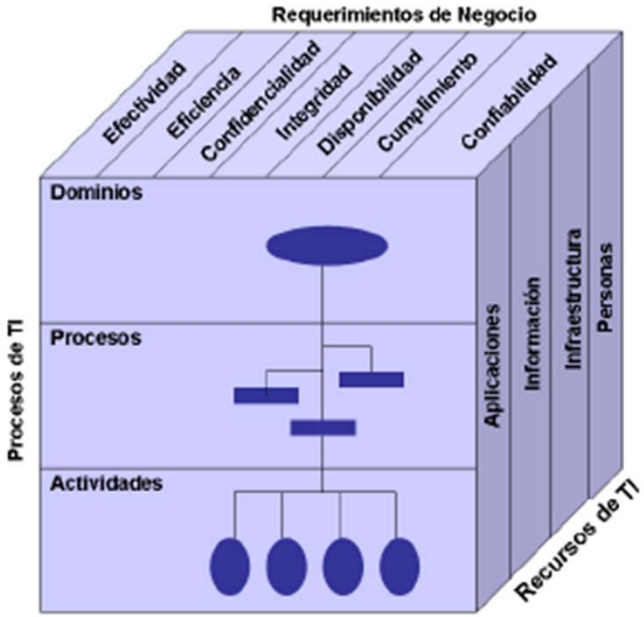
## Objetivos y Beneficios

- ✓ Proveer un marco único reconocido a nivel mundial de las "**mejores prácticas**" de control y seguridad de TI
- ✓ **Consolidar y armonizar estándares** originados en diferentes países desarrollados.
- ✓ Concienciar a la comunidad sobre la **importancia del control y la auditoría de TI**.
- ✓ Enlaza los **objetivos y estrategias de los negocios** con la estructura de control de la TI, como factor crítico de éxito.
- ✓ Aplica a todo tipo de organizaciones **independiente de sus plataformas TI**.
- ✓ Ratifica la importancia de **la información, como uno de los recursos más valiosos** de toda organización exitosa.

## Representatividad

- ISACA – 95 países 20.000 miembros
- Investigación: E.U. – Europa – Australia – Japón
- Consolidación y armonización de 18 estándares.






MAZARS

# Objetivos de Control para la Información y la Tecnología relacionada

**La Gerencia**

- Apoyo a decisiones de inversión en TI y control sobre su desempeño, balanceo del riesgo y el control de la inversión en un ambiente a menudo impredecible

**Los Usuarios**

- Obtienen una garantía sobre el control y seguridad de los productos que adquieren interna y externamente.

**Los Auditores**

- Soportar sus opiniones sobre los controles de los proyectos de TI, su impacto en la organización y determinar el control mínimo requerido

**Responsables de TI**

- Para identificar los controles que requieren sus Áreas.

**Organismos estatales de Control**

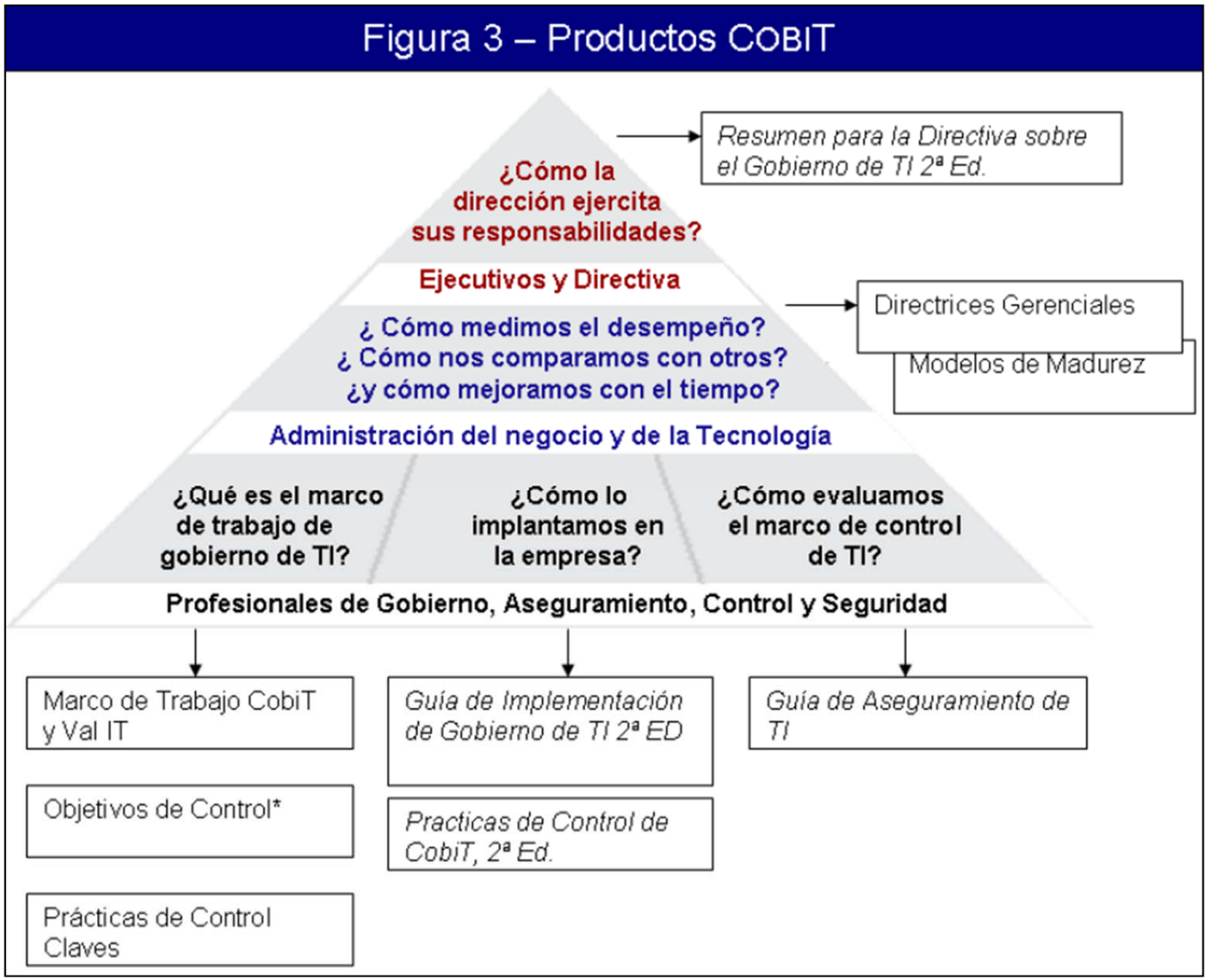
- Para saber que es lo mínimo que pueden exigir

# Requerimientos de la Información del Negocio

**CobiT combina los principios contenidos por modelos existentes y conocidos, como COSO, SAC y SAS**

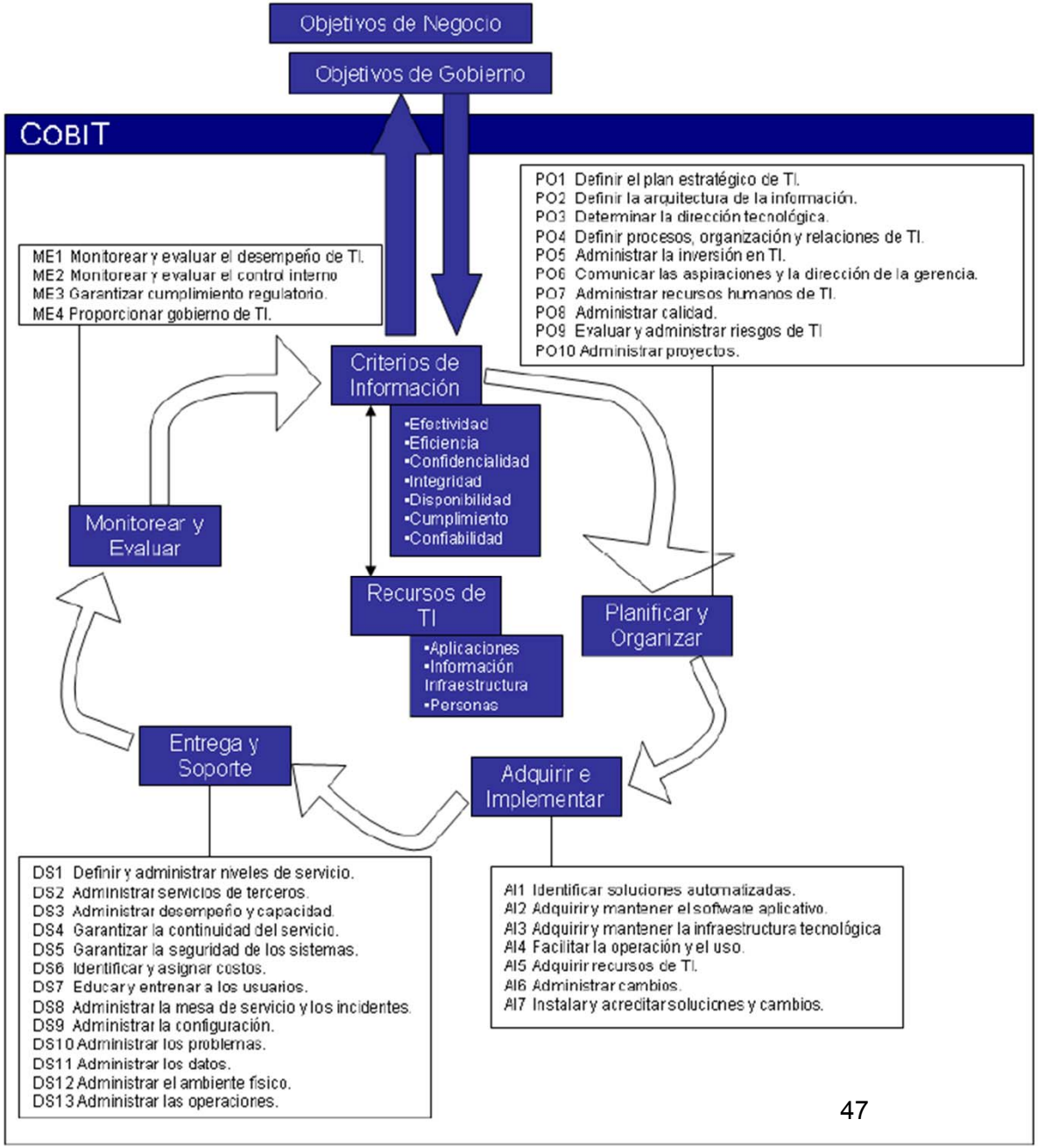
| | |
|---|---|
| **Requerimientos de Calidad** | ✓ Calidad (cumplimiento de requerimientos)<br>✓ Costo (dentro del presupuesto)<br>✓ Oportunidad (en el tiempo indicado) |
| **Requerimientos Financieros (COSO)** | ✓ Efectividad y eficiencia operacional<br>✓ Confiabilidad de los reportes financieros<br>✓ Cumplimiento de leyes y regulaciones |
| **Requerimientos de Seguridad** | ✓ Confidencialidad<br>✓ Integridad<br>✓ Disponibilidad |

