La Auditoría Interna en los Sistemas de Información

Los Desayunos de Mazars:

AUDITORÍA INTERNA INFORMÁTICA

Principales problemas a los que se enfrenta la Auditoría Interna

Barcelona, 2 de diciembre de 2009

MAZARS

La Auditoría Interna en los Sistemas de Información

"Los Desayunos de Mazars"

MAZARS

« Los Desayunos de Mazars »: Objetivos

- **Mazars** pone 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 como 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

Desarrollo de la sesión

Agenda

- **9:00** Café
- **9:30** Intervenciones e intercambio de opiniones sobre «Principales problemas de la Auditoría Interna de Sistemas de Información»
- **10:30** Pausa Café
- **11:00** Ejemplo de Auditoría de Seguridad.
- **11:30** Conclusiones y preguntas

Desarrollo de la sesión

Exposiciones

- **Mazars, una organización integrada**
- **Principales problemas de la Auditoría Interna de Sistemas de Información**

✓ ¿Porqué Auditoría Informática dentro de Auditoría Interna? ¿Quién hace qué?

✓ La estructura del Área de Sistemas. Diferentes modelos.

✓ Marcos normativos y Estándares. No inventar la rueda.

✓ ¿Contratar o subcontratar? El perfil del Auditor Informático.

✓ Un ejemplo de alcance de auditoría interna de seguridad

✓ Pautas para calcular los presupuestos anuales de Auditoría Informática

- **Una conclusión …**

… antes de abordar los temas de la próxima sesión.

