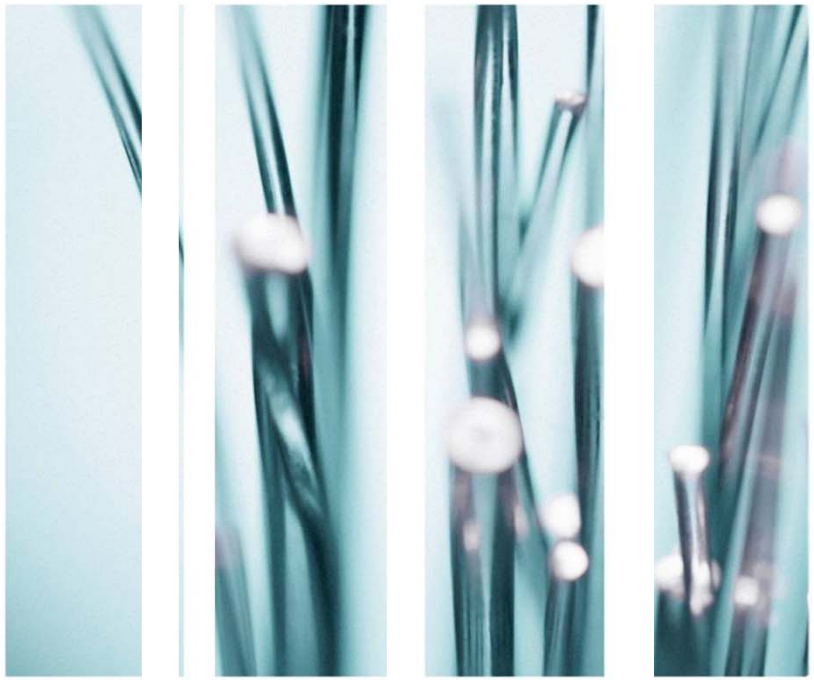
Oferta de servicios de Control Interno de MAZARS

Control Interno, Gobierno Corporativo, y Gestión de Riesgos Tecnológicos

Octubre de 2010

MAZARS



MAZARS: una organización consolidada

Valores diferenciales de Mazars

Servicios de Auditoría & Control Interno
- 3.1 Auditoría Interna
- 3.2 Control Interno y Gobierno Corporativo

Servicios de Auditoría Informática
- 4.1 Cumplimiento legal
- 4.2 Seguridad de la Información
- 4.3 Control de Servicios Externalizados
- 4.4 Governance IT
- 4.5 Soporte a la Auditoría y Control Interno

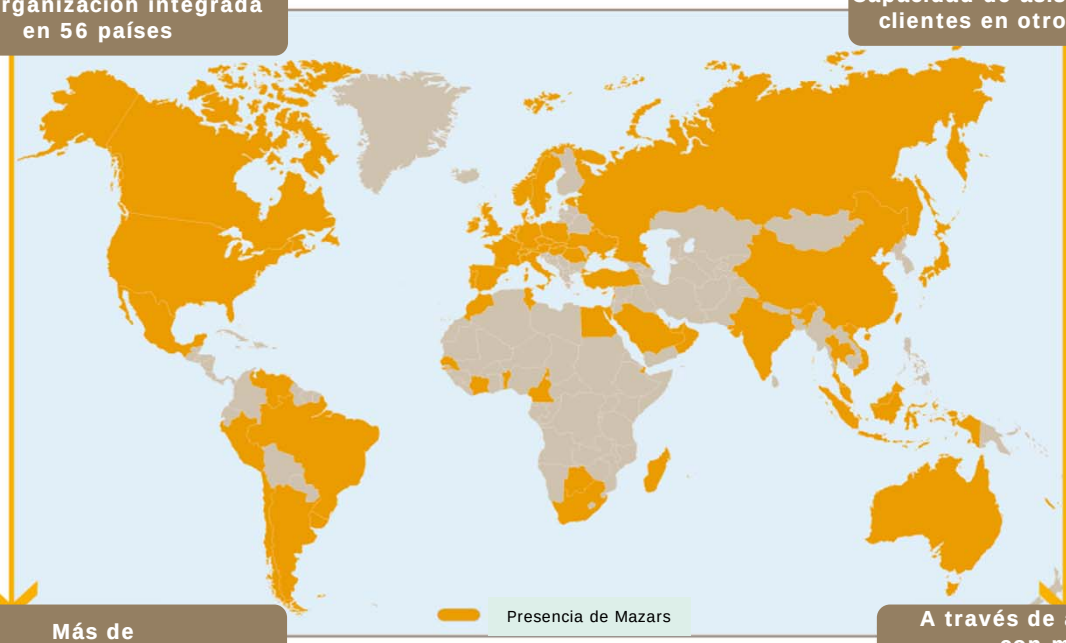
MAZARS

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



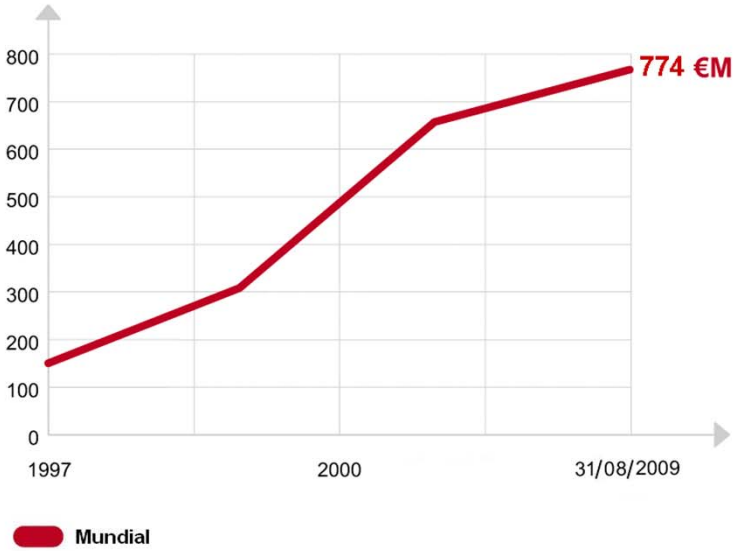
Más de 12.500 profesionales

A través de asociaciones con más de 25.000 profesionales

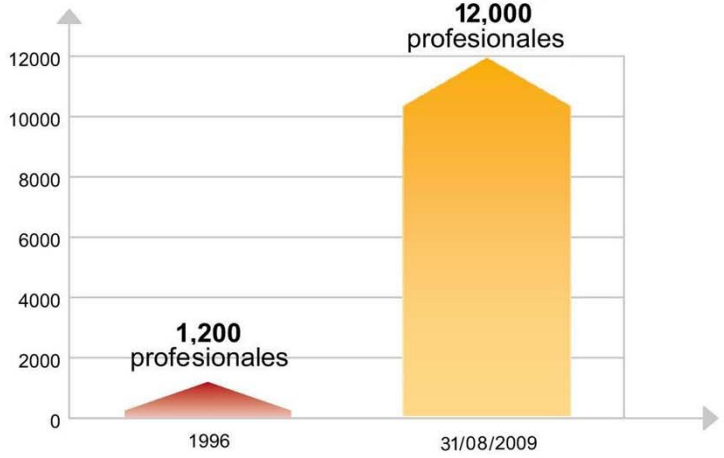
MAZARS

Una organización internacional integrada

… nuestra prioridad: la **calidad**



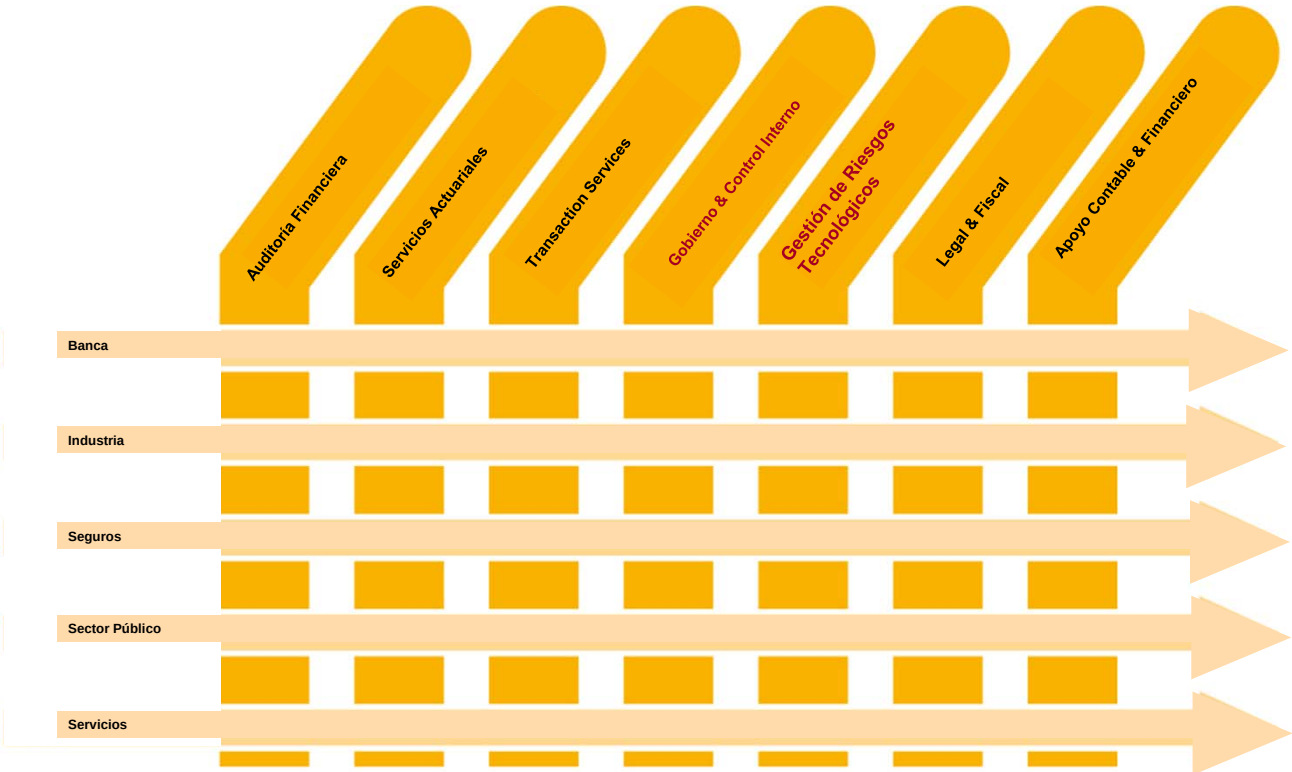
… para asegurar la **continuidad**



MAZARS

Organización matricial entre líneas de servicio y sectores de clientes

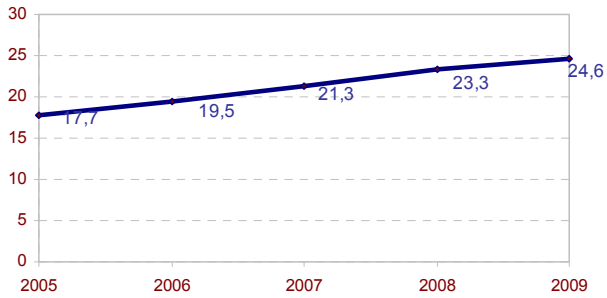
… para cumplir con las **necesidades** de nuestros **clientes**



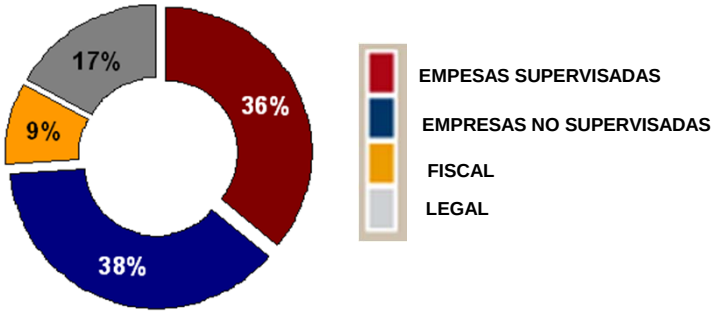
MAZARS

Mazars España en cifras

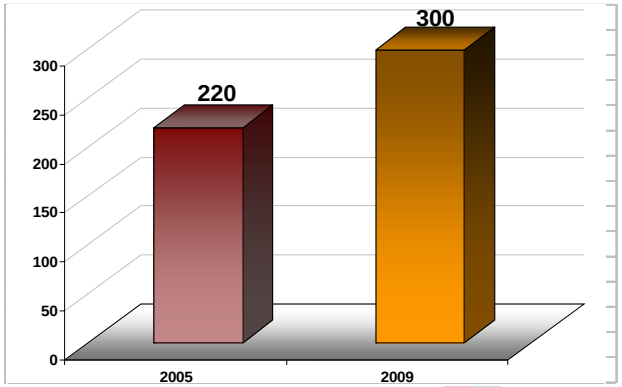
Evolución de la cifra de negocios (M€)