## Productos de CobiT



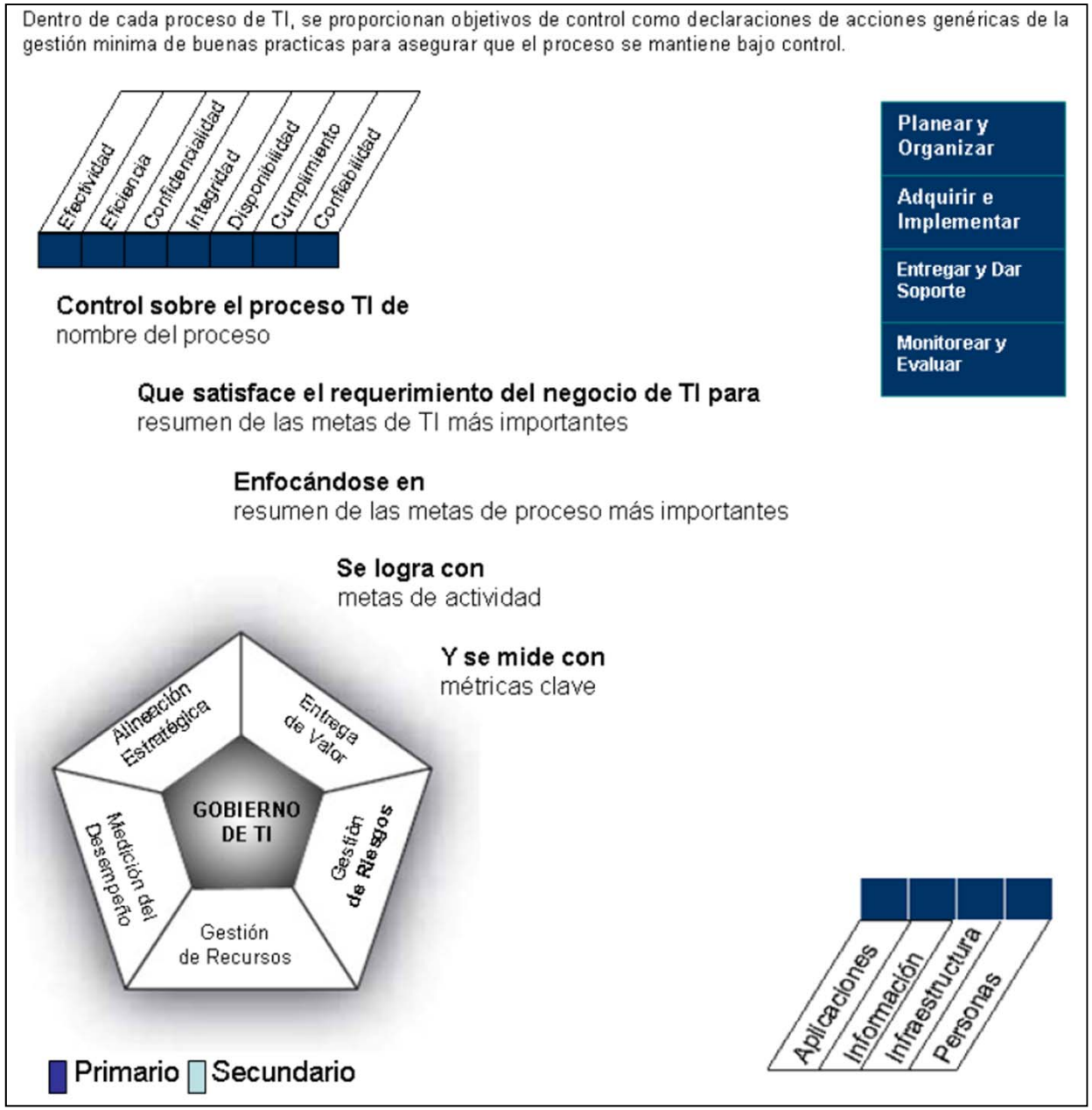

También hay productos derivados para propósitos específicos (***Objetivos de Control de TI para SOX***), para dominios tales como seguridad (***Línea Base Seguridad de CobiT y Gobierno de Seguridad de la Información: Guía para la Directiva de Directores y Gerentes Ejecutivos***) o para empresas específicas (***CobiT QuickStart para pequeñas y medianas empresas*** o grandes empresas que deseen introducirse de forma rápida en la implementación de gobierno de TI.