La Auditoría Interna en los Sistemas de Información

Mazars, una organización internacional integrada

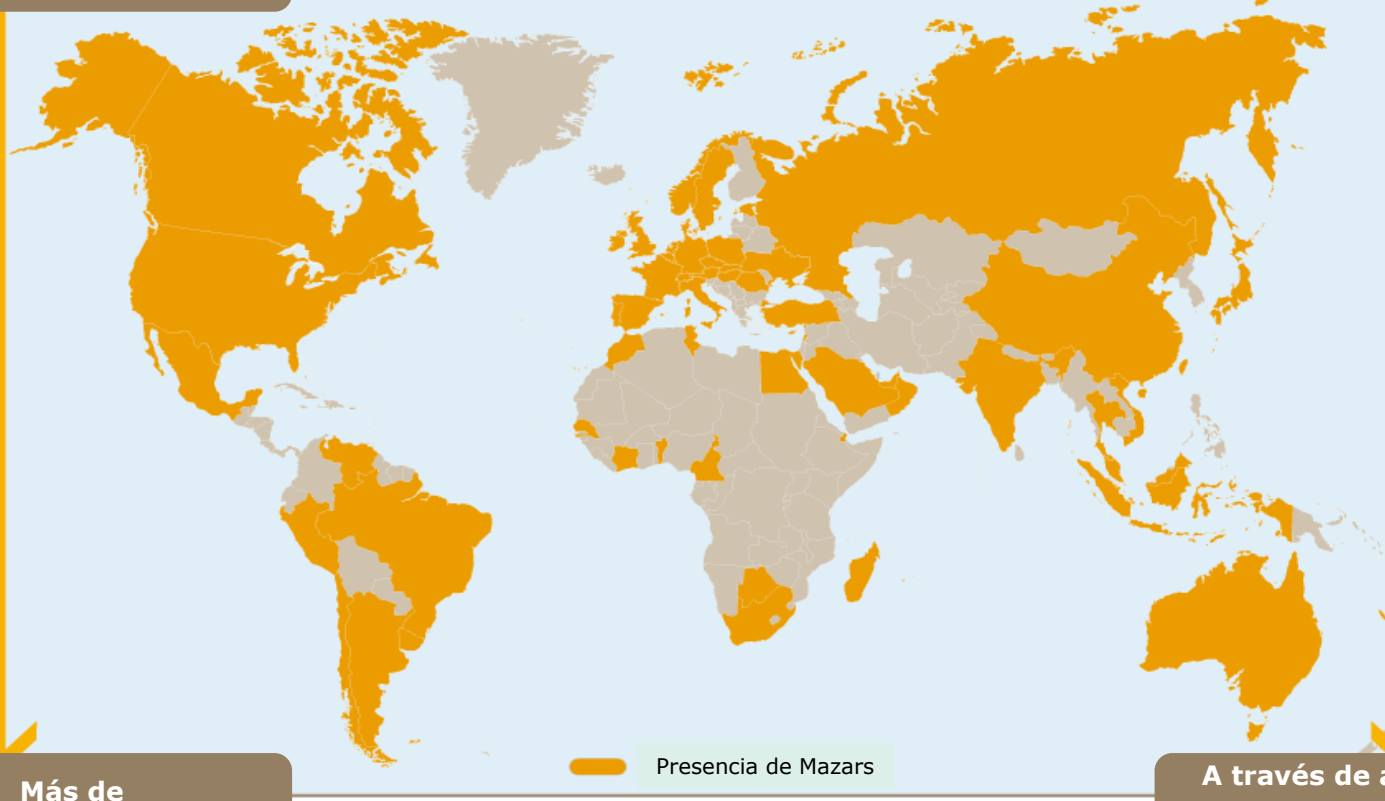
MAZARS

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 50 países

Capacidad de asistir a nuestros clientes en otros 22 países



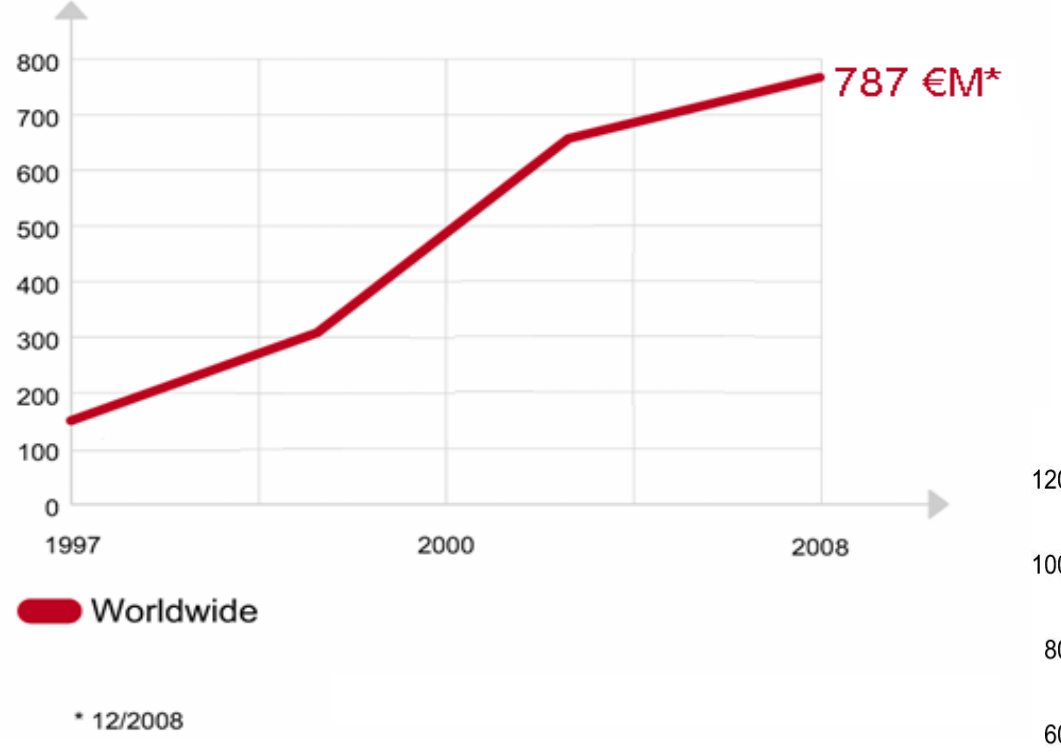
Más de 10.500 profesionales