Cifra de negocios por ICL



Número de profesionales

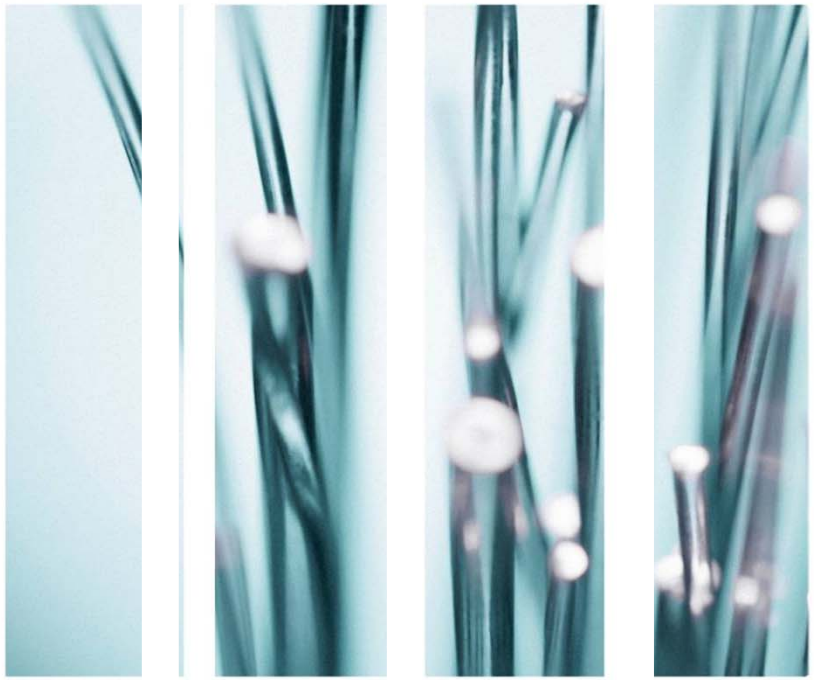


MAZARS

Mazars en España – Nuestras Referencias

Trabajamos con más de 460 sociedades cotizadas en 55 países

MAZARS



MAZARS: una organización consolidada

Valores diferenciales de Mazars

Servicios de Auditoría & Control Interno
- 3.1 Auditoría Interna
- 3.2 Control Interno y Gobierno Corporativo

Servicios de Auditoría Informática
- 4.1 Cumplimiento legal
- 4.2 Seguridad de la Información
- 4.3 Control de Servicios Externalizados
- 4.4 Governance IT
- 4.5 Soporte a la Auditoría y Control Interno

MAZARS

Valores diferenciales de Mazars

1. Equipos multidisciplinares para el asesoramiento en Control Interno y Gobierno Corporativo

- ✓ La revisión de los diferentes procesos, requieren en ocasiones de especialistas que colaboren puntualmente: expertos en fiscal, expertos en contabilidad y auditoría contable, auditores internos, etc.
- ✓ **MAZARS por su configuración, abarca las diferentes áreas de especialistas necesarios** para una buena revisión y asesoramiento en riesgos y controles.

2. Especialistas en Auditoría Informática

- ✓ La creciente automatización de los procesos de negocio, hace imprescindible una **configuración de equipo de trabajo mixto** para la revisión de los mismos, compuesta por auditores internos con conocimientos contables, y auditores informáticos que revisen los controles automatizados dentro del proceso.

3. Calidad y flexibilidad

- ✓ **MAZARS aborda sus proyectos con flexibilidad**, de cara a adaptarse al máximo a las necesidades de sus clientes, siempre bajo los principios de calidad y conocimiento de las metodologías más adecuadas en cada caso.

MAZARS

Nos distinguimos por nuestra Calidad y Profesionalidad

Conocimientos, experiencia y calidad como nuestro principal objetivo

Mazars apuesta fuertemente por su equipo de Auditoría Informática, incorporando profesionales con altos conocimientos y una larga experiencia.

Mazars es una firma independiente de las empresas tecnológicas, lo que aporta una garantía de objetividad indispensable para llevar a cabo su labor Auditora y de Asesoramiento en el Control Interno IT.

Mazars apuesta por las certificaciones internacionales de su personal, equipos multidisciplinares, y bajo una misma metodología de Grupo.

- Equipos multidisciplinares
- Orientación a Objetivos del Negocio
- Independencia Tecnológica
- Certificaciones Internacionales

Para garantizar la satisfacción de nuestros clientes

Mazars antepone la calidad de sus proyectos, para que se ajusten a las necesidades de sus clientes, y se obtengan resultados satisfactorios…

Los proyectos se orientan a la gestión de riesgos tecnológicos que impactan en la consecución de los objetivos de negocio, como factor clave…

Bajo los códigos de ética y profesionales del Grupo Mazars, y garantizando la confidencialidad de la información tratada.

CISA Certified Information Systems Auditor · CIA Certified Internal Auditor · CISM Certified Information Security Manager · CGEIT Certified in the Governance of Enterprise IT

Algunas de nuestras referencias

Auditoría interna / control interno

Gobierno corporativo

Fraude

Dirección de proyectos

MAZARS

Algunas de nuestras referencias

Gestión de Riesgos

Auditoría a terceros

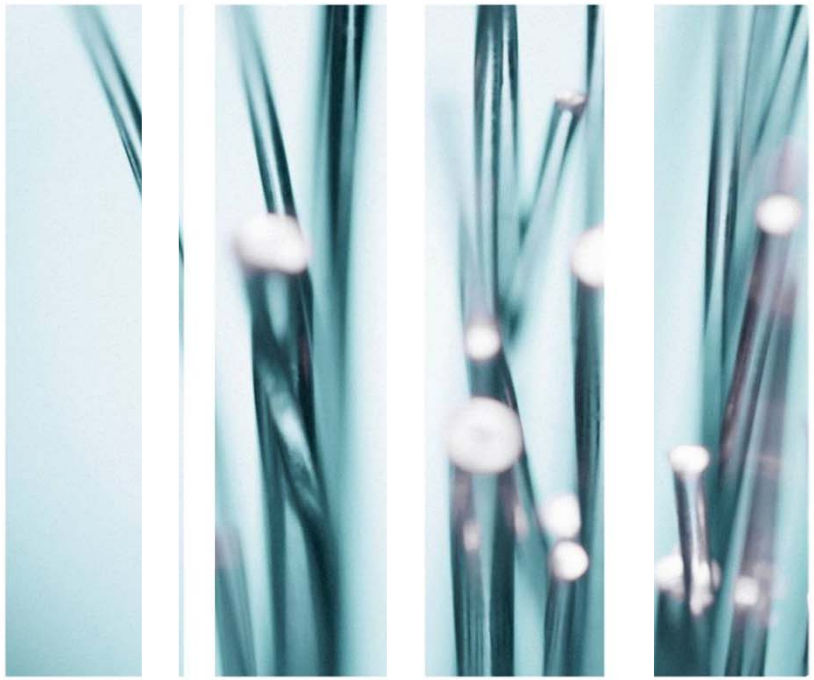
SAS 70

Análisis de datos

MAZARS

Principales Referencias de Auditoría & Control Interno IT en España

Auditoría Informática



MAZARS: una organización consolidada

Valores diferenciales de Mazars

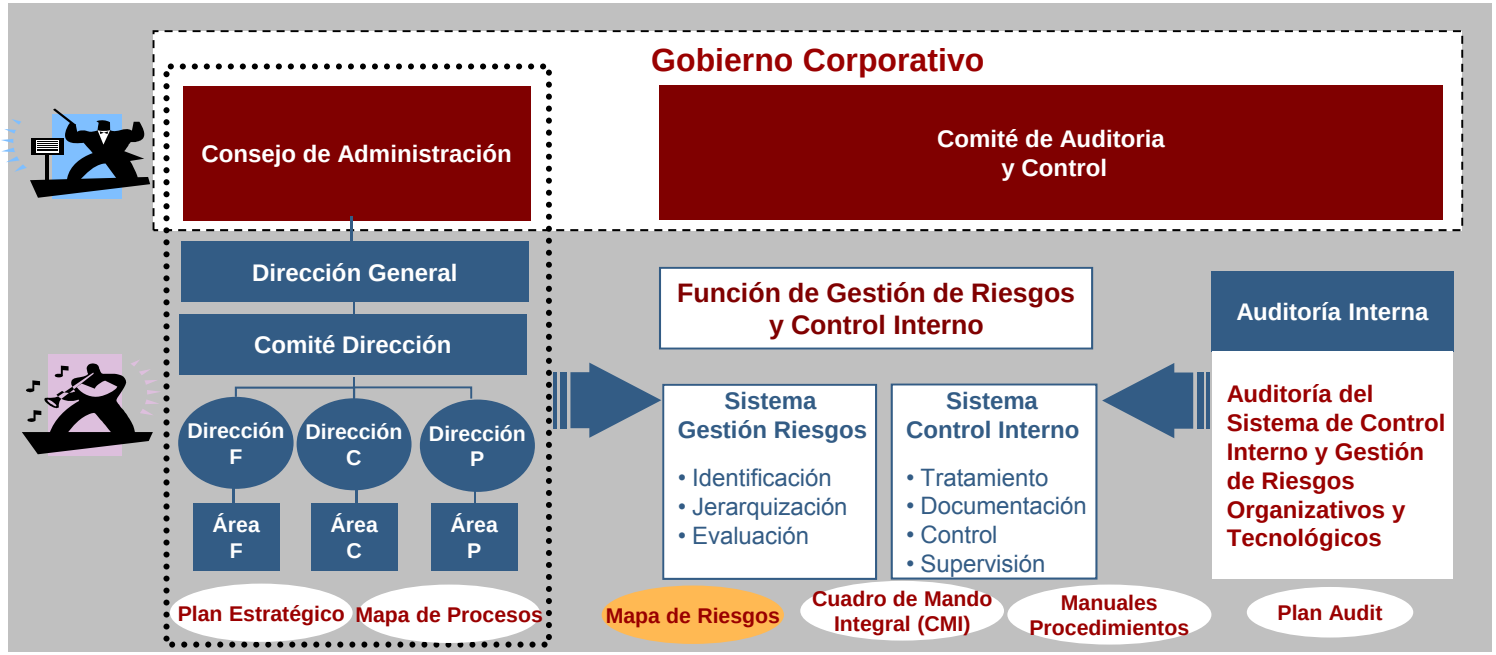
Servicios de Auditoría & Control Interno
- 3.1 Auditoría Interna
- 3.2 Control Interno y Gobierno Corporativo

Servicios de Auditoría Informática
- 4.1 Cumplimiento legal
- 4.2 Seguridad de la Información
- 4.3 Control de Servicios Externalizados
- 4.4 Governance IT
- 4.5 Soporte a la Auditoría y Control Interno

MAZARS

Servicios de Auditoría y Control Interno

El **Sistema de Gestión de Riesgos y Control Interno** es una herramienta básica del Consejo de Administración para **implementar los principios de buen gobierno** y supervisar el cumplimiento de sus objetivos **minimizando los riesgos del negocio**



MAZARS

Nuestros Servicios de Auditoría y Control Interno

1. Auditoría Interna (pág. 17)

- Auditoría de Procesos de Negocio
- Gestión de Riesgos (Mapa de Riesgos)
- Auditoría a terceros
- SAS-70

2. Control Interno y Gobierno Corporativo (pág.24)

- Documentación de Procedimientos y Control Interno
- Cuadro de Mando Integral (CMI)
- La Pérdida Desconocida

Nuestros Servicios de Auditoría y Control Interno

1. Auditoría Interna (pág. 17)

- Auditoría de Procesos de Negocio
- Gestión de Riesgos (Mapa de Riesgos)
- Auditoría a terceros
- SAS-70

2. Control Interno y Gobierno Corporativo (pág. 24)

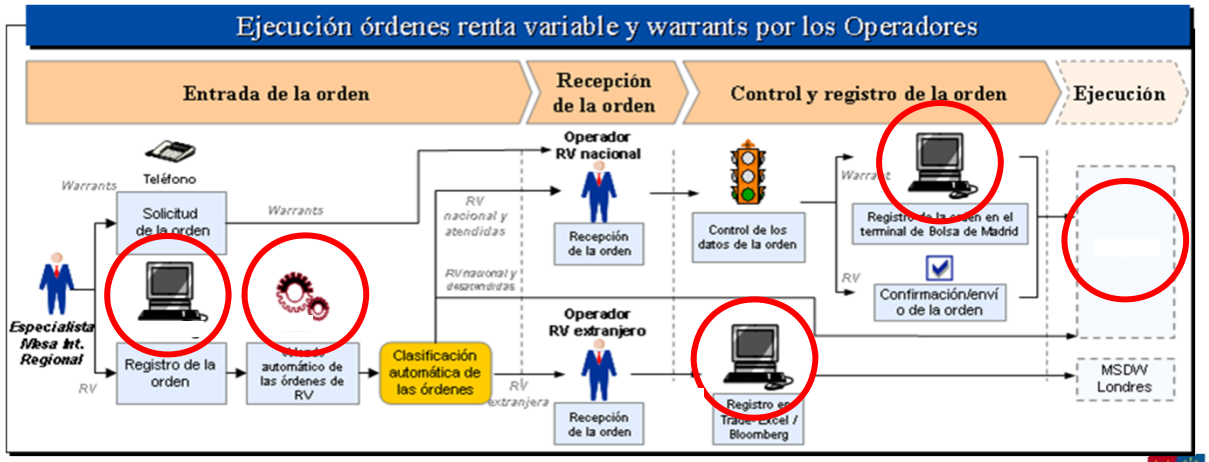
- Documentación de Procedimientos y Control Interno
- Cuadro de Mando Integral (CMI)
- La Pérdida Desconocida

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

1.1 Auditoría de Procesos de Negocio

INTRODUCCIÓN

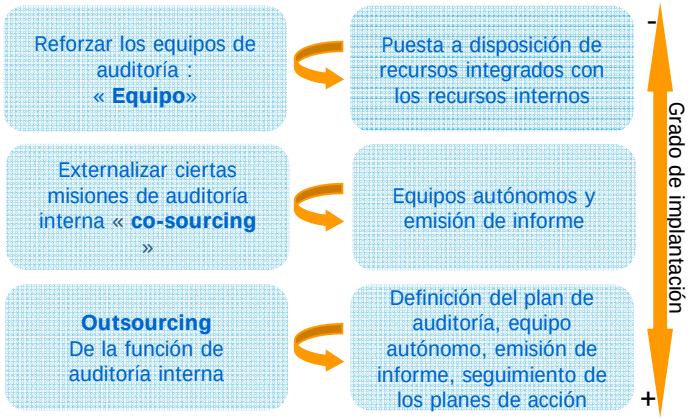
Dentro del contexto de refuerzo de responsabilidades de la Dirección, **la auditoría interna juega un elemento clave en el dispositivo de pilotaje de la empresa.**

Disponer de un colaborador externo presenta múltiples ventajas:

- Una mayor flexibilidad y una optimización de los costes de auditoría.
- El acceso al **expertise** necesario para realizar misiones de auditoría específicas.
- El aprovechamiento de mejores prácticas de otros sectores.