# Introducción a CobiT




## Marco de trabajo

# Introducción a CobiT




## Navegación

# Relación entre CobiT y COSO

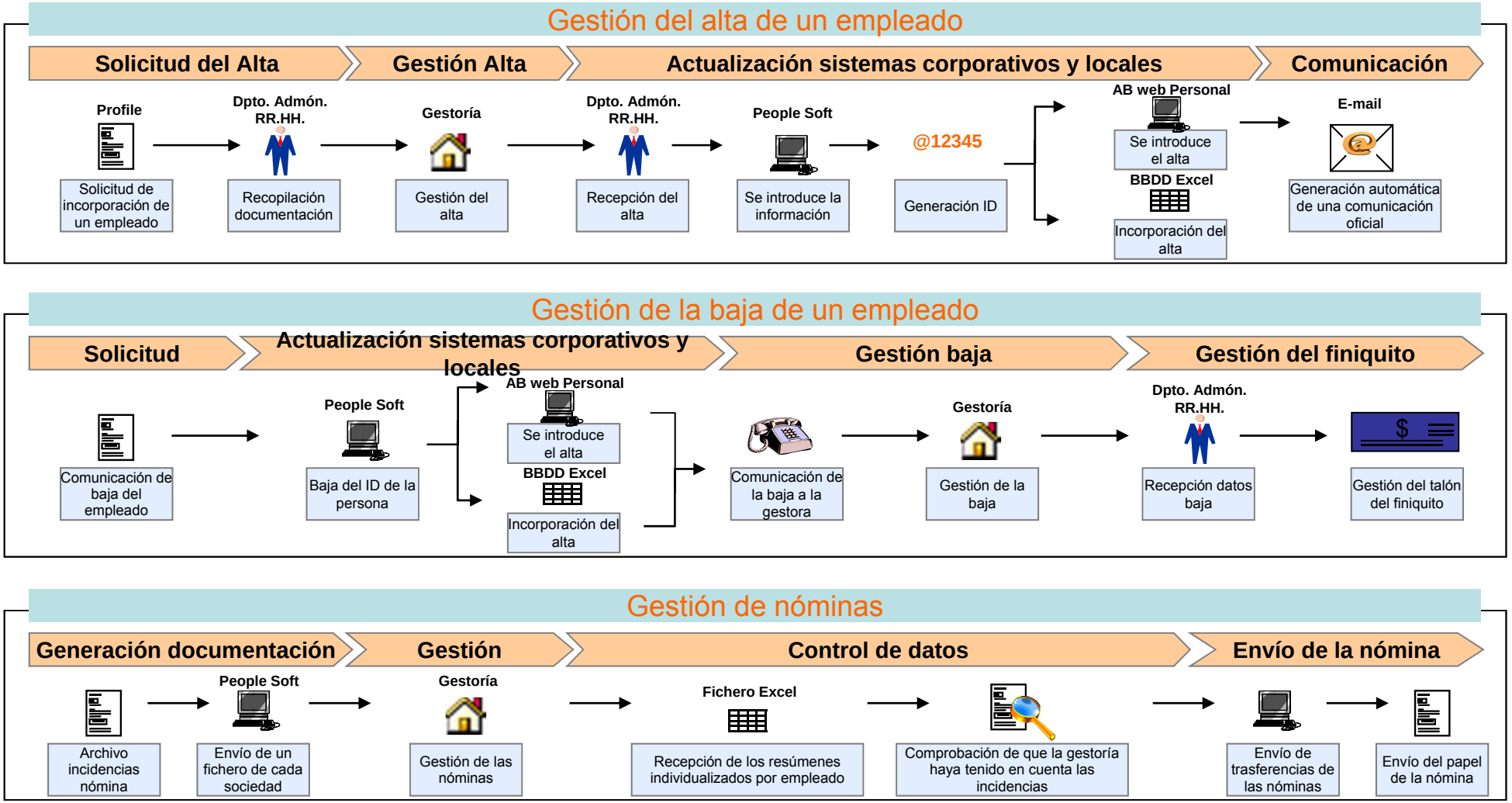
| | | Áreas de enfoque de Gobierno TI | | | | | COSO | | | | | Recursos TI de CobiT | | | | Criterios de Información de CobiT | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IMPORTANCIA | Alineación estratégica | Entrega de valor | Administración de | Administración de | Medición del desempeño | Entorno de Control | Evaluación de riesgos | Actividades de control | Información y | Monitoreo | Aplicación | Información | Infraestruetura | Personas | Efectividad | Eficiencia | Confidencialidad | Integridad | Disponibilidad | Cumplimiento | Confiabilidad |
| **Planear y Organizar** | | | | | | | | | | | | | | | | | | | | | | |
| PO1 Definir un plan estratégico de TI | A | P | | S | S | | | P | | S | S | | | | | P | S | | | | | |
| PO2 Definir la arquitectura de la información | B | P | S | P | S | | | | P | P | | | | | | S | P | S | P | | | |
| PO3 Determinar la dirección tecnológica | M | S | S | P | S | | | S | P | S | | | | | | P | P | | | | | |
| PO4 Definir los procesos, organización y relaciones de TI | B | S | | P | P | | P | | | S | S | | | | | P | P | | | | | S |
| PO5 Administrar la inversión en TI | M | S | P | S | | S | | S | P | | | | | | | P | P | | | | | |
| PO6 Comunicar las aspiraciones y la dirección de la gerencia | M | P | | | P | | P | | | P | | | | | | P | | | | | S | |
| PO7 Administrar recursos humanos de TI | B | P | | P | S | S | P | | | S | | | | | | P | P | | | | | |
| PO8 Administrar la calidad | M | P | S | | S | | P | | P | S | P | | | | | P | P | | S | | | S |
| PO9 Evaluar y administrar los riesgos de TI | A | P | | | P | | | P | | | | | | | | S | S | P | P | P | S | S |
| PO10 Administrar proyectos | A | P | S | S | S | S | S | S | P | | S | | | | | P | P | | | | | |
| **Adquirir e Implementar** | | | | | | | | | | | | | | | | | | | | | | |
| AI1 Identificar soluciones automatizadas | M | P | P | S | S | | | | P | | | | | | | P | S | | | | | |
| AI2 Adquirir y mantener software aplicativo | M | P | P | | S | | | | P | | | | | | | P | P | | S | | | S |
| AI3 Adquirir y mantener infraestructura tecnológica | B | | | P | | | | | P | | | | | | | S | P | | S | S | | |
| AI4 Facilitar la operación y el uso | B | S | P | S | S | | | | P | S | | | | | | P | P | | S | S | S | S |
| AI5 Adquirir recursos de TI | M | | S | P | | | | | P | | | | | | | S | P | | | | S | |
| AI6 Administrar cambios | A | | P | S | | | | S | P | | S | | | | | P | P | | P | P | | S |
| AI7 Instalar y acreditar soluciones y cambios | M | S | P | S | S | S | | | P | S | S | | | | | P | S | | S | S | | |
| **Entregar y Dar Soporte** | | | | | | | | | | | | | | | | | | | | | | |
| DS1 Definir y administrar los niveles de servicio | M | P | P | P | | P | S | | P | S | S | | | | | P | P | S | S | S | S | S |
| DS2 Administrar los servicios de terceros | B | | P | S | P | S | P | S | P | | S | | | | | P | P | S | S | S | S | S |
| DS3 Administrar el desempeño y la capacidad | B | S | S | P | S | S | | | P | | S | | | | | P | P | | | S | | |
| DS4 Garantizar la continuidad del servicio | M | S | P | S | P | S | S | | P | S | | | | | | P | S | | | P | | |
| DS5 Garantizar la seguridad de los sistemas | A | | | | P | | | | P | S | S | | | | | | | P | P | S | S | S |
| DS6 Identificar y asignar costos | B | | S | P | | S | | | P | | | | | | | | P | | | | | P |
| DS7 Educar y entrenar a los usuarios | B | S | P | S | S | | P | | | S | | | | | | P | S | | | | | |
| DS8 Administrar la mesa de servicio y los incidentes | B | | P | | | S | S | | | P | P | | | | | P | P | | | | | |
| DS9 Administrar la configuración | M | | P | P | S | | | | P | | | | | | | P | S | | | S | | S |
| DS10 Administrar los problemas | M | | P | | S | S | | | P | S | S | | | | | P | P | | | S | | |
| DS11 Administrar los datos | A | | P | P | P | | | | P | | | | | | | | | | P | | | P |
| DS12 Administrar el ambiente físico | B | | | S | `P | | | S | P | | | | | | | | | | P | P | | |
| DS13 Administrar las operaciones | B | | | P | | | | | P | S | | | | | | P | P | | S | S | | |
| **Monitorear y Evaluar** | | | | | | | | | | | | | | | | | | | | | | |
| ME1 Monitorear y evaluar el desempeño de TI | A | S | S | S | S | P | | | | S | P | | | | | P | P | S | S | S | S | S |
| ME2 Monitorear y evaluar el control interno | M | | P | | P | | | | | | P | | | | | P | P | S | S | S | S | S |
| ME3 Garantizar el cumplimiento regulatorio | A | P | | | P | | | | P | S | S | | | | | | | | | | P | S |
| ME4 Proporcionar gobierno de TI | A | P | P | P | P | P | P | S | | S | P | | | | | P | P | S | S | S | S | S |

# La Auditoría Interna en los Sistemas de Información

## DEFINICIÓN DE UN PROCESO

MAZARS

# Ejemplo gráfico de descripción de un proceso



## Ejemplo de descripción de un proceso

| Fase del Proceso | Descripción |
|---|---|
| Cierre de:<br>-Proveedores (ACP)<br>-Clientes (ACR)<br>-Tesorería (CMG)<br>-Contabilidad (GLD) | BAAN - Pantalla de "Mantener estatus períodos"<br>Permite controlar el cierre de ACP (Proveedores), ACR (Clientes), CMG (Tesorería), Contabilidad (GLD) en BAAN.<br>Cuando el usuario cambia en la pantalla el estado de un período debe realizar las comprobaciones pertinentes para garantizar que no se provocarán inconsistencias en los Sistemas Internos derivados de la nueva situación. |
| | BAAN – Pantalla de "Confirmación Global"<br>Permite realizar comprobaciones internas de integridad dentro de los datos de BAAN, antes de la finalización de los asientos (pase de estado del asiento de "Provisional" a "Definitivo"). |
| | BAAN – Pantalla "Procesar transacciones"<br>Permite finalizar los asientos (pasar de estado "Provisional" a "Definitivo").<br>El proceso puede invocarse manualmente, y eligiendo las diferentes opciones que aparecen en pantalla, o bien invocarse para todos los costes por la noche (se realiza periódicamente). |
| Interface BAAN → GEP (Traspaso) | GEP – Pantalla de "Traspaso Costes / Ingresos de BaaN a GEP"<br>Permite sincronizar la información respecto a costes e ingresos existentes en las dos aplicaciones BAAN y GEP.<br>Para ello lee los registros de la tabla correspondiente de costes o ingresos de BAAN y crea los registros correspondientes en GEP, asignando de esta forma los costes e ingresos a los diferentes proyectos.<br>Entorno tecnológico: Oracle 9i + Developer. No utiliza tablas intermedias para el traspaso.<br>Nota: En GEP existe la posibilidad de generar listados y exportarlos en Excel. En este sentido Control de Gestión hace bastantes verificaciones manuales. |
| Contabilización de asientos de integración | BAAN – Contabilizar asientos integración a asientos contables<br>Permite traspasar todos los costes de facturación a contabilidad, indicando la operación financiera.<br>Este proceso se lanza manualmente a final de mes. |
| Contabilización de amortizaciones | BAAN (Finanzas) → Procesar cálculo periódico amortización<br>Proceso de amortización mensual que se lanza manualmente a final de mes, aunque se puede pasar tantas veces como se quiera.<br>Traspasa información de amortizaciones de inmovilizado a BAAN Contabilidad y Proyectos.<br>Por la noche se lleva a GEP (por el proceso ya descrito).<br>Nota: 180.000 registros. El proceso dura 2 o 3 horas. Lo lanzan cuando se van. Se puede quedar cortado y re-iniciar. Lo comprueban el día siguiente. Nos indican que el proceso ha sido optimizado. |

# Ejemplo de descripción de un proceso

| Fase del Proceso | Descripción |
|---|---|
| Contabilización Gastos de Empleado | GAE – Proceso de Contabilización de Gastos de Empleados<br>La introducción de los gastos del empleado se puede realizar por dos vías diferentes, desde el entorno Cliente/Servidor (Developer) y desde Web (Java).<br>Este proceso se encarga de contabilizar dichos gastos de empleado. Se ejecuta dos veces al mes (anticipos y liquidación).<br>Por otra parte se genera el lote de pagos de transferencias a los Bancos.<br>El proceso, una vez que se encuentra el gasto como Visado CSA:<br>1) Genera el asiento en buzón para importar en BAAN - Proyectos<br>2) Se traspasa de BAAN a GEP (proceso descrito anteriormente)<br>Nota: El gasto hasta que no se contabiliza, no entra en proyecto. |
| Retenciones Nómina | GAE → META-4<br>GAE – Proceso de Generación de Retención de Nóminas<br>El proceso crea una tabla de retenciones que posteriormente se importa manualmente en META-4.<br>El traspaso se realiza a través de un fichero de texto. |
| Carga de Nómina | GEP – Carga de Nómina<br>Para las empresas que se gestionan en Meta-4 este paso no se efectúa porque la nómina la carga directamente el Departamento de RRHH. Las empresas que no van en Meta-4 sí se deberán cargar en GEP.<br>Para ello se prepara un fichero en Excel, con los datos de fecha, empleado, concepto e importe. |
| Cuadre de cuentas GAE con Contabilidad | GAE ←→ BAAN (manual)<br>GAE – Informe de saldo de Gastos de Viaje por Empleado<br>Opción que utiliza el usuario para comparar manualmente los informes de saldos a una fecha en BAAN y en GAE para detectar incidencias y descuadres. |
| Cierre Dedicaciones | GEP – Dedicaciones – Calendario de Cierre<br>Permite configurar el período, la fecha de cierre provisional y definitivo, el último día de captura y el último día de visado. |
| | GEP – Dedicaciones – Cierre Mensual<br>Se revisan todas las incidencias de las dedicaciones a partir de unos listados. |