A través de asociaciones con más de 14.000 profesionales

MAZARS

Una organización internacional integrada

… nuestra prioridad: la **calidad**

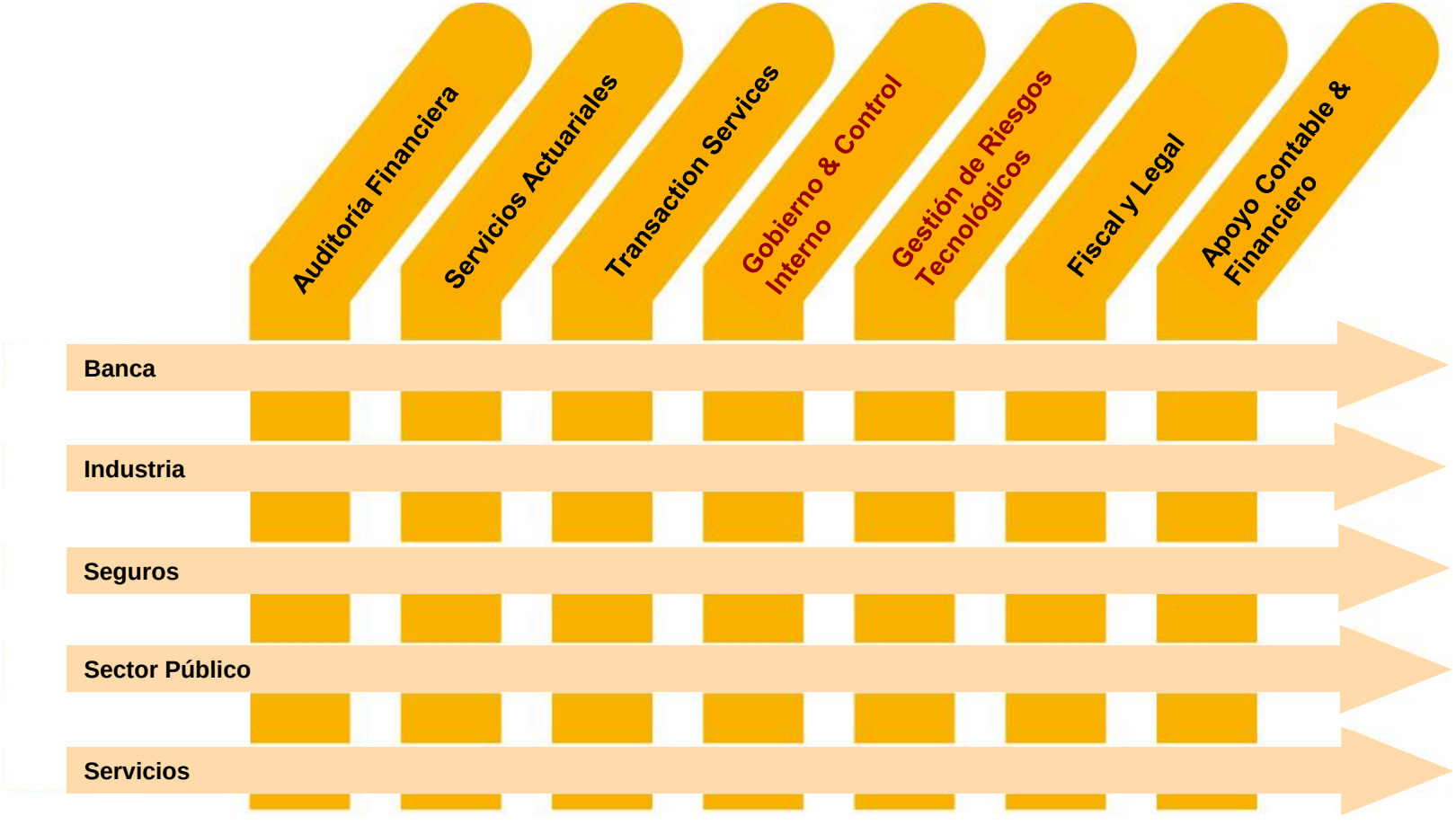


… para asegurar la **continuidad**

MAZARS

Organización matricial entre líneas de servicio y sectores de clientes

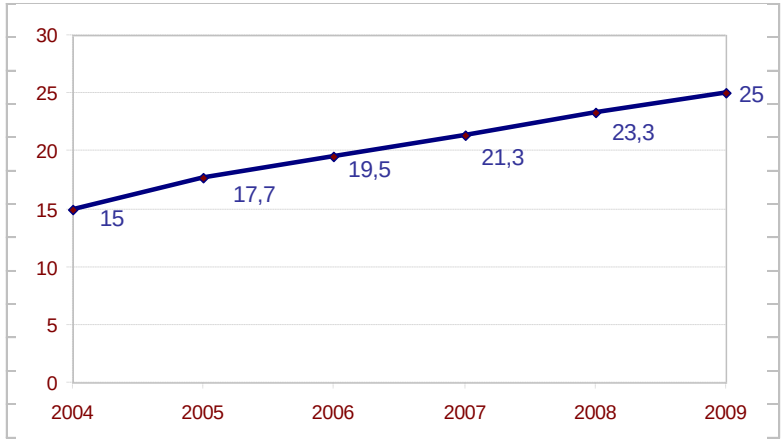
… para cumplir con las **necesidades** de nuestros **clientes**