PRINCIPALES PUNTOS DE ATENCIÓN

- ✓ Los **recursos** destinados deben estar **alineados con los proyectos a realizar**, en términos de efectivos, de organización geográfica o de competencias y expertise.
- ✓ Aporta un valor añadido: ¿Cuáles son los riesgos no cubiertos por el Plan de Auditoría? ¿Cómo vamos controlando y realizando el seguimiento de los riesgos?
- ✓ Una reflexión: **No existe un modelo único ni standard de departamento de auditoría interna** : todo depende de la cultura de la empresa y de los proyectos encargados a la auditoría interna.



MAZARS

1.2 Gestión de Riesgos: Mapa de Riesgos

INTRODUCCIÓN

Algunas preguntas a responder: ¿Cuales son los riesgos específicos de mi sector de actividad y en mi empresa? ¿Cuales son los riesgos que pueden afectar directamente la supervivencia de mi empresa? ¿Cuales son los riesgos que yo puedo aceptar? ¿Es compartida esta visión con mi Comité de Auditoría? ¿Estoy avisado sistemáticamente, y en tiempo real, en caso de riesgos significativos?

PRINCIPALES PUNTOS DE ATENCIÓN

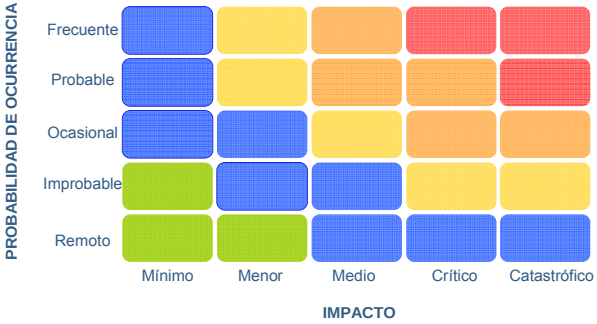
- Revisión del **conjunto de los riesgos** (procesos / puestos / funciones) en función de su actividad y sus objetivos estratégicos. Se trata de formalizar el **lenguaje común**, que servirá de marco para las evaluaciones, los análisis y las consolidaciones.
- Realizando para cada riesgo identificado la operativa siguiente:
  - ✓ **Análisis « riesgos causas » y « riesgos consecuencias »**, permitiendo obtener una visión dinámica de los acontecimientos / interacciones de riesgos entre los mismos
  - ✓ **análisis según las situaciones**, permitiendo trabajar de manera más eficaz en los planes de acciones
- Le ayudamos a aplicar el dispositivo adecuado de **seguimiento** y de **gestión**: alerta y reporting de información, consolidación, comité de los riesgos, monitorización de los planes de acción.

METODOLOGÍA

1.2 Gestión de Riesgos: Mapa de Riesgos

Resultados del Mapa de Riesgos

La creación de un mapa de riesgos.



El mapa de riesgos debe servir para ponderar los riesgos identificados con el fin de establecer controles que mitiguen la probabilidad de ocurrencia.

La definición de controles.

Riesgos Identificados ➡ **Controles recomendados para mitigar los riesgos**

Riesgo 1.

1. Control 1
2. Control 2
3. Control 3

MAZARS

1.3 Auditoría a Terceros

INTRODUCCIÓN

✓ Los **contratos** afectan a la mayoría de las operaciones de las empresas: distribución y logística, alianzas y participaciones, desarrollo, servicios generales, procesos de soporte (informática, contabilidad, gestión de la relación cliente) y el seguimiento de la **correcta ejecución** de estos contratos puede ser incorrecto.

✓Por otra parte, nuestros clientes no pueden intervenir a menudo sobre las empresas externas en la medida en que podrían tener acceso a **informaciones relativas a otras sociedades**.

✓ Contar con **auditor independiente**, puede asegurar el respeto de las reglas de carácter confidencial y presentar conclusiones objetivas.

PRINCIPALES PUNTOS DE ATENCIÓN

- **Un inventario de contratos con el fin de identificar las zonas de riesgo** - En base a los flujos contables (compras) analizamos los contratos (en base a las herramientas de análisis de datos). Nos aseguramos que las principales compras son efectivamente realizadas según contrato y analizamos la coherencia de estos contratos entre si o con los contratos marco. Al final de esta etapa se identifican las zonas de riesgo o no cubiertas.
- **Una auditoría sobre la ejecución de los contratos** - Intervenimos principalmente sobre el proveedor o cliente y nos aseguramos que se respectan los aspectos financieros plasmados en los contratos (precio, remuneración, transferencia de costes o de beneficios), analizamos igualmente cuando esto es posible, los elementos cualitativos relativos a las prestaciones.

METODOLOGÍA

MAZARS

1.4 SAS-70

INTRODUCCIÓN

✓ **La norma SAS 70,** de origen americano, es una norma de verificación del control interno adoptada por numerosos proveedores en Estados Unidos y en Europa. Esta norma aporta confianza en cuanto a la existencia y la eficacia del dispositivo de control interno puesto de marcha en una sociedad de servicios.

✓**La certificación en SAS 70 es realizada por un auditor independiente**. Esta certificación es ampliamente utilizada por las sociedades aseguradoras y empresas de consultoría y servicios a terceros y permite asegurar a sus clientes sobre el estado de su dispositivo de control interno.

PRINCIPALES PUNTOS DE ATENCIÓN

- El certificado SAS 70 está orientado sobre 4 etapas principales :
  - ✓ Definición del **perímetro** y el tipo de SAS 70 (tipo 1 o 2), Pre-evaluación
  - ✓ Identificación de los **controles clave**
  - ✓ Realización de **tests** de realidad y eficacia
  - ✓ **Revisión final** y certificación

- Un enfoque pluri-anual de la certificación permite :
  - ✓ **medir** las mejoras o los deterioros,
  - ✓ efectuar un **seguimiento regular** del dispositivo de control,
  - ✓ ajustar, optimizar y adaptar los tests a la **actividad** de la sociedad.

METODOLOGÍA

Fase 0.- Planificación y Organización → **Fase 1.- Recopilación de Información** → **Fase 2.- Trabajo de Campo** → **Fase 3.- Informe SAS-70**

Nuestros Servicios de Auditoría y Control Interno

1. Auditoría Interna (pág. 17)

- Auditoría de Procesos de Negocio
- Gestión de Riesgos (Mapa de Riesgos)
- Auditoría a terceros
- SAS-70

2. Control Interno y Gobierno Corporativo (pág.24)

- **Documentación de Procedimientos y Control Interno**
- **Cuadro de Mando Integral (CMI)**
- **La Pérdida Desconocida**

2.1 Documentación de procedimientos y control interno

INTRODUCCIÓN

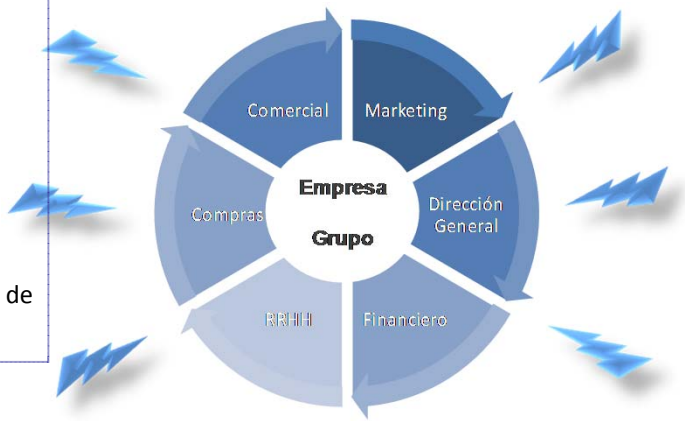
La elección de una herramienta de control interno debe realmente representar un beneficio para la organización.

- ✓Ahora existen controles internos que imperativamente tienen que ser impuestos. Estar al nivel exigido es lo habitual sin embargo ir con retraso puede ser discriminante.
- ✓Las organizaciones han evolucionado mucho, con un impacto sobre el control interno que debe además adaptarse.
- ✓El control interno debe ser una herramienta de gestión al servicio de la Dirección General con la meta de aportar garantía en el proceso de decisión y alcance de los objetivos.

PRINCIPALES PUNTOS DE ATENCIÓN

Nuestros servicios son realizados en función del nivel de madurez del dispositivo de control interno actual dentro de la empresa:

- La puesta en marcha de **un dispositivo de control interno** (identificación de riesgos, controles claves, elección de herramientas, etc..)
- El desarrollo de una **herramienta de control** interno.
- La evaluación de un dispositivo de control interno.
- La realización de la **compaña de autoevaluación**.
- **La integración** en el dispositivo de control interno **de nuevas adquisiciones**.
- La puesta al día de los dispositivos de control interno en función de **nuevas normativas y reglamentaciones.**



2.2 Cuadro de Mando Integral (CMI)

INTRODUCCIÓN

El **Cuadro de Mando Integral – CMI (Balanced Scorecard – BSC)** es un método para medir las actividades de una compañía en términos de su visión y estrategia. Proporciona a los administradores una mirada global de las prestaciones del negocio.

ACTIVIDADES A REALIZAR

☑ El CMI sugiere que veamos a la organización desde cuatro perspectivas, cada una de las cuales debe responder a una pregunta determinada:

- **Financiera**: ¿Cómo nos vemos a los ojos de los accionistas?. Índices frecuentes: de liquidez, de endeudamiento, de rendimiento del capital invertido.
- **Del cliente:** ¿Cómo nos ven los clientes? El conocimiento de los clientes y de los procesos que más valor generan es muy importante para lograr que el panorama financiero sea próspero.
- **Interna del Negocio: Procesos** ¿En qué debemos sobresalir? Se distinguen cuatro tipos de procesos:
  - Procesos de Operaciones. Indicadores son los relativos a costos, calidad, tiempos o flexibilidad de los procesos.
  - Procesos de Gestión de Clientes. Indicadores: captación de clientes, retención y crecimiento de clientes.
  - Procesos de Innovación (difícil de medir). Ejemplo de indicadores: % de productos nuevos respecto competencia.
  - Procesos relacionados con el Medio Ambiente y la Comunidad. Indicadores de Responsabilidad Social Corporativa.
- **Desarrollo y Aprendizaje:** ¿Podemos continuar mejorando y creando valor?

METODOLOGÍA

F1. Análisis de la Empresa y la Información disponible → **F2. Definición de Indicadores** → **F3. Implementación de los indicadores y del CMI** → **F4. Seguimiento**

2.3 La Pérdida Desconocida

INTRODUCCIÓN

Las empresas muchas veces no son conscientes de que se están produciendo pérdidas identificadas o sin identificar y que puede representar importes globales elevados.

- ✓ La pérdida desconocida representa alrededor del 1% (dependiendo del sector) de la facturación de las empresas. Este valor incide directamente sobre la cuenta de resultados ya que no llega a materializarse en entradas para la empresa.
- ✓ Una gestión adecuada en identificación y control de la pérdida desconocida puede ayudar a reducir ésta y por tanto a generar mayor beneficio para las empresas. El objetivo de Mazars es aportar una reflexión a las empresas en relación un aspecto que importa cada vez más.

ACTIVIDADES A REALIZAR

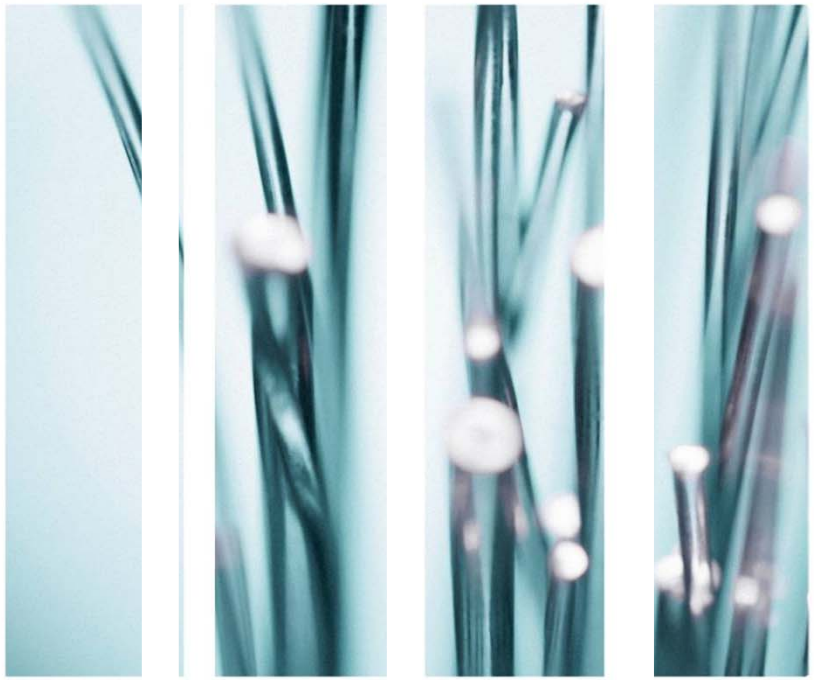
- **Identificación de las áreas donde se produce la pérdida desconocida.**
- **Apoyos a las áreas responsables de la pérdida desconocida** total o parcialmente en el desarrollo de proyectos relacionado con el tratamiento de BBDD, la Dirección del proyecto o la gestión de apoyos en el proyecto.
- **Definición y gestión de controles** necesarios para reducir la pérdida desconocida.
- **Apoyo en la elaboración de manuales de franquiciados o redes propias** relacionados con normativa sobre gestión interna (tratamiento de devoluciones, gestión de los almacenes en la tienda, recepción de la mercancía o priorización de productos anti hurto).