# Ejemplo de descripción de un proceso

| Fase del Proceso | Descripción |
|---|---|
| **Contabilización de Nómina** | **GEP – Generación de Movimientos Contables a Nómina.**<br>**En este proceso se prepara el asiento contable. El informe de "Movimientos Nómina por Asiento", saca el asiento contable que va a generar la nómina. Se comprueba manualmente que los datos cuadran con los datos que tenemos de la nómina.** |
| | **GEP – Generación de Costes de Personal a Proyectos**<br>**El proceso permite traspasar los costes de las dedicaciones a los proyectos.**<br>**Se procesan las dedicaciones mensuales, generando un registro x tasa x proyecto x horas (Generación de costes de personas a proyectos). Las tasas se aplican a proyectos normales y el coste real a los proyectos de núcleo (desviaciones).**<br>**Tras este proceso se realizan unas comprobaciones manuales.** |
| | GEP → Traspaso a BAAN<br>**Se procede con los pasos siguientes:**<br>-Traspaso Movimiento contable BAAN (GLD)<br>-Traspaso Costes de Personal GEP-BAAN<br>-Incorporación de Trabajos Extraordinarios.<br>Con esto se pretende sincronizar los datos con los siguientes módulos de BAAN:<br>-BAAN – Asientos Contables (GLD)<br>-BAAN- Finanzas – Nómina<br>-BAAN – Proyectos<br>Nota: Al no estar contemplados dentro de la tasa, los trabajos extraordinarios y gratificaciones los graba RRHH en GEP. Si la incorporación da error, hay que avisar a RRHH para que introduzcan la diferencia. |
| | **BAAN – Contabilización de la nómina**<br>**Una vez finalizados todos los procesos en GEP, hay que finalizar el asiento en Baan, pero como el asiento no se introdujo directamente en BAAN, sino en otra aplicación, primero hay que recuperar ese asiento. Lo hacemos con la siguiente opción de "Integración módulos externos – Importar asientos modelos externos":**<br>**-Importar lote asiento diario por número ID.**<br>**-Iniciar proceso en segundo plano.**<br>**-Consultar diarios importados** |

## Ejemplo de descripción de un proceso

| Fase del Proceso | Descripción |
|---|---|
| Cierre de la emisión de propuestas de facturas | GEP – Períodos de Control en la Emisión de Propuestas de Facturación<br>Permite definir los períodos activos para la emisión de facturas.<br>El usuario del Área de Centro de Servicios – Responsable de Facturación se encarga de cerrar, abrir y re-abrir los períodos. |
| Cobros | BAAN – Convertir extractos telebanco<br>Permite procesar los extractos para los cobros bancarios |
| | BAAN – Seleccionar lotes por finalización<br>Permite finalizar lotes de facturación |
| Facturas Finanzas | BAAN – Generar datos de facturación por proyecto, segmento, mercado, solución o producto. |
| Avance Venta | GEP – Generación de venta<br>Este proceso se ejecuta después de que los jefes de proyecto hayan introducido el avance de la venta. |
| | GEP- Generación de Deuda, DPF y ALO por proyecto |
| Establecimientos Permanentes | GEP – Establecimientos Permanentes – Procesos Interfaces<br>Realiza la integración de información correspondiente a establecimientos permanentes de XXXXX, en otros países, que utilizan los Sistemas Internos para gestionar las dedicaciones, contrataciones, gastos, avales, etc.<br>Dentro de GEP se disponen las siguientes opciones:<br>-Interfase de Datos Generales de Proyectos de la Compañía Matriz hacia la compañía.<br>-Interfase de Costes de la Compañía Matriz hacia la compañía E.P.<br>-Carga Inicial de Matriz hacia EP por Proyecto |


# La Auditoría Interna en los Sistemas de Información

## CONTROLES GENERALES DE TI Y CONTROLES DE APLICACIÓN

MAZARS

## Los Controles de Aplicación

Los controles de aplicación consisten en **actividades manuales y/o automatizadas que aseguran que la información cumple con ciertos criterios**, como son los requerimientos de negocio**. Estos criterios son:**

- Efectividad
- Eficiencia
- Confidencialidad
- Integridad
- Disponibilidad
- Cumplimiento
- Confiabilidad

Es necesario asegurarse que existen **suficientes controles** para mitigar los riesgos y que están operando con la **efectividad necesaria** para proveer información confiable.

## Los Controles de Aplicación

Los controles de aplicación se establecen para proporcionar una seguridad razonable de que los **objetivos que la gerencia establece sobre las aplicaciones, se alcanzan.** Estos objetivos se articulan típicamente a través de funciones específicas para la solución, la definición de las reglas de negocio para el procesamiento de la Información y la definición de procedimientos manuales de soporte.

**Ejemplo de ello son:**

- Totalidad (Integridad)
- Exactitud
- Validez
- Autorización
- Segregación de funciones

Durante el ciclo de vida de los sistemas, diversas partes de la organización realizan actividades, responsabilidades y roles asociados con los controles de aplicación.

## Controles Generales TI

**Dependencia de los Controles Generales de TI**

Los controles generales de TI son aquellos que tienen que ver con el ambiente de proceso de TI en el cual operan los controles de aplicación.

Entre los controles generales están por ejemplo:

- Control de cambios a programas
- Controles de acceso físico
- Controles de acceso lógico
- Controles de continuidad operativa

El hecho de que los controles generales sean adecuados, no garantiza que los controles de aplicación serán adecuados.

Pero **si los controles generales son deficientes, los controles de aplicación muy probablemente lo serán también**.

## Objetivos de Control de Aplicación en Cobit 4.0

| | |
|---|---|
| **AC1 - Preparación y Autorización de Información Fuente** | Asegurar que los documentos fuente están preparados por personal autorizado y calificado siguiendo los procedimientos establecidos, teniendo en cuenta la adecuada segregación de funciones respecto al origen y aprobación de estos documentos. Detectar errores e irregularidades para que sean informados y corregidos |
| **AC2 – Recolección y Entrada de Información Fuente** | Establecer que la entrada de datos se realice en forma oportuna por personal calificado y autorizado. Las correcciones y reenvíos de los datos que fueron erróneamente ingresados se deben realizar, sin comprometer los niveles de autorización de las transacciones originales. En donde sea apropiado para la reconstrucción, retener los documentos fuentes originales durante el tiempo necesario. |
| **AC3 – Chequeos de Exactitud, Integridad y Autenticidad** | Asegurar que las transacciones son exactas, completas y válidas. Validar los datos ingresados, y editar o devolver para corregir, tan cerca del punto de origen como sea posible. |

## Objetivos de Control de Aplicación en Cobit 4.0

| | |
|---|---|
| **AC4 – Integridad y Validez del Procesamiento** | Mantener la integridad y validación de los datos a través del ciclo de procesamiento. Detectar transacciones erróneas y que no interrumpan el procesamiento de transacciones válidas. |
| **AC5 – Revisión de Salidas, Reconciliación y Manejo de Errores** | Establecer procedimientos y responsabilidades asociadas para asegurar que la salida se maneja de una forma autorizada, entregada al destinatario apropiado, y protegida durante la transmisión; que se verifica, detecta y corrige la exactitud de la salida; y que se usa la información proporcionada en la salida. |
| **AC6 – Autenticación e Integridad de Transacciones** | Antes de pasar datos de la transacción entre aplicaciones internas y funciones de negocio / operativas (dentro o fuera de la empresa), verificar el apropiado direccionamiento, autenticidad del origen e integridad del contenido. Mantener la autenticidad y la integridad durante la transmisión o el transporte. |

## Objetivos de Control de Aplicación en Cobit 4.1

| Controles de origen de datos/ autorización | | |
|---|---|---|
| **AC1** | **Procedimientos de preparación de datos** | Los departamentos usuarios implementan y dan seguimiento a los procedimientos de preparación de datos. En este contexto, el diseño de los formatos de entrada asegura que los errores y las omisiones se minimicen. Los procedimientos de manejo de errores durante la generación de los datos aseguran de forma razonable que los errores y las irregularidades son detectadas, reportadas y corregidas. |
| **AC2** | **Procedimientos de autorización de documentos fuente** | El personal autorizado, actuando dentro de su autoridad, prepara los documentos fuente de forma adecuada y existe una segregación de funciones apropiada con respecto a la generación y aprobación de los documentos fuente. |
| **AC3** | **Recolección de datos de documentos fuente** | Los procedimientos garantizan que todos los documentos fuente autorizados son completos y precisos, debidamente justificados y transmitidos de manera oportuna para su captura. |
| **AC4** | **Manejo de errores en documentos fuente** | Los procedimientos de manejo de errores durante la generación de los datos aseguran de forma razonable la detección, el reporte y la corrección de errores e irregularidades. |
| **AC5** | **Retención de documentos fuente** | Existen procedimientos para garantizar que los documentos fuente originales son retenidos o pueden ser reproducidos por la organización durante un lapso adecuado de tiempo para facilitar el acceso o reconstrucción de datos así como para satisfacer los requerimientos legales. |

# Objetivos de Control de Aplicación en Cobit 4.1

| Controles de entrada de datos | | |
|---|---|---|
| **AC6** | **Procedimientos de autorización de captura de datos** | Los procedimientos aseguran que solo el personal autorizado capture los datos de entrada. |
| **AC7** | **Verificaciones de precisión, integridad y autorización** | Los datos de transacciones, ingresados para ser procesados (generados por personas, por sistemas o entradas de interfases) están sujetos a una variedad de controles para verificar su precisión, integridad y validez. Los procedimientos también garantizan que los datos de entrada son validados y editados tan cerca del punto de origen como sea posible. |
| **AC8** | **Manejo de errores en la entrada de datos** | Existen y se siguen procedimientos para la corrección y re-captura de datos que fueron ingresados de manera incorrecta. |