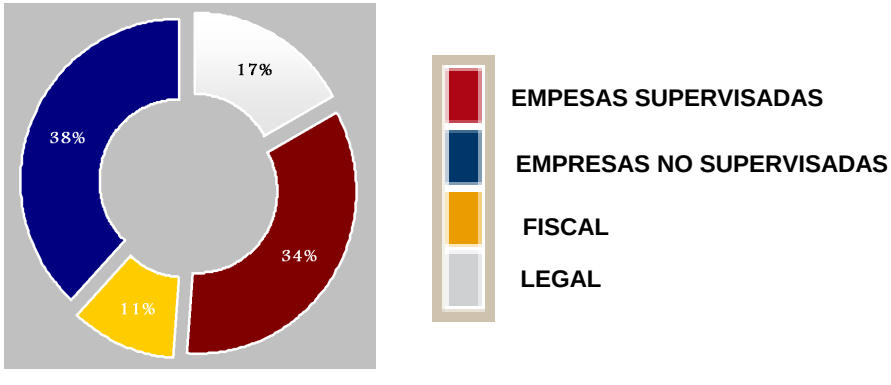
MAZARS

Mazars España en cifras

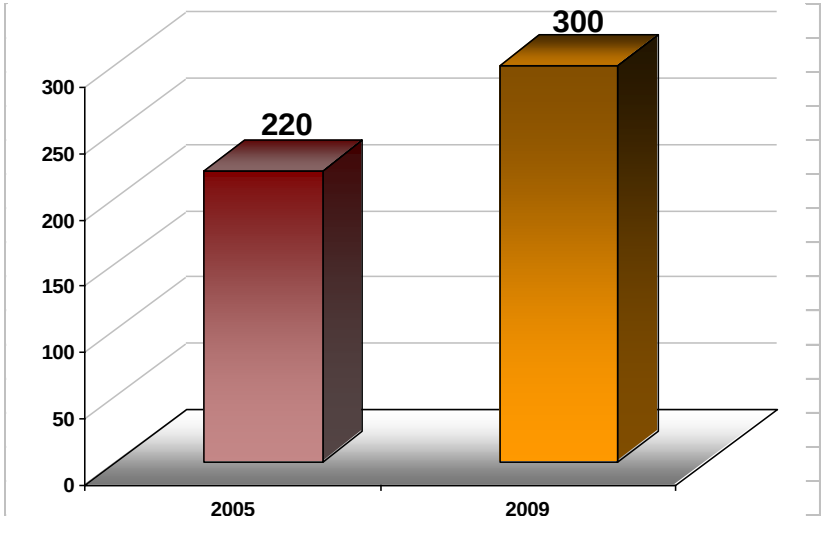
Evolución de la cifra de negocios (M€)



Cifra de negocios por ICL



Número de profesionales



MAZARS

La Auditoría Interna en los Sistemas de Información

¿Es realmente necesaria la Auditoría Informática Interna?