Conocer los daños ocasionados por la pérdida desconocida

Comprender cómo se desarrolla y crece

Descubrir una metodología que sea eficaz en su lucha

MAZARS



MAZARS: una organización consolidada

Valores diferenciales de Mazars

Servicios de Auditoría & Control Interno
- 3.1 Auditoría Interna
- 3.2 Control Interno y Gobierno Corporativo

Servicios de Auditoría Informática
- 4.1 Cumplimiento legal
- 4.2 Seguridad de la Información
- 4.3 Control de Servicios Externalizados
- 4.4 Governance IT
- 4.5 Soporte a la Auditoría y Control Interno

MAZARS

Nuestros servicios de Gestión de Riesgos Tecnológicos

1. Cumplimiento legal (pág. 30)

- Adecuación a la LOPD (Ley Orgánica de Protección de Datos de Carácter Personal)
- Auditoría bienal LOPD
- Adecuación a la LSSICE y LISI, de Impulso de la Sociedad de la Información y Comercio Electrónico
- Peritaje Informático
- Auditoría de Software Legal

2. Seguridad de la Información (pág. 40)

- Implantación del Sistema de Gestión de la Seguridad de la Información (SGSI)
- Auditoría de Buenas Prácticas de Seguridad (ISO 27002)
- Pre-auditoría de Certificación del SGSI
- Auditoría de Seguridad de Servicios Web
- Adecuación del Plan de Continuidad
- Seguridad en Tarjetas de Crédito (PCI DSS)

3. Control de Servicios Externalizados (pág. 58)

- Auditoría de Calidad de los Servicios Tecnológicos externalizados
- Asesoramiento en contratos de Servicios Tecnológicos en proceso de externalización

4. Governance IT (pág. 61)

- Asesoramiento en la implantación de CobiT
- Due-diligence de los Sistemas de Información
- Formación a medida

5. Soporte a Auditoría/Control Interno (pág. 65)

- Herramientas de Análisis de Datos. Forensic
- Análisis CCI-99 del Libro Diario
- Implantación de Proaudit Advisor como soporte al Control Interno

Nuestros servicios de Gestión de Riesgos Tecnológicos

1. Cumplimiento legal (pág. 30)

- **Adecuación a la LOPD (Ley Orgánica de Protección de Datos de Carácter Personal)**
- **Auditoría bienal LOPD**
- **Adecuación a la LSSICE y LISI, de Impulso de la Sociedad de la Información y Comercio Electrónico**
- **Peritaje Informático**
- **Auditoría de Software Legal**

2. Seguridad de la Información (pág. 40)

- Implantación del Sistema de Gestión de la Seguridad de la Información (SGSI)
- Auditoría de Buenas Prácticas de Seguridad (ISO 27002)
- Pre-auditoría de Certificación del SGSI
- Auditoría de Seguridad de Servicios Web
- Adecuación del Plan de Continuidad
- Seguridad en Tarjetas de Crédito (PCI DSS)

3. Control de Servicios Externalizados (pág. 58)

- Auditoría de Calidad de los Servicios Tecnológicos externalizados
- Asesoramiento en contratos de Servicios Tecnológicos en proceso de externalización

4. Governance IT (pág. 61)

- Asesoramiento en la implantación de CobiT
- Due-diligence de los Sistemas de Información
- Formación a medida

5. Soporte a Auditoría/Control Interno (pág. 65)

- Herramientas de Análisis de Datos. Forensic
- Análisis CCI-99 del Libro Diario
- Implantación de Proaudit Advisor como soporte al Control Interno

Nuevo Reglamento que desarrolla la LOPD (RD 1720/2007)

Sanciones en España

LEVE	600 €	60.000 €
GRAVE	60.000 €	300.000 €
MUY GRAVE	300.000 €	600.000 €

SANCIONES IMPUESTAS

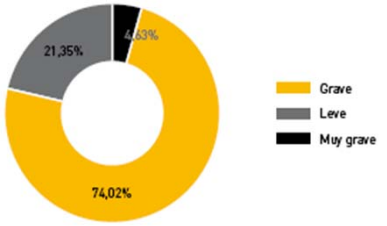
	2007	2008	2009	% VAR. 2008/2009
TOTAL	17.584.198,42 €	22.013.632,57 €	24.872.979,72 €	+12,99

La tabla recoge el total de sanciones declaradas.

ACTUACIONES PREVIAS Y TUTELAS DE DERECHOS INICIADAS

TIPO	2007	2008	2009	% VAR. 2008/2009
Tutela de los derechos de acceso, rectificación, cancelación y oposición	896	1.687	1.881	+11,50
Actuaciones previas de inspección* (iniciadas a partir de denuncia o a iniciativa del Director)	1.624	2.362	4.136	+75,11
TOTAL	2.520	4.049	6.017	+48,60

SANCIONES IMPUESTAS SEGÚN LA GRAVEDAD 2009



Las resoluciones de la Agencia Española de Protección de Datos (tanto si resuelven archivar, como si resuelven sancionar) son PUBLICAS, por lo que afectan directamente en la imagen de la firma

MAZARS

¿Qué necesitamos para cumplir con la legislación vigente?

Ficheros inventariados y registrados en la Agencia	Todos los ficheros con datos de carácter personal, tanto informatizados, como en papel, tienen que estar inscritos en la AEPD.
Documento de Seguridad difundido y que se cumpla	Es obligatorio disponer de un Documento de Seguridad con los ficheros a proteger, las medidas organizativas y técnicas, las normas y procedimientos exigidos. Tiene que estar actualizado y cumplirse.
Medidas de Seguridad implantadas	La legislación vigente define las medidas de seguridad que deben contar los ficheros informatizados y en papel, en función de su nivel de protección.
Cláusulas en Formularios de captación de datos de carácter personal	Cuando se recaban los datos de un interesado (cliente, empleado, proveedor, etc) debemos informarle de la existencia del fichero y dónde ejercer sus derechos, y solicitarle consentimiento en algunos casos.
Cláusulas en contratos con terceros	En los contratos con otras empresas se deben recoger las responsabilidades de los terceros respecto a los datos que pueden manejar.
Procedimientos / herramientas para: gestión de soportes, incidencias, controlar el ejercicio de derechos, controles periódicos	Las aplicaciones de Gestión LOPD facilitan la actualización del Documento de Seguridad y la implantación de todos los requerimientos requeridos.
Auditoría (en algunos casos)	Para los datos de nivel medio o alto, tanto informatizados como en papel, se exige una auditoría de las medidas de seguridad, cada dos años.

Ley Orgánica de Protección de Datos de Carácter Personal

INTRODUCCIÓN

La necesidad de garantizar un **derecho fundamental de los ciudadanos**, como es el de la **defensa** de su privacidad y la **de sus datos**, ha generado un marco legal en nuestro país, articulado a través de una serie de leyes, reales decretos e instrucciones.

Todas las Organizaciones que tratan datos de carácter personal, **deben adecuarse a la legislación vigente**. Su incumplimiento puede conllevar **sanciones entre 600€ y 600.000€,** además de riesgos de pérdidas en la imagen pública.

ACTIVIDADES A REALIZAR

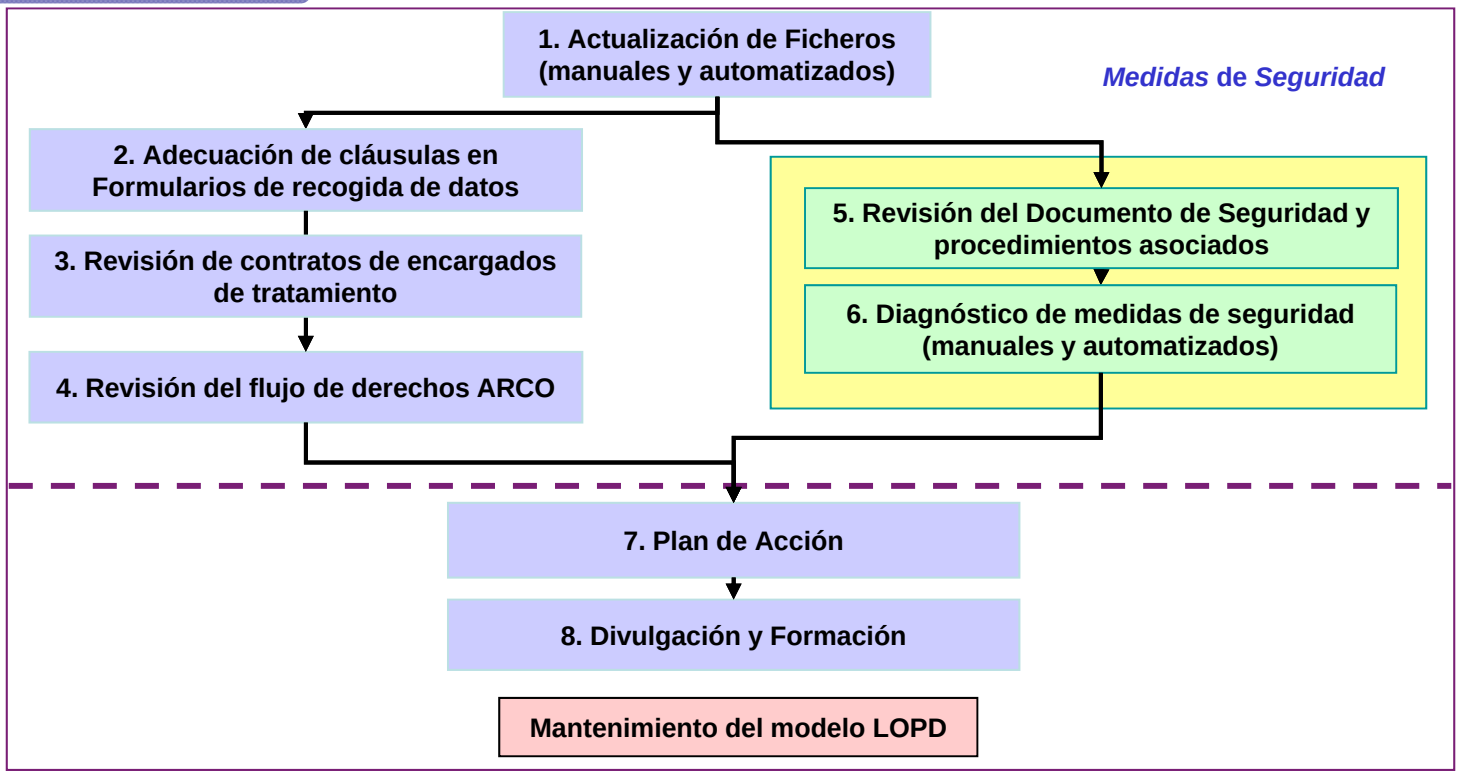
- ☑Revisar y adecuar el **Inventario de ficheros** automatizados que contengan datos de carácter personal.
- ☑Diagnóstico para conocer el grado de **adecuación de las medidas organizativas** a la LOPD (procedimientos, formularios, contratos).
- ☑ Diagnóstico del grado de adecuación de las **Medidas de Seguridad** de los Sistemas de Información y ficheros manuales al Título VIII del RD 1720/2007.
- ☑Adecuar el **Documento de Seguridad** exigido por el RD 1720/2007.
- ☑Elaborar un **plan de acción para la adecuación** de la organización a la legislación vigente.
- ☑**Formar** y concienciar a las personas involucradas en la protección de los datos.

MARCO LEGAL

- ☑ **L.O. 15/1999** de Protección de los Datos de Carácter Personal (LOPD).
- ☑ **RD. 994/1999.** Reglamento de Medidas de Seguridad.
- ☑ **RD 1720/2007**, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de protección de datos de carácter personal.

Ley Orgánica de Protección de Datos de Carácter Personal

METODOLOGÍA



1.2 Auditoría bienal LOPD

Ley Orgánica de Protección de Datos de Carácter Personal

INTRODUCCIÓN

La realización de auditorías con carácter mínimo bienal es una **exigencia del R.D. 1720/2007** por el que se aprueba el Reglamento de desarrollo de la L.O. 15/1999 de Protección de Datos de Carácter Personal.