# Objetivos de Control de Aplicación en Cobit 4.1

| Controles en el Procesamiento de datos | | |
|---|---|---|
| **AC9** | **Integridad en el procesamiento de datos** | Los procedimientos para el procesamiento de datos aseguran que la separación de funciones se mantiene y que el trabajo realizado de forma rutinaria se verifica. Los procedimientos garantizan que existen controles de actualización adecuados, tales como totales de control de corrida-a-corrida, y controles de actualización de archivos maestros. |
| **AC10** | **Validación y edición del procesamiento de datos** | Los procedimientos garantizan que la validación, la autenticación y la edición del procesamiento de datos se realizan tan cerca como sea posible del punto de generación. Los individuos aprueban decisiones vitales que se basan en sistemas de inteligencia artificial. |
| **AC11** | **Manejo de errores en el procesamiento de datos** | Los procedimientos de manejo de errores en el procesamiento de datos permiten que las transacciones erróneas sean identificadas sin ser procesadas y sin una indebida interrupción del procesamiento de otras transacciones válidas. |

# Objetivos de Control de Aplicación en Cobit 4.1

| Controles de salida de datos | | |
|---|---|---|
| **AC12** | **Manejo y retención de salidas** | El manejo y la retención de salidas provenientes de aplicaciones de TI siguen procedimientos definidos y tienen en cuenta los requerimientos de privacidad y de seguridad. |
| **AC13** | **Distribución de salidas** | Los procedimientos para la distribución de las salidas de TI se definen, se comunican y se les da seguimiento. |
| **AC14** | **Cuadre y conciliación de salidas** | Las salidas cuadran rutinariamente con los totales de control relevantes. Las pistas de auditoría facilitan el rastreo del procesamiento de las transacciones y la conciliación de datos alterados. |
| **AC15** | **Revisión de salidas y manejo de errores** | Los procedimientos garantizan que tanto el proveedor como los usuarios relevantes revisan la precisión de los reportes de salida. También existen procedimientos para la identificación y el manejo de errores contenidos en las salidas. |
| **AC16** | **Provisión de seguridad para reportes de salida** | Existen procedimientos para garantizar que se mantiene la seguridad de los reportes de salida, tanto para aquellos que esperan ser distribuidos como para aquellos que ya están entregados a los usuarios. |

# Objetivos de Control de Aplicación en Cobit 4.1

| **Controles de límites** | | |
|---|---|---|
| **AC17** | **Autenticidad e integridad** | Se verifica de forma apropiada la autenticidad e integridad de la información generada fuera de la organización, ya sea que haya sido recibida por teléfono, por correo de voz, como documento en papel, fax o correo electrónico, antes de que se tomen medidas potencialmente críticas. |
| **AC18** | **Protección de información sensitiva durante su transmisión y transporte** | Se proporciona una protección adecuada contra accesos no autorizados, modificaciones y envíos incorrectos de información sensitiva durante la transmisión y el transporte. |

# La Auditoría Interna en los Sistemas de Información

## GUÍAS DE AUDITORÍA DE LOS CONTROLES DE APLICACIÓN

MAZARS

# AC1 - Preparación y Autorización de Información Fuente

## *CONDUCTORES*

**Conductores de Valor:**

- Integridad de la información
- Documentación de transacciones normalizada y autorizada
- Rendimiento de aplicación mejorada
- Accuracy of transaction data

**Conductores de Riesgo:**

- Integridad comprometida de información crítica
- Transacciones desautorizadas y/o erróneas
- Ineficiencias de procesamiento y re-trabajo

## *EVALUACIÓN DEL DISEÑO DEL CONTROL*

- Asegurar que el diseño del sistema cubre la información y gestión de los niveles de autorización.
- Investigar y confirmar que el diseño del sistema cubre el uso de listas de autorización pre-aprobadas y firmas para el uso relacionadas, determinando que los documentos han sido adecuadamente autorizados.
- Evaluar si los documentos fuente y/o pantallas de entrada están diseñados con códigos predeterminados, opciones, etc., para promover que se completen a tiempo y minimizar la posibilidad de error.
- Investigar y confirmar que el diseño del sistema promueve la revisión de los formularios para completar y autorizar, e identifica las situaciones en las existen intentos de procesar documentos incompletos y/o desautorizados.
- Investigar y confirmar que, tras identificar documentos incompletos y/o desautorizados, éstos son localizados, rechazados y devueltos a su propietarios para que sean corregidos.

# AC1 - Preparación y Autorización de Información Fuente

***PRUEBAS DE LOS RESULTADOS DEL CONTROL***

- Verificar, con la inspección de las listas de autorización, que los niveles de autorización están definidos adecuadamente para cada grupo de transacciones. Observar que los niveles de autorización se aplican adecuadamente.
- Inspeccionar y observar la creación y documentación de los procedimientos de preparación de información, e investigar y confirmar que se entienden los procedimientos y que se utiliza las fuentes correctas.
- Donde lo requieran los procedimientos, observar y asegurarse de que las funciones se distribuyen adecuadamente entre el creador y el autorizador.
- Inspeccionar documentos, hacer seguimiento de transacciones en el proceso y, cuando sea posible, utilizar recopilación automatizada de datos, incluyendo información muestra, módulos de auditoría incrustados o CAATs, para hacer seguimiento de transacciones y verificar que los controles de autorización de acceso son efectivos.
- Investigar y confirmar que los departamentos mantienen una lista de personal autorizado y sus firmas. Cuando sea posible, utilizar recopilación automatizada de datos, incluyendo información muestra, módulos de auditoría incrustados o CAATs, para hacer seguimiento de transacciones y verificar que la lista de personal autorizado está eficazmente diseñada para permitir/evitar que el personal introduzca información.
- Inspeccionar la lista de personal autorizado y otra documentación, y observar los procesos y procedimientos para verificar que los procesos y procedimientos utilizados para mantener la lista son adecuados y efectivos. Seleccionar una muestra de empleados y evaluar si sus niveles de autorización son proporcionados a sus funciones y responsabilidades.

# AC1 - Preparación y Autorización de Información Fuente

***PRUEBAS DE LOS RESULTADOS DEL CONTROL***

- Investigar y confirmar que todos los documentos fuentes incluyen componentes estándar como códigos de entrada predeterminados y valores por defecto para reducir errores, registrar hora y fecha de la transacción para proporcionar un seguimiento, y capturar información de autorización para asegurar la validez.
- Cuando sea posible, utilizar recopilación automatizada de datos, incluyendo información muestra, módulos de auditoría incrustados o CAATs, para seleccionar de transacciones para una verificación posterior sobre el uso de componentes estándar que mejoran la corrección y proporcionan evidencia de la autorización.
- Investigar y confirmar que, en la introducción de información, se revisan los documentos fuente; los documentos incompletos, no firmados o mal autorizados se devuelven a sus creadores para su corrección y se registran; y que los registros se revisan periódicamente para verificar que los documentos corregidos sean devueltos por su creadores a tiempo. Inspeccionar documentos fuente y revisar registros y otros documentos para verificar que los documentos incompletos se detectan eficazmente y que los creadores los completan a tiempo.
- Revisar formularios de documentos fuente y verificar que se pueden utilizar, facilitan la prevención de errores y permiten una preparación rápida y eficiente.

# AC2 – Recolección y Entrada de Información Fuente

## *CONDUCTORES*

**Conductores de Valor:**

- Introducción exacta de datos y procesamiento eficiente
- Errores detectados a tiempo
- Información delicada sobre transacciones asegurada

**Conductores de Riesgo:**

- Ineficacias de procesamiento por introducción incompleta de datos
- Integridad de datos críticos comprometida
- Violaciones de control de acceso
- Errores de introducción de datos no detectados

## *EVALUACIÓN DEL DISEÑO DEL CONTROL*

- Investigar y confirmar que los criterios de puntualidad, integridad y exactitud de los documentos fuentes están definidos y se comunican.
- Investigar y confirmar que existen procedimientos documentados para la corrección de errores, condiciones fuera de balance e introducción de anulaciones. Asegurar que los procedimientos incluyen mecanismos para un seguimiento a tiempo, corrección, aprobación y re-entrega. Evaluar procedimientos para factores como descripciones de mensajes de error y mecanismos de cancelación.
- Investigar y confirmar que existen políticas y procesos para establecer criterios para la identificación de clases de transacciones críticas que requieren documentos fuente pre-numerados u otros métodos únicos de identificar información fuente.
- Investigar y confirmar que existen políticas y procedimientos para determinar las políticas de retención de documentos. Los factores para considerar la evaluación de la política de retención de documentos incluyen la importancia de la transacción, forma de la información fuente, método de retención, ubicación de la retención, periodo de retención y requisitos de cumplimiento y regulatorios.
- Para cada gran grupo de transacciones, investigar y confirmar si hay documentación de criterios para definir la autorización para la entrada, edición, aceptación, negación y cancelación.
- Inspeccionar documentación de políticas y procedimientos para asegurar que se representan adecuadamente los criterios de puntualidad, integridad y exactitud.

# AC2 – Recolección y Entrada de Información Fuente

***PRUEBAS DE LOS RESULTADOS DEL CONTROL***

- Investigar y confirmar que los documentos fuente significativos están pre-numerados y que los números no secuenciales se identifican que se tienen en cuenta.
- Investigar y confirmar que se generan mensajes de error a tiempo, que las transacciones no se procesan a no ser que los errores sean corregidos o cancelados adecuadamente, que los errores que no se pueden corregir inmediatamente se registran y que el proceso válido de transacción continua, y que los registros de error se revisan y se actúa dentro de un periodo de tiempo específico y razonable.
- Investigar y confirmar que el personal adecuado revisa los informes sobre errores y condiciones fuera de balance; todos los errores se identifican, se corrigen y comprueban dentro de un periodo de tiempo razonable, y los errores se reportan hasta que se corrigen.
- En una muestra de flujos de transacción, investigar y confirmar que la retención de documentos fuentes se define y aplica en relación con criterios establecidos para la retención de documentos fuente.
- Seleccionar un grupo de transacciones críticas y:
  - Comparar el estado actual de los controles de acceso sobre entradas de transacciones, edición, aceptación, etc., con los criterios establecidos, políticas o procedimientos.
  - Inspeccionar si los documentos fuente críticos están pre-numerados o si se utilizan otros métodos de identificación de información fuente.
  - Inspeccionar documentación o transacciones de recorrido para identificar al personal que puede introducir, editar, autorizar, aceptar y denegar transacciones y cancelar errores.
  - Tomar una muestra de transacciones dentro de este grupo durante un periodo específico, e inspeccionar los documentos fuente para dichas transacciones. Verficar que todos los documentos fuente están disponibles.

# AC2 – Recolección y Entrada de Información Fuente

***PRUEBAS DE LOS RESULTADOS DEL CONTROL***

- Identificar y revisar números no secuenciales, vacíos y duplicados utilizando herramientas automatizadas (CAATs).
- Inspeccionar documentos, hacer seguimiento de transacciones en todo el proceso y, cuando sea posible, utilizar recopilación automatizada de datos, incluyendo datos muestra, módulos incrustados de auditoría o CAATs, para hacer seguimiento de las transacciones para verificar que los controles de autorización son efectivos y que hay evidencia suficiente que se registra y revisa de forma segura.
- Inspeccionar documentos, hacer seguimiento de transacciones en todo el proceso y, cuando sea posible, utilizar recopilación automatizada de datos, incluyendo datos muestra, módulos incrustados de auditoría o CAATs, para hacer seguimiento de las transacciones para verificar que se generan, aplican y revisan adecuadamente los mensajes de error, restricciones de procesos de transacción y errores en registro.
- Inspeccionar informes de error y fuera de balance, correcciones de error, y otros documentos, para verificar que las condiciones de error y fuera de balance se revisan, corrigen, comprueban y reportan eficazmente, hasta que se corrigen.

# AC3 – Chequeos de Exactitud, Integridad y Autenticidad

## *CONDUCTORES*

**Conductores de Valor:**

- Errores de procesamiento de datos eficientemente remediados
- Durante el proceso, se mantiene la exactitud, integridad y validez de los datos
- Procesamiento de transacción interrumpido
- Segregación de tareas para la introducción y procesamiento de datos

**Conductores de Riesgo:**

- Ineficiencias de procesamiento y re-trabajo debido a una introducción de datos incompleta, inválida o inexacta
- Integridad comprometida de datos críticos
- Errores de introducción de datos sin detectar
- Introducción de datos desautorizada

## *EVALUACIÓN DEL DISEÑO DEL CONTROL*

- Investigar y confirmar que existen políticas y procedimientos para la gestión de transacciones que no realizan comprobaciones de edición o validación.
- Investigar y confirmar que existen procesos y procedimientos para la segregación de tareas para la introducción, modificación y aprobación de información de la transacción, así como para las normas de validación. Los factores a tener en cuenta en la evaluación de las políticas de segregación de tareas incluyen la importancia del sistema de transacción y métodos para la aplicación de la segregación de tareas.
- Investigar y confirmar que se revisan, confirman y actualizan a tiempo los criterios de validación y parámetros sobre introducción de datos, de forma apropiada y autorizada.
- Para los sistemas importantes o críticos, inspeccionar el diseño de introducción de datos para asegurar que los controles de autorización sólo permiten la introducción o modificación de datos a personas debidamente autorizadas.
- Obtener una descripción funcional e información del diseño de controles de introducción de datos. Inspeccionar la funcionalidad y diseño de los controles adecuados. Los ejemplos de controles incluyen la presencia de secuencia, límite, rango, validez, razonabilidad, búsquedas en tablas, existencia, verificación clave, comprobación de dígitos, integridad (por ejemplo, cantidad monetaria total, artículos totales, documentos totales, encriptaciones totales), duplicación, verificaciones lógicas de relaciones y ediciones de tiempo.

# AC3 – Chequeos de Exactitud, Integridad y Autenticidad

## *EVALUACIÓN DEL DISEÑO DEL CONTROL*

- Obtener descripciones funcionales y información de diseño en controles de autorización de introducción de datos. Inspeccionar la funcionalidad y el diseño para la presencia de chequeos de la autorización.
- Obtener descripciones funcionales y información de diseño de transacciones de introducción de datos. Inspeccionar la funcionalidad y el diseño para la presencia de chequeos completos y a tiempo y mensajes de error. A ser posible, observar la transacción de introducción de datos.
- Obtener descripciones funcionales y información de diseño en transacciones de validación de datos.

## *PRUEBAS DE LOS RESULTADOS DEL CONTROL*

- Inspeccionar informes de error y fuera de balance, corrección de errores y otros documentos para verificar que los errores y las condiciones fuera de balance se revisan, corrigen, comprueban y reportan con efectividad hasta el momento de su corrección.
- Inspeccionar correcciones de errores, condiciones de fuera de balance, invalidación de entradas y otros documentos para verificar que se siguen los procedimientos.
- Seleccionar un ejemplo de fuente de entradas de documentos fuente. Usando inspección, CAATs, u otra recopilación automatizada de datos y herramientas de evaluación, validar que los datos de entrada son una representación completa y exacta de documentos fuente.
- Seleccionar un ejemplo de entrada de datos fuente. Investigar y confirmar que hay mecanismos que aseguren que los procesos de entrada de datos fuente se han realizado de acuerdo con el criterio establecido en tiempo, compleción y exactitud.
- Investigar y confirmar que las rutinas de edición y validación de defectos en transacciones son seguidos de forma adecuada hasta su solución.

# AC4 – Integridad y Validez del Procesamiento

## *CONDUCTORES*

**Conductores de Valor:**

- Procesar errores detectados oportunamente
- Habilidad de investigar problemas

**Conductores de Riesgo:**

- Evidencia insuficiente de los errores o mal uso
- Errores no detectados de introducción de datos
- Procesamiento de datos no autorizado

## *EVALUACIÓN DEL DISEÑO DEL CONTROL*

- Investigar y confirmar que el procesamiento de datos se lleva a cabo sólo después de ser debidamente autorizado.
- Revisar la documentación de las herramientas y aplicaciones para verificar que son aplicables y adecuadas para la tarea. En el caso de que sea apropiado para transacciones criticas, revisar el código para confirmar que los controles en las herramientas y las aplicaciones operan tal y como se ha diseñado. Reprocesar un ejemplo representativo para verificar que las herramientas automatizadas operan tal y como se pretendía.
- Obtener descripciones funcionales e información de diseño en controles de entrada de datos. Inspeccionar la funcionalidad y el diseño para la presencia de secuencia y duplicación de errores, comprobaciones referenciales de integridad, control, y funciones resumen de totales. Con herramientas de búsqueda, identificar casos en donde se han encontrado errores de manera errónea y casos donde no se han detectado errores.
- Revisar la descripción funcional y el diseño de las transacciones de entrada de datos, de cara a verificar si las rutinas que provocan fallos de edición y validación provocan la suspensión de los ficheros. Verificar si los archivos suspendidos son producidos correctamente y de forma consistente y los usuarios son informados de las transacciones destinadas a cuentas suspendidas. Verificar que los procesos y transacciones no se retrasen por errores de entrada o autorización de la transacción. Utiliza la recopilación de datos automatizada, incluyendo los datos de muestra, los casos base de transacciones preparadas con un resultado esperado, los módulos integrados de auditoría o CAAT, de cara a trazar transacciones para verificar que las transacciones se procesan con eficacia, las operaciones son procesadas sin interrupciones por transacciones inválidas y que las transacciones erróneas sean reportadas.

# AC4 – Integridad y Validez del Procesamiento

## *EVALUACIÓN DEL DISEÑO DEL CONTROL*

- Analizar una muestra representativa de transacciones erróneas de suspensión de cuentas y archivos, verificando que las rutinas de validación de transacciones fallidas son chequeadas hasta su solución. Verificar que las cuentas y ficheros suspendidas por las rutinas de validación de errores de transacción, contienen únicamente errores recientes, que confirmen que los antiguos han sido adecuadamente solucionados.
- Investigar y confirmar que se indica la secuencia de trabajos a operaciones informáticas. Investigar y confirmar que los trabajos proporcionan instrucciones adecuadas al sistema de planificación para que los datos no se añadan, cambien o pierdan inadecuadamente durante el procesamiento. Inspeccionar los documentos fuente, hacer seguimiento de transacciones durante el proceso y, cuando sea posible, utilizar la recopilación automatizada de evidencias, incluyendo datos muestra, módulos de auditoría incrustados o CAATS, para hacer seguimiento de transacciones y verificar que el software de planificación de producción de trabajo se utiliza eficazmente para que los trabajos evolucionan en la secuencia correcta y proporcionan instrucciones adecuadas a los sistemas.
- Investigar y confirmar que se asigna a cada transacción un número o identificador único y secuencial (por ejemplo, índice, fecha, hora). Inspeccionar documentos, hacer seguimiento de las transacciones durante el proceso y, si es posible, recopilación automatizada de evidencias, incluyendo datos muestra, módulos de auditoría incrustados o CAATS, para hacer seguimiento de las transacciones y verificar que no hay duplicados de transacciones que requieran identificadores únicos y que no existen vacíos que deban ser numerados secuencialmente.
- Investigar y confirmar que se mantiene la pista de auditoría de las transacciones procesadas. Inspeccionar la pista de auditoría y otros documentos para verificar que están eficazmente diseñados. Recopilación automatizada de evidencias, incluyendo datos muestra, módulos de auditoría incrustados o CAATS para hacer seguimientos de las transacciones y verificar que se mantienen adecuadamente las pistas de auditoría. Verificar que se mantienen imágenes de antes y después y que el personal adecuado las revisa periódicamente.
- Investigar y confirmar que la pista de auditoría de la transacción se mantiene y revisa periódicamente para la actividad inusual. Verificar que un supervisor, que no introduzca datos, se encarga de la revisión. Inspeccionar la pista de auditoría, transacciones (o lotes), revisiones y otros documentos; hacer seguimiento de transacciones a lo largo de los procesos; y, si es posible, recopilación automatizada de evidencias, incluyendo datos muestra, módulos de auditoría incrustados o CAATS, verificar que la revisión periódica y mantenimiento de la pista de auditoría detectan con eficacia la actividad inusual y que las revisiones de supervisores son efectivas para verificar la validez de los ajustes, cancelaciones y transacciones de alto valor a tiempo.