Su incumplimiento en ficheros con datos de nivel medio (comisión de infracciones administrativas o penales, solvencia patrimonial y crédito, aspectos de personalidad, y datos responsabilidad de Administraciones Tributarias, Servicios Financieros y Gestoras de la Seguridad Social) **y alto** (Ideología, Afiliación sindical, religión, creencias, origen racial, salud, vida sexual, y trafico/localización en prestadores de servicios de comunicaciones) **podría conllevar sanciones de hasta 300.000 €.**

ACTIVIDADES A REALIZAR

- ☑**Revisión del Documento de Seguridad** e identificar los cambios necesarios, si proceden, para adecuarlo a la legislación vigente y al entorno tecnológico-organizativo.
- ☑**Conocer el grado de implantación y cumplimiento del citado Documento de Seguridad**, las deficiencias existentes y las acciones correctoras necesarias.
- ☑**Disponer del Informe de Auditoría** exigido en el Reglamento para los ficheros con datos de nivel medio y/o alto.
- ☑**Opcional:** Diagnóstico de adecuación de las Medidas Organizativas

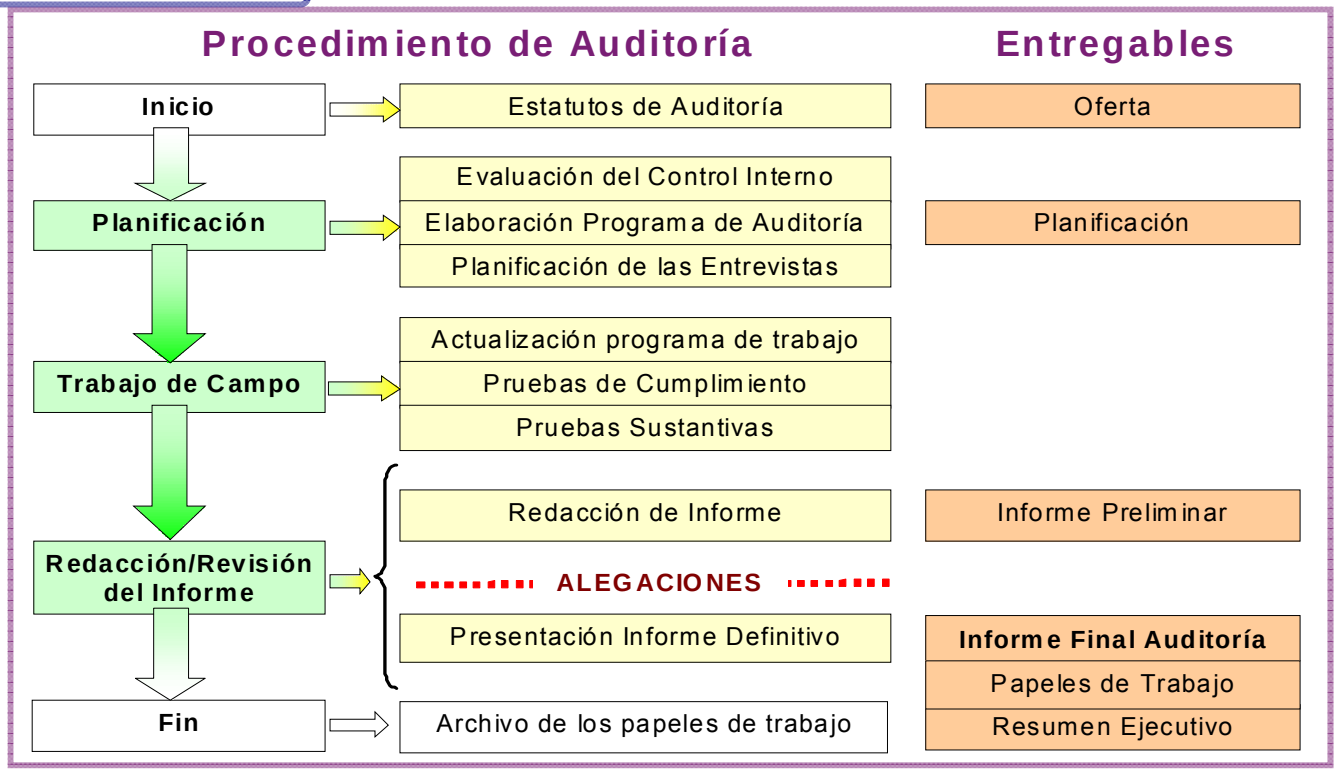
MARCO LEGAL

- ☑ **L.O. 15/1999** de Protección de los Datos de Carácter Personal (LOPD).
- ☑ **RD 1720/2007**, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de protección de datos de carácter personal.

1.2 Auditoría bienal LOPD

Ley Orgánica de Protección de Datos de Carácter Personal

METODOLOGÍA



MAZARS

1.3 Adecuación a la LSSICE y LISI

Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSICE)
Ley de Medidas de Impulso de la Sociedad de la Información (LISI)

INTRODUCCIÓN

- La **Sociedad de la Información** viene determinada por Internet como vehículo de intercambio de información. La Ley 34/2002 pretende establecer un **marco jurídico adecuado**, que genere en todos los actores la **confianza necesaria para el empleo de este medio**. Su **incumplimiento** puede acarrear **sanciones de hasta 600.000 €**.
- **La Ley 56/2007, de Medidas de Impulso de la Sociedad de la Información**, conocida como **LISI**, entró en vigor el 29 de Diciembre de 2008. La ley establece la obligación para las empresas con especial incidencia en la actividad económica, tales como las compañías dedicadas al suministro de electricidad, agua y gas, telecomunicaciones, entidades financieras, aseguradoras, grandes superficies, transportes, agencias de viaje, de asegurar a sus usuarios, un canal de comunicación electrónica que les permita el uso de la firma electrónica y **DNI-e**.

ACTIVIDADES A REALIZAR

- ☑Elaborar un **diagnóstico** para conocer el grado de adecuación de la organización a la LSSICE y LISI.
- ☑Elaborar un **plan de acción** para la adecuación de los Servicios ofrecidos por Internet.
- ☑**Formación y Concienciación** de las personas involucradas en los Servicios ofrecidos utilizando las redes de telecomunicaciones.

MARCO LEGAL

- ☑ LEY 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, y modificaciones posteriores.
- ☑ Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.

METODOLOGÍA

Fase 0.- Planificación y Organización → **Fase 1.- Recopilación de Información** → **Fase 2.- Diagnóstico de Adecuación a la LSSI/LISI** → **Fase 3.- Plan de Acción** → **Fase 4.- Formación**

1.4 Peritaje Informático

INTRODUCCIÓN

- **MAZARS** configura una estructura de grupo, donde **tanto profesionales con diferentes perfiles jurídicos**, y **profesionales informáticos certificados internacionalmente** en auditoría, están habituados a colaborar con el fin de llevar a cabo las investigación con el objeto de obtener evidencias electrónicas que aporten, y estén redactadas convenientemente para presentarlas frente a un Tribunal.
- Habitualmente se recurre a pruebas periciales informáticas en asuntos de delitos contra la propiedad privada e intelectual, espionaje industrial, protección de datos personales, fraudes, sabotajes, asuntos penales (p.e. pornografía infantil en internet), etc.

ACTIVIDADES A REALIZAR

1. **Adquisición de las pruebas:** Recogida de todos elementos que van a intervenir en la investigación. Es importante que el proceso de intervención de los equipos informáticos se lleve a cabo con todas las garantías para las partes, preservando la validez de las evidencias y la cadena de custodia.
2. **Investigación:** El perito informático realiza un análisis exhaustivo de los equipos informáticos, en busca de todos aquellos elementos que puedan constituir evidencia electrónica.
3. **Elaboración de la memoria:** En el informe constan los pasos para la adquisición de pruebas, las acciones realizadas durante la fase de investigación, las herramientas empleadas para la adquisición de la evidencia electrónica, y los resultados obtenidos con el fin de extraer las conclusiones finales de la investigación, expuesto de una manera clara, ordenada y correcta, contando con instrumentos para asegurar la corrección y calidad de la argumentación.

Un buen informe pericial puede llevar a las partes a adoptar un **acuerdo**, sin que el juicio llegue a celebrarse.

1.5 Auditoría de Software Legal

INTRODUCCIÓN

Los riesgos que conlleva la realización de copias no autorizadas de software original son diversos para las empresas o entidades de cualquier tipo, entre otros:

- ✓Sanciones y multas
- ✓Problemas técnicos, por inexistencia de asistencia técnica
- ✓No actualización tecnológica,
- ✓Impacto negativo en la calidad del software y deterioro de la imagen empresarial.

ACTIVIDADES A REALIZAR

- ☑Recopilación de información. Cuestionario preliminar para conocer las normas de la organización en cuanto a software legal, y las licencias adquiridas.
- ☑Inspección in-situ del número de equipos que se defina en la propuesta de proyecto.
- ☑Elaboración de un Informe de Conclusiones y un Plan de Acción para solventar las deficiencias detectadas.

MARCO METODOLÓGICO

- ☑ Guía de Auditoría de Software Original de la Business Software Alliance

METODOLOGÍA

Fase 0.- Planificación y Organización ▶ **Fase 1.- Recopilación de Información** ▶ **Fase 2.- Trabajo de Campo** ▶ **Fase 3.- Informe y Plan de Acción**

Nuestros servicios de Gestión de Riesgos Tecnológicos

1. Cumplimiento legal (pág. 30)

- Adecuación a la LOPD (Ley Orgánica de Protección de Datos de Carácter Personal)
- Auditoría bienal LOPD
- Adecuación a la LSSICE y LISI, de Impulso de la Sociedad de la Información y Comercio Electrónico
- Peritaje Informático
- Auditoría de Software Legal

2. Seguridad de la Información (pág. 40)

- **Implantación del Sistema de Gestión de la Seguridad de la Información (SGSI)**
- **Auditoría de Buenas Prácticas de Seguridad (ISO 27002)**
- **Pre-auditoría de Certificación del SGSI**
- **Auditoría de Seguridad de Servicios Web**
- **Adecuación del Plan de Continuidad**
- **Seguridad en Tarjetas de Crédito (PCI DSS)**

3. Control de Servicios Externalizados (pág. 58)

- Auditoría de Calidad de los Servicios Tecnológicos externalizados
- Asesoramiento en contratos de Servicios Tecnológicos en proceso de externalización

4. Governance IT (pág. 61)

- Asesoramiento en la implantación de CobiT
- Due-diligence de los Sistemas de Información
- Formación a medida

5. Soporte a Auditoría/Control Interno (pág. 65)

- Herramientas de Análisis de Datos. Forensic
- Análisis CCI-99 del Libro Diario
- Implantación de Proaudit Advisor como soporte al Control Interno

Sistema de Gestión de la Seguridad de la Información (SGSI)

INTRODUCCIÓN

Premisas básicas a considerar en materia de Seguridad de la Información:

- La información es un activo estratégico para las organizaciones.
- Cualquier incidencia de seguridad que afecte negativamente en la información tiene un grave impacto económico/social y en la imagen de las organizaciones.
- La seguridad absoluta no existe, pero se puede alcanzar un nivel de riesgo aceptable.

La seguridad NO es una actividad estática ni pasiva

Es necesario establecer un Sistema de Gestión de la Seguridad de la Información, que:

- Asegure la conformidad con la legislación vigente.
- Reduzca el impacto de los incidentes.
- Garantice la consistencia de las acciones de seguridad que se emprendan.
- Mejore la confianza de usuarios y afectados.
- Propicie una mejora continua del nivel de seguridad, reduciendo los riesgos de la organización.

MARCO METODOLÓGICO

Familia 27000 – Gestión de Seguridad de la Información

☑ ISO 27000. Documento típico de vocabulario y definiciones.

☑ ISO 27001. Permite certificar (especifica requisitos), por entidad acreditada para ello, el Sistema de Gestión de Seguridad de la Información. Basado como otros en el ciclo PDCA.

☑ ISO 27002. **Código de buenas prácticas para la Gestión de Seguridad de la Información.**

Sistema de Gestión de la Seguridad de la Información (SGSI)

ACTIVIDADES A REALIZAR

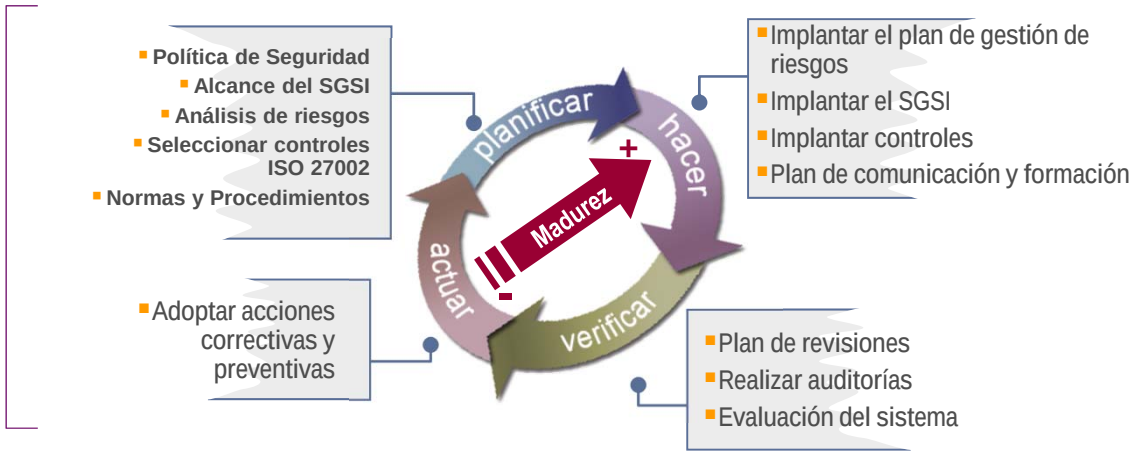
☑Definición del SGSI

- o Delimitación del Alcance
- o **Análisis de Riesgos**
- o Gestión de Riesgos
- o Declaración de Aplicabilidad
- o Definición de la **Política y Normativa de Seguridad**
- o Definición de Procedimientos de Gestión de la Seguridad
- o Implantación del SGSI. Oficina técnica de Seguridad y cuadro de mando.
- o Gestión de Incidencias
- o Elaboración del **Plan Director de Seguridad**
- o Plan de Continuidad de Negocio
- o Gestión el cambio. Plan de Concienciación y Formación.

☑Ejecución, seguimiento y revisión del SGSI y el **Plan Director de Seguridad**

Sistema de Gestión de la Seguridad de la Información (SGSI)

METODOLOGÍA



Hay que medir para controlar

Hay que medir para saber a dónde vamos

ISO 27002 - Buenas prácticas para la Gestión de Seguridad de la Información

INTRODUCCIÓN

- Muchas organizaciones reconocen los beneficios potenciales que las Tecnologías de la Información (T.I.) pueden proporcionar. No obstante, una preocupación que surge en los niveles más altos de las organizaciones, es que **cuanto mayor sea el empleo de la tecnología, mayor será también la dependencia de ella, y consecuentemente mayores serán los riesgos derivados de su utilización**.
- Una Auditoría de buenas prácticas de Seguridad, **proporciona a la Dirección, una visión independiente del nivel de seguridad en que se encuentran los Sistemas de Información de su Organización**.

ACTIVIDADES A REALIZAR

☑Revisar las Políticas de Seguridad y los Procedimientos asociados e identificar los cambios necesarios, si proceden, para adecuarlo a la norma ISO 27002.

☑Conocer el grado de implantación y cumplimiento de las Políticas de Seguridad y los procedimientos asociados, las deficiencias existentes y las acciones correctoras necesarias.

☑Disponer un Informe Independiente que se pronuncie sobre la Adecuación de la Seguridad de los Sistemas de Información al standard ISO 27002.

MARCO METODOLÓGICO

☑ ISO 27002:2005. Código de buenas prácticas para la Gestión de Seguridad de la Información.

ISO 27002 - Buenas prácticas para la Gestión de Seguridad de la Información

MARCO METODOLÓGICO

ISO 27002 - Buenas prácticas para la Gestión de Seguridad de la Información

METODOLOGÍA

Fases	*Actividades*	*Entregables*
Fase 0.- Organización del proyecto	❖ Presentación del proyecto al Área de Auditoría Interna y al Área de Sistemas de Información (SS.II). ❖ Solicitud de Información Preliminar	
Fase 1.- Planificación de la Auditoría	❖ Revisión de documentación y análisis de activos/servicios IT. ❖ Elaboración del Programa de Auditoría. ❖ Planificación de las Entrevistas	☑ Plan de Auditoría
Fase 2.- Trabajo de Campo	❖ Entrevistas con los diferentes Dptos. de Sistemas de Información.	
Fase 3.- Informe de Auditoría	❖ Redacción de Informe de Auditoría ❖ Revisión del borrador con Área SS.II.	☑ Borrador de Informe de Auditoría
Fase 4.- Presentación de resultados	❖ Cierre del Informe Final de Auditoría. ❖ Elaboración del Resumen Ejecutivo. ❖ Presentación de Resultados.	☑ Informe Final Auditoría ☑ Resumen Ejecutivo

2.3 Pre-auditoría de Certificación del SGSI

Sistema de Gestión de la Seguridad de la Información (SGSI)

INTRODUCCIÓN

La pre-auditoría de Certificación del SGSI tiene por objetivo minimizar la aparición de no conformidades durante la realización de la auditoría de certificación que se lleve a cabo por una empresa certificadora (AENOR o APPLUS).

La auditoría se realizará siguiendo las siguientes etapas:

- **Auditoría Documental.** Etapa en la que se revisará la documentación propia del SGSI y se preparará la etapa II de la simulación de la auditoría de certificación del SGSI.
- **Auditoría In-Situ.** Etapa en la que se realizarán todas las pruebas de trabajo de campo incluidas dentro del programa de auditoría definido previamente, de forma que se obtenga una garantía suficiente de que se ha implantado correctamente el SGSI.

MARCO METODOLÓGICO

- ☑ ISO 27001. Permite certificar (especifica requisitos), por entidad acreditada para ello, el Sistema de Gestión de Seguridad de la Información. Basado como otros en el ciclo PDCA.
- ☑ ISO 27002. **Código de buenas prácticas para la Gestión de Seguridad de la Información.**

METODOLOGÍA

2.3 Pre-auditoría de Certificación del SGSI

Sistema de Gestión de la Seguridad de la Información (SGSI)

ACTIVIDADES A REALIZAR

Auditoría Documental

Objeto: Identificar el estado de la organización y su SGSI frente a la Auditoría de Certificación del SGSI.

Actividades relevantes:

- Revisión del ámbito, alcance y enfoque el SGSI, analizando:
    1. Ámbito y alcance del SGSI.
    2. Proceso de Selección de Controles
    3. Proceso de implantación de controles.
    4. Declaración de Selección de Controles.
- Conocer las áreas de la organización implicadas en la implantación y éxito del SGSI.
- Recopilar el resto de la documentación del SGSI disponible, respecto a:
    1. Política de Seguridad.
    2. Análisis de Riesgos.
    3. Gestión de Riesgos:
    4. Implantación de procesos SGSI y controles definidos.
- Elaboración y Presentación del Informe de Auditoría Documental. Incluirá una propuesta de detener o proseguir con la auditoría in-situ, con las siguientes consideraciones:
- No conformidades mayores: se detiene el proceso de auditoría, y se recomienda la solución de los problemas con una propuesta de solución en un plazo determinado se vuelve a realizar la primera etapa.
- No conformidades menores: se solicita la rectificación con la propuesta de resolución y en un breve plazo se revisa de nuevo la documentación.
- Observaciones: se realizan las observaciones a modo de recomendación.

Sistema de Gestión de la Seguridad de la Información (SGSI)

ACTIVIDADES A REALIZAR

Auditoría In-situ

Objeto: Comprobar la eficacia del SGSI.

Actividades relevantes:

• Trabajo de Campo

Se ejecutará el programa de auditoría elaborado en la etapa anterior, con el objeto de obtener las evidencias suficientes que permita detectar las salvedades que podrían presentarse en un proceso de Certificación del SGSI.

Se verificará el grado de:

- Alcance del SGSI en la práctica, y de sus objetivos de seguridad.
- Divulgación de las Políticas de Seguridad y procedimientos asociados.
- Consolidación de la organización de seguridad
- Implantación de los procedimientos asociados al SGSI, y correspondientes al ciclo PDCA.
- Corrección del inventario de activos, del Análisis de Riesgos y posterior Gestión de Riesgos, realizado previo a la selección de controles.
- Implantación de los controles seleccionados (asociados a la ISO/IEC 27002). Se realizará un muestreo de áreas de bajo, medio y alto riesgo.
- Efectividad de los Indicadores establecidos.
- Efectividad de la mejora progresiva dentro del ciclo PDCA.
- Elaboración y Presentación de Resultados

2.4 Auditoría de Seguridad de Servicios Web

INTRODUCCIÓN

Las organizaciones son conscientes del **riesgo creciente de brechas de seguridad** en sus redes:

1. Las redes tienen múltiples puntos de entrada.
2. Las redes han crecido de manera muy compleja y su administración es más complicada.
3. Las herramientas de hacking se han automatizado y requieren de menos conocimientos para su uso, aumentando el número de hackers, y siendo los ataques mayores y más dañinos.
4. El número de vulnerabilidades que pueden ser explotadas está en aumento.
5. La reducción de los ciclos de vida de desarrollo de software han resultado en productos de baja calidad, lo cual expone a los usuarios a mayores riesgos y vulnerabilidades ocultas.

Análisis de Vulnerabilidades: Búsqueda de vulnerabilidades (puertos abiertos, parches de seguridad, etc.), que incluye verificaciones manuales de falsos positivos, identificación de los puntos débiles de la red, y emisión de recomendaciones para solventarlos.

Test de Intrusión: proyectos orientados a objetivos en los cuales dicho objetivo es obtener un trofeo, que incluye ganar acceso privilegiado.

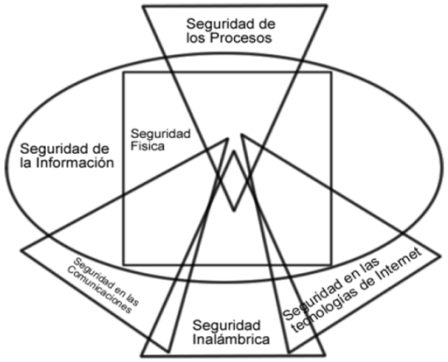
MARCO METODOLÓGICO

- ☑ **OSSTMM 2.1** – Manual de Metodología Abierta de Testeo de Seguridad del Institute for Security and Open Methodologies, método aceptado para ejecutar un test de seguridad minucioso y de una forma ordenada.
- ☑ **OWASP.** Metodología para garantizar la seguridad en aplicaciones web abiertas al exterior.

2.4 Auditoría de Seguridad de Servicios Web

METODOLOGÍA OSSTMM

La calidad del resultado de un test de seguridad es difícil de juzgar sin una metodología estándar. Es importante definir el modo correcto de testear, basándose en las mejores prácticas en la materia.



El **Manual de la Metodología Abierta de Comprobación de la Seguridad** (**OSSTMM**, Open Source Security Testing Methodology Manual) es uno de los estándares profesionales más completos y comúnmente utilizados en Auditorías de Seguridad desde Internet. Incluye un marco de trabajo que describe las fases que habría que realizar para la ejecución de la auditoría. Se ha logrado gracias a un consenso entre más de 150 expertos internacionales sobre el tema, que colaboran entre sí mediante Internet.

Valores de la Evaluación de Riesgo (RAV): Los RAV realzarán estas instantáneas agregando dimensiones de frecuencia a los tests de seguridad.

Plantillas: Reflejan qué módulos y tareas han sido testeados hasta su conclusión, cuáles no han sido testeados y su justificación, indicando aquellos test no aplicables.

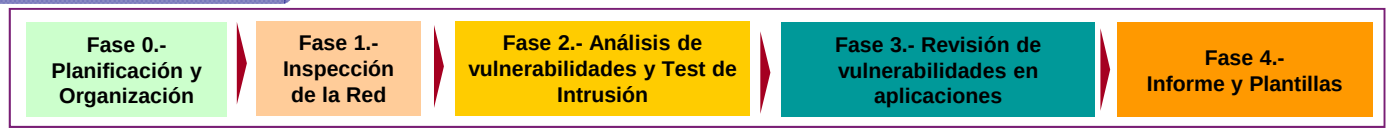
2.4 Auditoría de Seguridad de Servicios Web

ACTIVIDADES A REALIZAR

Objetivos principales a cubrir en el proyecto:

- ☑ **Inspección de la red** desde el exterior, a partir del nombre del dominio Internet a analizar.
- ☑ Realizar un **Análisis de Vulnerabilidades y Test de Intrusión**, siguiendo el modelo de "Caja Negra" donde no se proporciona información alguna del sistema a revisar
- ☑ Cumplimentación de las **Plantillas** incluidas en la metodología y que sean aplicables a las secciones incluidas en la Auditoría.
- ☑ **Documentación de datos que se han generado en las pruebas**, describiendo las pruebas realizadas y los resultados obtenidos.
- ☑ Establecer una colección de **Recomendaciones** tendentes a eliminar las deficiencias identificadas.

METODOLOGÍA



2.5 Adecuación del Plan de Continuidad

Una empresa que deja de operar dos semanas, probablemente quedará fuera de mercado…

INTRODUCCIÓN

Normalmente, durante la interrupción imprevista de la actividad de una organización, se generan pérdidas financieras, sin embargo, el impacto más significativo es normalmente la pérdida de imagen corporativa que resulta de un incidente mal gestionado. Por el contrario, un incidente bien gestionado puede realzar la imagen de una organización.

La GCN (Gestión de Continuidad del Negocio) debe desarrollarse en la organización tanto verticalmente (niveles estratégico, táctico y operativo), como horizontalmente (en todas sus sedes y su cadena de valor, incluyendo la propia cadena de suministro), de cara a garantizar que el plan contemplará los riesgos reales del negocio.

MARCO METODOLÓGICO

El **BS-25999** es un estándar británico que establece **mejores prácticas, recomendaciones y actividades específicas para lograr la continuidad de negocio** teniendo en cuenta los riesgos a los que se enfrenta una organización.

- ☑ **Parte 1: Buenas prácticas para la implementación de un Plan de Continuidad.**
- ☑ **Parte 2: Definición del Plan de Continuidad.**

Metodología: ISO 27002:2005. Código de buenas prácticas para la gestión de la Seguridad de la Información

MAZARS

2.5 Adecuación del Plan de Continuidad

MARCO METODOLÓGICO

10. Gestión de la continuidad del negocio

- **Aspectos de la seguridad de la información de la gestión de la continuidad del negocio**
  - Incluir la seguridad de la información en el proceso de gestión de continuidad del negocio
  - Continuidad del negocio y evaluación del riesgo
  - Desarrollar e implementar los planes de continuidad incluyendo la seguridad de la información
  - Marco Referencial de la planeación de la continuidad del negocio
  - Prueba, mantenimiento y re-evaluación de los planes de continuidad del negocio

2.5 Adecuación del Plan de Continuidad

ACTIVIDADES A REALIZAR

La auditoría verificará si se han cubierto las siguientes fases y requerimientos, el contenido de los documentos resultantes del Plan de Continuidad, y los riesgos derivados de las salvedades que se detecten:

- Entendimiento del negocio. Identificar procesos y sus actividades y funciones críticas. Identificar sus dependencias clave externas e internas. Identificar influencias externas y posibles impactos en estos procesos.
- Análisis de impacto en el negocio (BIA). Tiene que tener en cuenta el tiempo entre el punto de interrupción, y el punto en el cual los sistemas sensibles en el tiempo deben estar funcionando nuevamente.
- Elección de la estrategia.
- Planes de emergencia: gestión de la fase inicial de un incidente.
- Planes de continuidad del negocio: mantener el funcionamiento de los procesos de negocio.
- Planes de recuperación del negocio: recuperar el estado inicial.
- Plan de pruebas e informes relacionados
- Contratos y acuerdos de nivel de servicio
- Plan de formación para las partes implicadas .
- Revisión periódica del plan.

PCI DSS - Norma de Seguridad de Datos de la Industria de Tarjetas de Pago

INTRODUCCIÓN

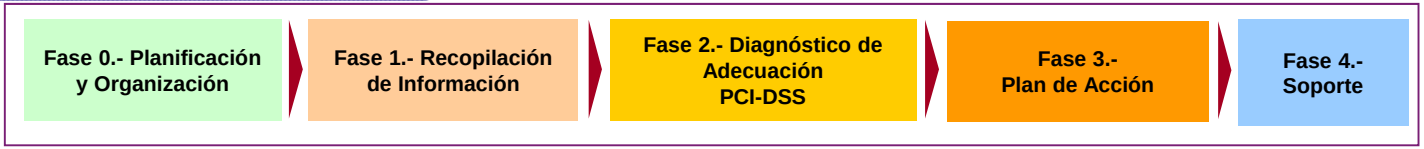
"PCI Security Standards Council", formado por las principales entidades de tarjetas de crédito, creó la Norma de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) con el objetivo de fomentar y mejorar la seguridad de los datos del titular de la tarjeta de crédito.