# AC4 – Integridad y Validez del Procesamiento

## *EVALUACIÓN DEL DISEÑO DEL CONTROL*

- Investigar y confirmar que se utilizan las herramientas adecuadas y que los límites de mantenimiento cumplen con los requisitos de seguridad. Investigar y confirmar que un supervisor revisa periódicamente la información y límites del sistema. Recopilación automatizada de evidencias, incluyendo datos muestra, módulos de auditoría incrustados o CAATS, para hacer seguimiento de transacciones y verificar que las herramientas funcionan como fueron diseñadas.
- Investigar y confirmar que se utilizan servicios, si es posible, para mantener automáticamente la integridad de la información durante interrupciones inesperadas en el procesamiento de datos. Inspeccionar la pista de auditoría y otros documentos, planes, políticas y procedimientos para verificar que las capacidades del sistema están eficazmente diseñadas para mantener automáticamente la integridad de la información. Revisar los registros de interrupciones reales sobre asuntos de integridad de datos y verificar que las herramientas adecuadas se utilizaron con eficacia.
- Investigar y confirmar que un supervisor, que no realice introducción de datos, revisa en detalle los ajustes, cancelaciones y transacciones de alto valor para comprobar su adecuación. Inspeccionar la pista de auditoría y otros documentos, planes, políticas y procedimientos para verificar que se han diseñado eficazmente los ajustes, cancelaciones y transacciones de alto nivel para ser revisados rápidamente en detalle. Inspeccionar la pista de auditoría, transacciones (o lotes), revisiones y otros documentos; hacer seguimiento de transacciones a lo largo de los procesos; y, si es posible, recopilación automatizada de evidencias, incluyendo datos muestra, módulos de auditoría incrustados o CAATS, para verificar que las revisiones del supervisor son eficaces para asegurar la validez de ajustes, cancelaciones y transacciones de alto valor a tiempo.
- Investigar y confirmar que la se realiza rutinariamente la reconciliación de totales de archivo y que se reportan condiciones fuera de balance. Inspeccionar reconciliaciones y otros documentos y hacer seguimiento de transacciones a lo largo de los procesos para verificar que las reconciliaciones determinan con eficacia si coinciden los totales de archivo o si la condición fuera de balance se reporta al personal adecuado.

# AC4 – Integridad y Validez del Procesamiento

## *PRUEBAS DE LOS RESULTADOS DEL CONTROL*

- Para una muestra de aplicación, investigar y confirmar que se realiza la división de funciones. Verificar si se ha implantado la división de funciones para la introducción, modificación y aprobación de información de transacciones, así como para las normas de validación.
- Para una muestra de procesos de transacciones críticas, comprobar si los controles de acceso previenen la introducción de información desautorizada. Con herramientas de búsqueda, identificar los casos donde personal desautorizado pueden introducir o modificar información.
- Para una muestra de sistemas de transacción, verificar si las cuentas y archivos suspensivos para transacciones, en las que fallan las rutinas de edición y validación, contienen sólo errores recientes. Confirmar que se han remediado antiguas transacciones fallidas.
- Para una muestra de transacciones, verificar que no se retrasa la introducción de datos por transacciones inválidas.
- Para transacciones altamente importantes, establecer un sistema de pruebas que opere como el sistema en vivo. Introducir diferentes tipos de error.
- Verificar si las detecciones e informes sobre errores son realizadas a tiempo y completas y si proporcionan información suficiente para corregir la transacción.
- Para transacciones altamente importantes, establecer un sistema de pruebas que opere como el sistema en vivo. Procesar transacciones en el sistema de pruebas para asegurar que se procesan adecuadamente y a tiempo las transacciones válidas.
- Asegurar que se reportan errores adecuadamente y a tiempo.
- Inspeccionar mensajes de error en la introducción de datos o procesamiento online.
- Asegurar los mensajes de error son adecuados para el flujo de la transacción. Los ejemplos de atributos de mensajes adecuados incluyen la comprensión, inmediatez y visibilidad.
- Determinar si se registran en archivos suspensivos las transacciones sin rutinas de edición y validación.
- Verificar si se producen archivos suspensivos correcta y consistentemente.
- Verificar si se informa al usuario sobre transacciones registradas en cuentas suspensivas.
- Tomar una muestra de transacciones de introducción de datos. Utilizar las herramientas de análisis y búsqueda para identificar casos en los que los errores se identificaron erróneamente y casos en los que no se detectaron.
- Recopilación automatizada de evidencias, incluyendo datos muestra, módulos de auditoría incrustados o CAATS, para verificar que se procesan sin interrupción las transacciones válidas. Inspeccionar y confirmar que se reportan transacciones inválidas a tiempo.

# AC5 – Revisión de Salidas, Reconciliación y Manejo de Errores

## *CONDUCTORES*

**Conductores de Valor:**

- Protección de salida de datos críticos
- Resultados completos y sin errores del procesamiento se entregan al receptor adecuado
- Los errores se detectan a tiempo

**Conductores de Riesgo:**

- Se entrega información crítica sobre transacciones al receptor incorrecto
- Se compromete la confidencialidad de información
- Procesamiento ineficaz de información
- Errores de salida de información no detectados

## *EVALUACIÓN DEL DISEÑO DEL CONTROL*

- Revisar criterios de diseño y confirmar que requieren el uso de procesos de control basados en integridad, como el uso de totales de control en registros de encabezamiento y/o arrastre y el equilibrio de totales de control de salida producidos por el sistema.
- Investigar y confirmar que se reportan las condiciones detectadas fuera de balance, que los informes han sido diseñados en el sistema y que se han desarrollado procedimientos para asegurar que los informes se entregan al nivel adecuado de dirección.
- Investigar y confirmar que los procedimientos requieren que las condiciones fuera de balance y otras anomalías requieren una investigación rápida e informe.
- Revisar la documentación para asegurar que los procesos especifican que se realicen inventarios periódicos de documentos críticos y que se investiguen las diferencias.
- Investigar y confirmar que se han diseñado procedimientos para asegurar que se valide la integridad y exactitud de la información de la aplicación antes de utilizar dicha información para procesamientos posteriores, incluyendo el procesamiento del usuario final.
- Investigar y confirmar que se han desarrollado procedimientos par asegurar que se revisa la información en cuento a razonabilidad, exactitud u otros criterios establecidos por el procesador, antes de su uso.
- Evaluar si se han definido procedimientos que requieran el registro de errores potenciales y su resolución antes de la distribución de los reportes.

# AC5 – Revisión de Salidas, Reconciliación y Manejo de Errores

## *PRUEBAS DE LOS RESULTADOS DEL CONTROL*

- Investigar y confirmar que se implantan totales de control en registros de encabezamiento y/o arrastre de información para equilibrar los totales de control producidos por el sistema.
- Investigar y confirmar que se informa sobre condiciones fuera de balance detectadas al nivel adecuado de dirección. Inspeccionar informes fuera de balance. Cuando sea posible, recopilación automatizada de evidencias en búsqueda de errores totales de control y verificar que se actúa correctamente y a tiempo.
- Investigar y confirmar que se realizan inventarios físicos de información crítica a intervalos apropiados. Asegurar que se comparan con los registros de inventario y que se actúa sobre las diferencias. Confirmar que se crean pistas de auditoría para registrar todas las excepciones y denegaciones de documentos críticos. Inspeccionar una muestra representativa de pistas de auditoría usando una recopilación automatizada de evidencias, si es posible, para identificar las excepciones y verificar si se han detectado y se ha actuado sobre ellas. Tomar una muestra de inventario físico y compararla con las pistas de auditoría correspondiente para verificar que la detección funciona eficazmente.
- Obtener una lista de información electrónica que se reusa en aplicaciones de usuario. Verificar que la información electrónica se testea en cuanto a integridad y exactitud antes de que la información se reutilice y reprocese. Seleccionar una muestra representativa de información electrónica y hacer seguimiento de documentos seleccionados a lo largo del proceso para asegurar que se verifica la integridad y exactitud antes de realizar otras operaciones. Volver a realizar pruebas de integridad y exactitud para validar que son efectivas.
- Investigar y confirmar que se revisa información en busca de razonabilidad y exactitud. Seleccionar una muestra representativa de informes de datos y comprobar la razonabilidad y exactitud de la información. Verificar que errores potenciales se reportan y registran centralmente. Seleccionar una muestra de transacciones representativas y verificar que se identifican y tratan los errores a tiempo. Inspeccionar errores de registro para verificar que se trata con ellos a tiempo.
- Investigar y confirmar que se define la información crítica, el procesador la acepta y se trata adecuadamente con ella. Esto puede incluir marcar la información crítica de la aplicación y, si fuera necesario, enviar información crítica a sistemas especiales de información con control de acceso. Para una muestra de datos críticos, buscar ficheros de información y confirmar que se marcan adecuadamente. Revisar los métodos de distribución de información crítica uy mecanismos de control de acceso de sistemas de información crítica. Verificar que los mecanismos refuerzan correctamente los derechos de acceso preestablecidos.