Debe cumplir los requerimientos que establece PCI DSS cualquier entidad que participe en el procesamiento, transmisión o almacenamiento de información de tarjetas de crédito.

ACTIVIDADES A REALIZAR

- ☑ Identificar donde se transmite, procesa o almacena información de tarjetas de crédito y definir el entorno que debe ser protegido para cumplir con la Norma.
- ☑ Elaborar un **diagnóstico** para conocer el grado de adecuación de la organización a los 12 requerimientos de la Norma.
- ☑ Elaboración de un **Informe de Conclusiones y un Plan de Acción** para solventar las deficiencias detectadas.
- ☑ Soporte en la elaboración de los procedimientos técnicos y organizativos que exige la Norma.

METODOLOGÍA



PCI DSS - Norma de Seguridad de Datos de la Industria de Tarjetas de Pago

MARCO METODOLÓGICO

PCI DSS – Norma de Seguridad de Datos de la Industria de Tarjetas de Pago

A continuación se muestra una descripción general de los 12 requerimientos del PCI DSS:

Cree y Mantenga una Red Segura:

1. Proteja los datos con un Firewall cuya configuración se mantenga correctamente.
2. Nunca utilice valores por defecto en contraseñas y parámetros de seguridad.

Proteja los datos de los titulares de tarjetas:

3. Proteja los datos del titular almacenados.
4. Cifre las transmisiones de información sensible como datos de los titulares en Redes Públicas.

Mantenga un Programa de Gestión de Vulnerabilidades:

5. Utilice un anti-virus permanentemente actualizado.
6. Desarrolle y mantenga sistemas y aplicaciones seguras.

Despliegue Medidas de Control de Acceso Robustas:

7. Restrinja el acceso a los datos a quienes lo tengan atribuido por su actividad.
8. Asigne identificadores únicos a cada persona que disponga de acceso informático.
9. Restrinja el acceso físico a los datos de los titulares.

Monitorice y Compruebe las Redes regularmente:

10. Registre y monitorice cualquier acceso a recursos de red y a datos de titulares.
11. Compruebe regularmente los sistemas y los procesos de seguridad.

Mantenga una Política de Seguridad de la Información:

12. Mantenga una política que contemple la seguridad de la información.

Nuestros servicios de Gestión de Riesgos Tecnológicos

1. Cumplimiento legal (pág. 30)

- Adecuación a la LOPD (Ley Orgánica de Protección de Datos de Carácter Personal)
- Auditoría bienal LOPD
- Adecuación a la LSSICE y LISI, de Impulso de la Sociedad de la Información y Comercio Electrónico
- Peritaje Informático
- Auditoría de Software Legal

2. Seguridad de la Información (pág. 40)

- Implantación del Sistema de Gestión de la Seguridad de la Información (SGSI)
- Auditoría de Buenas Prácticas de Seguridad (ISO 27002)
- Pre-auditoría de Certificación del SGSI
- Auditoría de Seguridad de Servicios Web
- Adecuación del Plan de Continuidad
- Seguridad en Tarjetas de Crédito (PCI DSS)

3. Control de Servicios Externalizados (pág. 58)

- **Auditoría de Calidad de los Servicios Tecnológicos externalizados**
- **Asesoramiento en contratos de Servicios Tecnológicos en proceso de externalización**

4. Governance IT (pág. 61)

- Asesoramiento en la implantación de CobiT
- Due-diligence de los Sistemas de Información
- Formación a medida

5. Soporte a Auditoría/Control Interno (pág. 65)

- Herramientas de Análisis de Datos. Forensic
- Análisis CCI-99 del Libro Diario
- Implantación de Proaudit Advisor como soporte al Control Interno

Revisión de la calidad de los servicios IT proporcionados

INTRODUCCIÓN

La presión por reducir costes y concentrarse en las actividades del negocio de mayor valor añadido ha obligado a las empresas a buscar soluciones para alcanzar este objetivo, manteniendo sus niveles de servicio. Una de las soluciones, pasa por externalizar los servicios de IT.

Es conveniente tener indicadores fiables sobre el nivel de desempeño y cumplimiento contractual del suministrador de los servicios externalizados, y una forma de obtenerlos es mediante una auditoría.

MARCO LEGAL

☑ El contrato establecido entre la organización y el suministrador de servicios IT.

ACTIVIDADES A REALIZAR

☑ **Planificación de la Auditoría**
- Comunicación de Inicio y Plan de Auditoría al auditado.
- Preparación de Auditoría. Obtener y revisar la documentación aportada.

☑ **Revisión in-situ.** Obtener evidencias de la conformidad de las actividades de suministrador respecto con los documentos contractuales y planes de calidad e infraestructuras definidos.

☑ **Elaboración y revisión del Informe Preliminar**
- Elaboración del borrador de Informe Preliminar a partir de las actas y de las evidencias obtenidas, en base a los criterios definidos.
- Solventar las dudas que pudiera presentar el Informe de Auditoría.
- Revisar el informe con las áreas técnicas de la organización, y presentarlo al auditado.

☑ **Cierre del Informe Final**, tras la revisión de las alegaciones presentadas y entrega de documentación

Soporte en la redacción de contratos para la externalización de Servicios IT

INTRODUCCIÓN

El establecimiento de una relación de outsourcing exige de unos mecanismos de contratación que aseguren la correcta prestación del servicio y de una perfecta coordinación entre comprador y proveedor.

El contrato de outsourcing debe recoger entre otros aspectos, los siguientes:

- ✓ Descripción de los productos a recibir, los niveles de servicio a mantener, y penalizaciones si no se alcanzan.
- ✓ Responsabilidades y elementos de relación para gestionar el proceso.
- ✓ Procedimientos para someter a continua revisión el contenido y alcance de las actividades objeto del contrato.
- ✓ Mecanismos que aseguren la continuidad del servicio en caso de rescisión.

MARCO METODOLÓGICO

- ☑ **ISO 27002.** Buenas prácticas para la gestión de la Seguridad de la Información
- ☑ **Cobit v4 –** Marco de control de la Gestión de los Sistemas de Información

ACTIVIDADES A REALIZAR

- ☑ Definición de los servicios IT a subcontratar y el modelo de outsourcing elegido.
- ☑ Análisis de las mejoras que aportará la subcontratación de servicios IT, e identificación de riesgos.
- ☑ Definición de Acuerdos de Nivel de Servicios (ANS) y penalizaciones.
- ☑ Definición del Plan de Retorno, y los motivos de cancelación del contrato.
- ☑ Definición de un cuadro de mando que aporte información clara e inmediata para la toma de decisiones.
- ☑ Posibilidad de auditar al suministrador y características de las mismas (interna, externa, etc.)
- ☑ Cláusulas de adecuación legal.

Nuestros servicios de Gestión de Riesgos Tecnológicos

1. Cumplimiento legal (pág. 30)

- Adecuación a la LOPD (Ley Orgánica de Protección de Datos de Carácter Personal)
- Auditoría bienal LOPD
- Adecuación a la LSSICE y LISI, de Impulso de la Sociedad de la Información y Comercio Electrónico
- Peritaje Informático
- Auditoría de Software Legal

2. Seguridad de la Información (pág. 40)

- Implantación del Sistema de Gestión de la Seguridad de la Información (SGSI)
- Auditoría de Buenas Prácticas de Seguridad (ISO 27002)
- Pre-auditoría de Certificación del SGSI
- Auditoría de Seguridad de Servicios Web
- Adecuación del Plan de Continuidad
- Seguridad en Tarjetas de Crédito (PCI DSS)

3. Control de Servicios Externalizados (pág. 58)

- Auditoría de Calidad de los Servicios Tecnológicos externalizados
- Asesoramiento en contratos de Servicios Tecnológicos en proceso de externalización

4. Governance IT (pág. 61)

- **Asesoramiento en la implantación de CobiT**
- **Due-diligence de los Sistemas de Información**
- **Formación a medida**

5. Soporte a Auditoría/Control Interno (pág. 65)

- Herramientas de Análisis de Datos. Forensic
- Análisis CCI-99 del Libro Diario
- Implantación de Proaudit Advisor como soporte al Control Interno

4.1 Asesoramiento en la implantación de CobiT

Soporte en la redacción de contratos para la externalización de Servicios IT

INTRODUCCIÓN

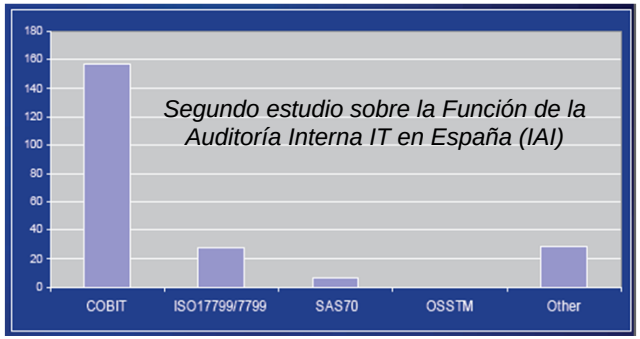
Las organizaciones necesitan demostrar niveles cada vez mayores de seguridad y control. CobiT permite implantar una política clara y el desarrollo de buenas prácticas para el control de la TI en las organizaciones. Así, CobiT se ha diseñado para ser la herramienta de la dirección de las TI, que ayude a la comprensión y gestión de los riesgos y beneficios asociados con la información y las tecnologías relacionadas.

ACTIVIDADES A REALIZAR

- ☑ Presentación de CobiT al personal clave.
- ☑ Delimitación del Alcance del proyecto
- ☑ Análisis de Riesgos
- ☑ Análisis del nivel de madurez de la Organización respecto a los diferentes procesos de CobiT.
- ☑ Declaración de Aplicabilidad
- ☑ Definición de la Política, Normativa y Procedimientos.
- ☑ Implantación de CobiT. Oficina técnica y cuadro de mando.
- ☑ Elaboración del Plan Director.
- ☑ Gestión el cambio. Plan de Concienciación y Formación.
- ☑ Seguimiento de progreso de los planes de acción definidos.

MARCO METODOLÓGICO

- ☑ CobiT v.4 – Marco Metodológico para el Control de los Sistemas de Información. Publicado por la ISACA (Information Systems Audit and Control Association).



MAZARS

Auditoría de los Sistemas de Información, antes de la compra de una empresa

INTRODUCCIÓN

En el caso de Fusiones y Adquisiciones de empresas, la parte compradora necesita conocer al detalle el estado de situación informática de la empresa a adquirir. La función básica de la auditoría de compra o "due diligence", es valorar los activos y analizar los riesgos de la compañía objetivo, investigando los aspectos significativos.

ACTIVIDADES A REALIZAR

El proceso de auditoría de compra es similar a cualquier proceso de auditoría.

El alcance del proyecto, abarca los siguientes aspectos:

- ☑ **Estrategia** (Estrategias comerciales e informáticas y coordinación de las dos)
- ☑ **Finanzas** (Presupuestos de informática, gestión de activos, control financiero)
- ☑ **Personal** (Organización de informática, competencias y necesidades principales)
- ☑ **Tecnología** (Entorno de sistemas e infraestructura informática, inventario de activos tanto físicos, como lógicos)
- ☑ **Procesos** (Procesos de gestión de informática y procedimientos asociados)
- ☑ **Seguridad** (Integridad, confidencialidad, disponibilidad y control de acceso)
- ☑ **Colaboradores** (Contratos de proveedores, contratos de servicio, soporte y mantenimiento, licencias de software, etc.)
- ☑ **Reglamentación** (Conformidad legal, propiedad intelectual, requerimientos propios del sector)

4.3 Formación a medida

Acciones de divulgación y concienciación, metodologías de gestión IT,…

INTRODUCCIÓN

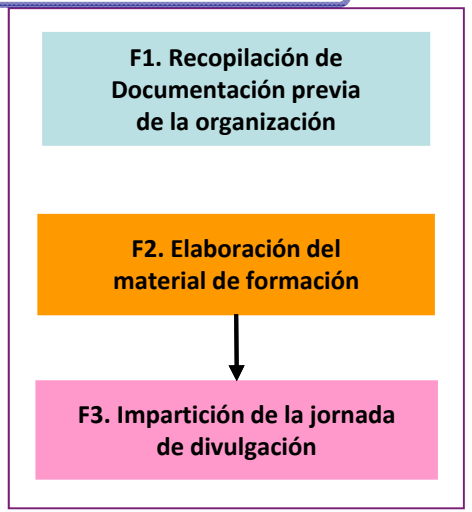
Que el personal esté formado y concienciado en materia de seguridad, es un aspecto fundamental para que se reaccione cuanto antes frente a un incidente, y ante todo lo haga de una forma correcta.

En muchos casos, la formación externa tiene más efecto en el personal de la organización, principalmente cuando es impartida por personal experto en la materia.

ACTIVIDADES A REALIZAR

- ☑ Definir los aspectos en que se quiere hacer hincapié durante la sesión de formación.
- ☑ Recabar información referente a la Política y Normativa propia de la organización.
- ☑ Definir el horario definitivo de impartición de la formación, así como el número de sesiones y el público al que va dirigido (usuarios, staff, etc.).
- ☑ Elaboración de la presentación, de forma que resulte amena para los asistentes. Puede contener ejemplos de consecuencias e infracciones reales, de cara a que el usuario se vea reflejado.
- ☑ Envío del documento PPT para su aprobación previa a la impartición de la misma.
- ☑ Impartición de la/s jornada/s de formación.