# AC6 – Autenticación e Integridad de Transacciones

## *CONDUCTORES*

**Conductores de Valor:**

- Straight Trough Processing (STP)
- Confianza en la validación y autenticación de transacciones
- Prevención de errores

**Conductores de Riesgo:**

- Transacciones erróneas y/o no autorizadas
- Transacciones erróneas no detectadas
- Trabajo duplicado e ineficiencias

## *EVALUACIÓN DEL DISEÑO DEL CONTROL*

- Investigar y confirmar que se ha designado un proceso para asegurar que, para transacciones críticas, se han establecido acuerdos con las partes interesadas apropiadas que incluyen estándares de presentación de transacciones y comunicación, responsabilidades, autenticación y requisitos de seguridad.
- Investigar y confirmar que se han diseñado sistemas para incorporar mecanismos apropiados para integridad, autenticidad y no repudio, tales como implementación de un estándar universal o uno propio verificado de manera independiente.
- Investigar y confirmar que los sistemas han sido diseñados en cumplimiento con los estándares de la industria para identificar la información de autenticación.
- Revisar los manuales y la documentación de las aplicaciones críticas para verificar que las especificaciones de diseño establecen la correcta verificación de la autenticación de la entrada de datos.
- Investigar y confirmar que el diseño de los sistemas asegura la identificación de transacciones procedentes de otras aplicaciones de procesamiento, y analizar la información para determinar la autenticidad de origen de la información, así como que la integridad de los datos se mantuvo durante la transferencia.

# AC6 – Autenticación e Integridad de Transacciones

## *EVALUACIÓN DEL DISEÑO DEL CONTROL*

- Recopilar y revisar acuerdos establecidos con partes interesadas para transacciones críticas, asegurando que dichos acuerdos especifican los requisitos de comunicación, estándars de presentación de transacciones, responsabilidades y requisitos de seguridad y atuenticación.
- Seleccionar un ejemplo de acuerdo con una parte interesada para transacciones críticas y verificar que es completo.
- Seleccionar un ejemplo de errores de autenticación para verificar que el acuerdo con la parte interesada opera de manera efectiva.
- Revisión de documentación y ejecución de un procedimiento para la identificación de aplicaciones que resultan críticas para la autenticación de transacciones, integridad y no repudio. Para estas aplicaciones, investigar y confirmar que se adoptan un mecanismos apropiados para la integridad, autenticidad y no repudio (ej., un estándar de seguridad o uno propio verificado de manera independiente).
- Revisar aplicaciones manuales y documentación de aplicaciones críticas para confirmar que el estado del diseño y la especificación obtenida es contrastada de manera apropiada con la información de autenticación.
- Efectuar una revisión del código de un ejemplo de aplicación para asegurar que se aplica este diseño y especificación. Verificar que estas especificaciones han sido probadas con resultados satisfactorios.
- Seleccionar unas transacciones representativas de ejemplo, y verificar que la integridad y autenticidad de la información se lleva a cabo correctamente a lo largo del ciclo de procesamiento.
- Revisar el log de errores de autenticación de las transacciones y verificar la causa.

## *PRUEBAS DE LOS RESULTADOS DEL CONTROL*

- Efectuar una revisión del código de algunas aplicaciones para confirmar que las especificaciones de autenticidad han sido aplicadas. Verificar que estas especificaciones han sido probadas con unos resultados satisfactorios.
- Revisar el log de errorers de autenticación de las transacciones y verificar la causa.

# La Auditoría Interna en los Sistemas de Información

## ÚLTIMAS NOVEDADES ASOCIADAS A LA GESTIÓN DE RIESGOS TECNOLÓGICOS

MAZARS

## Los 10 principales ítems a revisar por los Auditores IT (ISACA Journal)

Durante estos tiempos económicos difíciles, los diferentes departamentos de las organizaciones se ven obligados a demostrar su eficiencia y el valor que aportan. Los departamentos de auditoría interna informática, no son diferentes. Los Auditores IT están revisando el alcance de sus auditorías para garantizar que se revisarán los principales riesgos a los que se enfrenta la organización.

**A continuación se presenta una propuesta de los 10 principales ítems a revisar en 2010-2011:**

1. **Conozca los "Activos Críticos de su Organización,** así como el proceso de Gestión del Riesgo Empresarial.
2. **Revise las Normas y Políticas de Seguridad y Privacidad.** Priorizando: control de acceso, clasificación de datos y seguridad de la red; y en años siguientes: gestión de proveedores, gestión de vulnerabilidades y prevención de fuga de datos.
3. **Evalúe la eficacia del proceso de Gestión de Acceso e Identidades.**
4. **Compruebe que los usuarios comprenden sus funciones y responsabilidades en materia de seguridad y privacidad.**
5. **Evalúe la eficacia de los procesos de monitorización y seguimiento.**
6. **Revise los procesos de GRC (Gobierno, Riesgo y Cumplimiento) de la Organización.**
7. **Audite las Subcontrataciones.** La seguridad es sólo tan fuerte como el eslabón más débil.
8. **Revise los Planes de Continuidad del Negocio.**
9. **Verifique que la Dirección es consciente y entiende las iniciativas de TI.**
10. **Verifique que los riesgos de la Organización están cubiertos por una póliza de seguro adecuada.**

## OWASP: Los diez riesgos más importantes en aplicaciones web (2010)

1. **Inyecciones.** Vulnerabilidades de inyección de código, desde SQL hasta comandos del sistema.
2. **Cross-site Scripting.** El anterior número uno. Una de las vulnerabilidades más extendidas y a la par subestimada.
3. **Gestión defectuosa de sesiones y autenticación.** Comprende los errores y fallos en las funciones de gestión de sesiones y autenticación.
4. **Referencias directas a objetos inseguras.** Errores al exponer partes privadas o internas de una aplicación sin control y accesibles públicamente.
5. **Cross-site Request Forgery.** Se mantiene en el mismo puesto anterior. Vulnerabilidad consistente en el desencadenamiento de acciones legitimas por parte un usuario autenticado, de manera inadvertida por este último y bajo el control de un atacante.
6. **Ausencia de, o mala, configuración de seguridad.** Más que un error en el código se trata de la falta o mala configuración de seguridad de todo el conjunto de elementos que comprende el despliegue de una aplicación web, desde la misma aplicación hasta la configuración del sistema operativo o el servidor web.
7. **Almacenamiento con cifrado inseguro.** Referida a la ausencia o mal uso de los sistemas de cifrado en relación a los datos almacenados o manejados por la aplicación.
8. **Falta de restricciones en accesos por URL.** Falta de validación en el procesamiento de URLs que podrían ser usadas para invocar recursos sin los derechos apropiados o páginas ocultas.
9. **Protección insuficiente de la capa de transporte.** Relacionada con A7 pero orientada a la protección del tráfico de red. Elección de un cifrado débil o mala gestión de certificados.
10. **Datos de redirecciones y destinos no validados.** Errores en el tratamiento de redirecciones y uso de datos no confiables como destino.

## Nuevos Términos - ¿de qué me hablan?

| | |
|---|---|
| **Virtualización de Servidores** | En computación, la virtualización es un medio para **crear una versión virtual de un dispositivo o recurso**, como un servidor, un dispositivo de almacenamiento, una red o incluso un sistema operativo, **donde se divide el recurso en uno o más entornos de ejecución.**<br>Por ejemplo, algo tan simple como particionar un disco duro es considerado una virtualización. Esto es así, porque se toma un disco duro y la partición sirve para crear dos unidades (o más), que simulan dos discos duros. |
| **Cloud Computing (¿moda o realidad?)** | Es un paradigma donde **la información está permanentemente almacenada en servidores de Internet y "bajada," mientras se usa, a PC, notebooks u otros dispositivos "clientes"** con los que trabaje el usuario. Cualquier dispositivo conectivo a Internet podría operar con cloud computing.<br>Los **ejemplos** de uso de cloud computing son muchos e incluyen cosas como las **aplicaciones actuales de productividad individual como procesadores de texto, planillas de cálculo y también las aplicaciones corporativas** como softwares de gestión, presupuesto, reportes empresariales y muchas otras. La tendencia consiste en que el browser web sea la vía de acceso a todo lo que necesitamos para nuestro trabajo y los procesos de la empresa. |

# La Auditoría Interna en los Sistemas de Información

## CONCLUSIONES

MAZARS

# CONCLUSIONES

- El **análisis de datos del Libro Diario**, nos permite detectar y revisar con detalle los apuntes que pueden tener algún indicio de fraude o error, de cara a disminuir el muestreo de la Auditoría Interna.
- **SAS 99** establece unas pautas para detectar Fraude en una Auditoría de Estados Financieros.
- Los **controles de aplicación** consisten en actividades manuales y/o automatizadas que aseguran que la información cumple con ciertos criterios, como son los requerimientos de negocio.
- Los **controles generales de TI** son aquellos que tienen que ver con el ambiente de proceso de TI en el cual operan los controles de aplicación.
- El hecho de que los controles generales sean adecuados, no garantiza que los controles de aplicación serán adecuados. Pero **si los controles generales son deficientes, los controles de aplicación muy probablemente lo serán también**.
- **CobiT** es un Marco de Referencia enfocado al **Negocio**, orientado a **Proceso**, basado en **Controles** y dirigido por **Medidas.** No sólo define los controles generales de TI, sino que contempla los controles de aplicación.

# La Auditoría Interna en los Sistemas de Información

## PREPARACIÓN DEL PRÓXIMO DESAYUNO

MAZARS

# Preparación de la próxima sesión

Fecha :

- 21 de Mayo en Barcelona

Tema propuesto inicialmente:

- Aplicación de métodos de valoración en compañías

Otros temas interesantes:

- Cómo comprobar la validez de documentos firmados digitalmente. DNI-e. e-Factura.
- La auditoría interna continua. Definición de indicadores. Herramientas.
- Cómo implantar un Sistema de Gestión de Seguridad de la Información. Familia ISO 27000. Plan de Seguridad Corporativa.
- El buen gobierno de la Auditoría: Octava Directiva.

- Contribuciones eventuales

Juan Luque
Socio Internacional
jluque@mazars.es


# GRACIAS


Cristina Bausá
Senior Manager
mbausa@mazars.es

Juan Ignacio Utrillo
Senior Manager
jutrillo@mazars.es

Ángel Baena
Auditor Senior
anbaena@mazars.es


Puede solicitar nuestros **e-boletines gratuitos**, enviando un mail a la dirección auditoria.it@mazars.es

- ✓ e-Boletín mensual sobre **LOPD**
- ✓ e-Boletín trimestral sobre **Control y Auditoría Intern@**

MAZARS