METODOLOGÍA



Nuestros servicios de Gestión de Riesgos Tecnológicos

1. Cumplimiento legal (pág. 30)

- Adecuación a la LOPD (Ley Orgánica de Protección de Datos de Carácter Personal)
- Auditoría bienal LOPD
- Adecuación a la LSSICE y LISI, de Impulso de la Sociedad de la Información y Comercio Electrónico
- Peritaje Informático
- Auditoría de Software Legal

2. Seguridad de la Información (pág. 40)

- Implantación del Sistema de Gestión de la Seguridad de la Información (SGSI)
- Auditoría de Buenas Prácticas de Seguridad (ISO 27002)
- Pre-auditoría de Certificación del SGSI
- Auditoría de Seguridad de Servicios Web
- Adecuación del Plan de Continuidad
- Seguridad en Tarjetas de Crédito (PCI DSS)

3. Control de Servicios Externalizados (pág. 58)

- Auditoría de Calidad de los Servicios Tecnológicos externalizados
- Asesoramiento en contratos de Servicios Tecnológicos en proceso de externalización

4. Governance IT (pág. 61)

- Asesoramiento en la implantación de CobiT
- Due-diligence de los Sistemas de Información
- Formación a medida

5. Soporte a Auditoría/Control Interno (pág. 65)

- **Herramientas de Análisis de Datos. Forensic**
- **Análisis CCI-99 del Libro Diario**
- **Implantación de Proaudit Advisor como soporte al Control Interno**

ACL como soporte a la Auditoría Interna y al Análisis Forense Financiero

INTRODUCCIÓN

El éxito de la implantación de herramientas de ayuda a la auditoría, depende en gran medida del asesoramiento profesional previo, durante y después de la implantación.

Mazars utiliza ACL en sus proyectos internos de Auditoría y en los proyectos de Análisis Forense, por lo que dispone de una alta experiencia práctica en la herramienta.

ACL permite:

- Potencia, rapidez en el análisis de datos y fácil uso
- Capacidad de analizar volumen de datos infinitos
- Reportes de alta calidad y fiabilidad. Capacidades graficas muy elaboradas
- Un fichero “LOG” siempre accesible
- Tratamiento multi-fichero y capacidad de automatización potente..

ACTIVIDADES A REALIZAR

- ☑ Definición de revisiones periódicas a realizar en el departamento de Auditoría Interna.
- ☑ Análisis de las fuentes externas que habría que importar, a partir de los sistemas y bases de datos existentes en la organización.
- ☑ Parametrización y programación de rutinas en ACL, para cubrir las necesidades de análisis e investigación definidas.
- ☑ Implantación de ACL en un servidor de la organización y en los diferentes equipos de los usuarios de ACL.
- ☑ Definición de la metodología de Auditoría Interna y procedimientos relacionados con ACL.
- ☑ Formación del personal auditor en ACL y en las rutinas desarrolladas.
- ☑ Seguimiento y asesoramiento.

Herramienta y Metodología de Análisis de Datos del Libro Diario

INTRODUCCIÓN

El Análisis de Datos es una técnica de auditoría asistida por ordenador, que **permite detectar anomalías en los datos de un sistema de información**, provocadas por un usuario o por un programa informático.
La herramienta CCI-99 facilita una **primera valoración del nivel de control interno a partir del Libro Diario y permite identificar la existencia de riesgo**, aplicando controles automáticos que permitan detectar posibles operaciones anormales.

ACTIVIDADES A REALIZAR

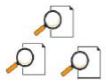
MAZARS ha desarrollado una serie de test de cara a detectar anomalías en los datos de libro diario, principalmente:

- **Controles de Frecuencia:** cuentas poco utilizadas, usuarios con un número bajo de entradas.
- **Controles de Patrones Numéricos:** cifras redondas, análisis de benford, importes repetidos
- **Controles de Materialidad:** entradas mayores por cada cuenta, volumen por usuario y cuentas.
- **Controles de Horario:** transacciones en fines de semana, o fuera del período de cierre.
- **Controles de Descripción:** en blanco o con textos inusuales o que pueden dar indicios de error.

METODOLOGÍA

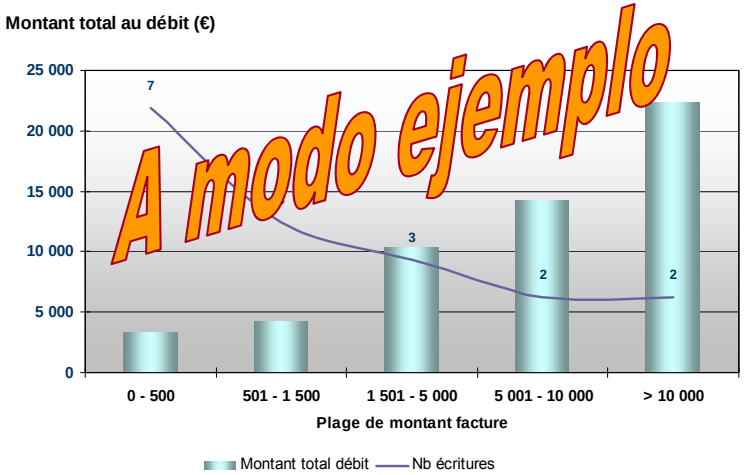
Fase 1.- Extracción de Datos → **Fase 2.- Análisis de Datos** → **Fase 3.- Investigaciones complementarias** → **Fase 3.- Conclusiones**






Herramienta y Metodología de Análisis de Datos del Libro Diario

Analyse des doublons d'écritures



Analyse par fournisseur

Code fournisseur	Reference facture fournisseur	Montant unitaire	Nb de doublons	Soldes doublons
TK4SDDGF	3050801376	11 200	2	22 400
F45LDKLG3	4324-46	6 455	2	12 910
GH4TGG4G/B	ZF4563-12S	1 643	3	4 929
EMPACIX	23464R	1 318	2	2 635
R0703419/M	BAP2508/GF	1 005	2	2 009
EH43F4	119956	335	2	670
LG53504RF/R	546743/RYT	34	2	68
....	....	....	....	....

Erreurs et fraudes détectées

Nº pièce	Comptes débit	Comptes crédit	Montant Débit	Journal	Libellé journal	Date de pièce	Date comptable	Date de saisie	Heure de saisie	Code user	Nom Prénom	Référence	Code fournisseur
1000005497	44561 - 60201	40100	11 200,08	KR	Vendor invoice	29/04/2008	22/05/2008	22/05/2008	09:36:24	LAMBERTC	Carole Lambert	3050801376	TK4SDDGF
1000005785	44561 - 60201	40100	11 200,08	KR	Vendor invoice	29/04/2008	22/05/2008	22/05/2008	10:18:55	LAMBERTC	Carole Lambert	3050801376	TK4SDDGF
1000010194	67200	40100	1 004,64	KR	Vendor invoice	25/08/2008	03/09/2008	03/09/2008	12:56:07	MACEP	Pierre Macé	BAP2508/GF	R0703419/M
1000048619	67200	40100	1 004,64	ODF	OD Fact FRS	25/08/2008	24/10/2008	27/10/2008	10:02:57	MACEP	Pierre Macé	BAP2508/GF	R0703419/M
1000005226	44569 - 62260	40100	334,88	KR	Vendor invoice	15/01/2008	15/05/2008	15/05/2008	09:49:10	ARMANDL	Lucie Armand	119956	EH43F4
1000009971	44569 - 62260	40100	334,88	RE	Invoice gross	15/01/2008	15/05/2008	20/05/2008	12:22:51	DOUSSETJ	Julien Dousset	119956	EH43F4
....	....	....	....	....	....	....	....	....	....	....	....	....	....
....	....	....	....	....	....	....	....	....	....	....	....	....	....

5.3 Herramienta Proaudit Advisor de Methodware

Implantación de Proaudit Advisor como soporte al Control Interno

INTRODUCCIÓN

PRo Audit Advisor facilita la realización de las auditorías internas y agiliza la generación de informes y la presentación gráfica de los resultados, siguiendo las mejores prácticas internacionales.

Características:

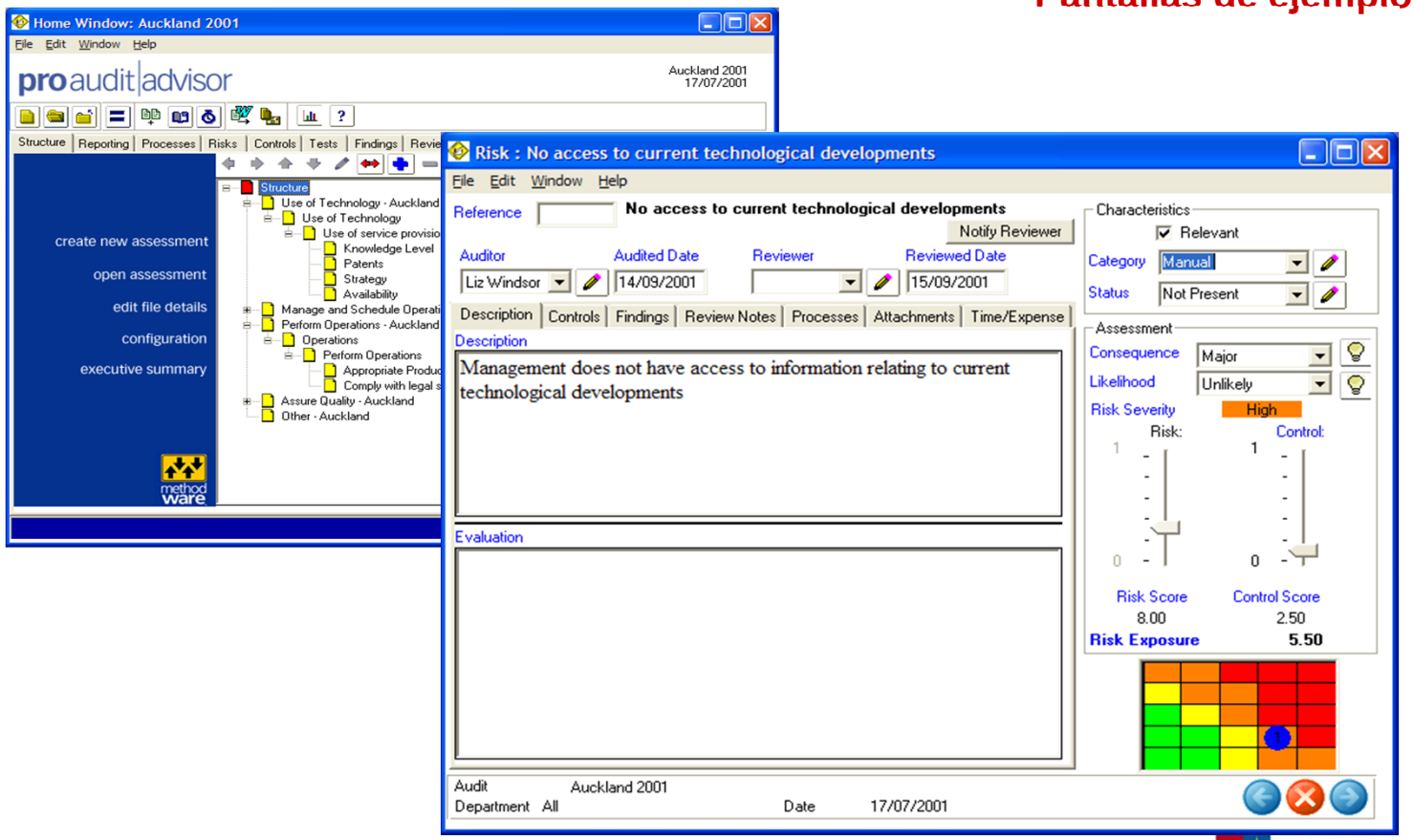
- Mejora la evaluación de riesgos basada en procesos a través de la evaluación de riesgos y controles.
- Incluye la estructura de COSO con 10 megaprocesos y los riesgos y controles predefinidos.
- Facilidades para la realización de auditorias en múltiples localizaciones. Auditorías multi-usuarios.
- Administración de las observaciones y recomendaciones de auditoría en una única base de datos.
- Habilidad de vincular documentos externos.
- Informes de auditoría de alta calidad. Representación visual del Mapa de Riesgos.

ACTIVIDADES A REALIZAR

- ☑ Presentación de la herramienta al personal involucrado. Designación de un interlocutor por parte de la organización, para ir definiendo las diferentes opciones parametrizables de la herramienta.
- ☑ Definición de las diferentes opciones de parametrización de la herramienta, e implementación.
- ☑ Definición de procesos, riesgos y controles de la organización, e introducción en ProAudit Advisor.
- ☑ Definición y alta de usuarios con los roles correspondientes.
- ☑ Definición del Plan de Auditoría sobre los Procesos.
- ☑ Formación de los propietarios de los procesos.
- ☑ Formación de los Auditores.
- ☑ Seguimiento y asesoramiento.

5.3 Herramienta Proaudit Advisor de Methodware

Pantallas de ejemplo



MAZARS

MAZARS

Alicante

Pintor Cabrera, 22

03003 Alicante

Tel: 965 926 253

Barcelona

c/Aragó, 271

08007 Barcelona

Tel: 93 405 08 55

Bilbao

C/ Rodríguez Arias, 23

48011 Bilbao

Tel: 94 470 25 71

Madrid

C/ Claudio Coello, 124

28006 Madrid

Tel : 91 562 26 70

Málaga

Pirandello, 6

29010 Málaga

Tel: 952 070 889

Valencia

Colón, 1

46004 Valencia

Tel: 963 509 212

Vigo

Plaza de Compostela 17

36201 Vigo

Tel: 986 441 920

www.mazars.es

Praxity MEMBER GLOBAL ALLIANCE OF INDEPENDENT FIRMS