¿Quién audita qué?

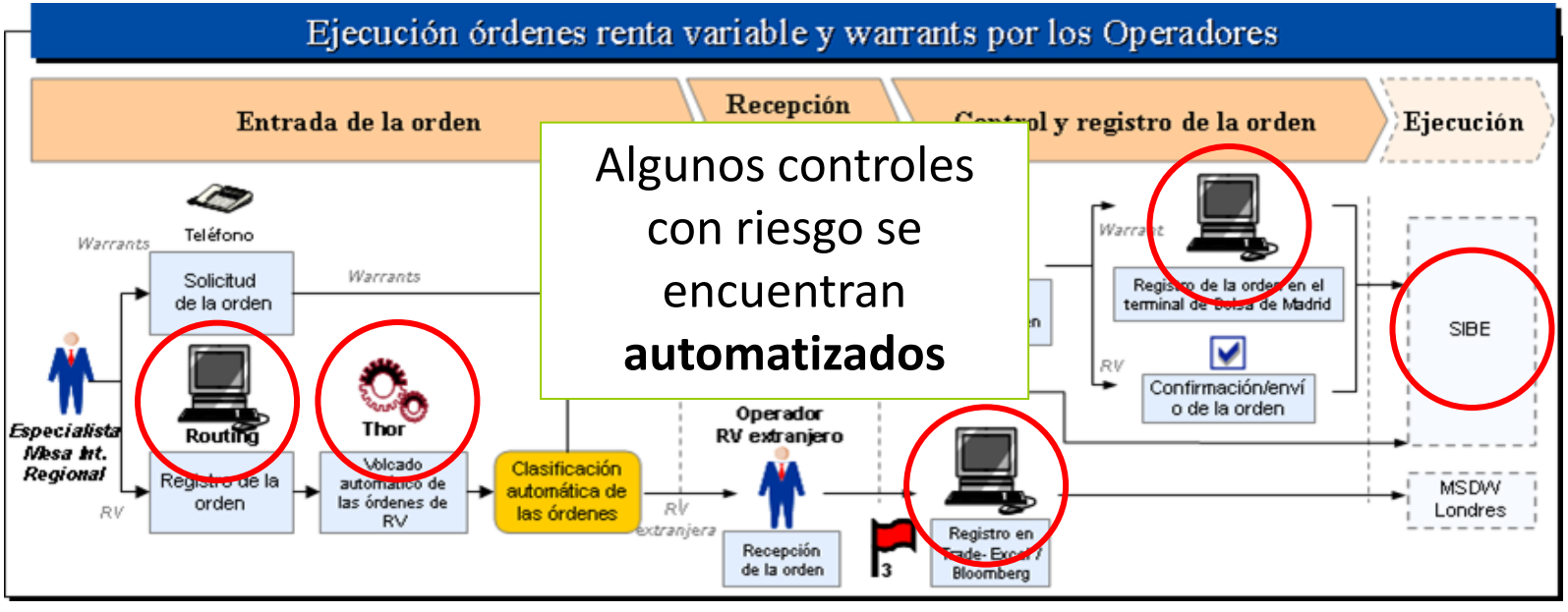
MAZARS

¿Podemos revisar los procesos sin considerar los Sistemas de Información?

2130 - Control

La actividad de auditoría interna debe asistir a la organización en el mantenimiento de controles efectivos, mediante la evaluación de la eficacia y eficiencia de los mismos y promoviendo la mejora continua.

- **2130.A1 -**La actividad de auditoría interna debe **evaluar la adecuación y eficacia de los controles en respuesta a los riesgos del gobierno, operaciones y sistemas de información de la organización**, respecto de lo siguiente:
- Fiabilidad e integridad de la información financiera y operativa,
- Eficacia y eficiencia de las operaciones, ….



Solapamientos con revisiones realizadas por Sistemas y otras Áreas:

- ¿Debemos auditar la Seguridad de los Sistemas?
- ¿Debemos auditar la LOPD y otras Regulaciones?
- ¿Debemos auditar el plan de Continuidad del Negocio (y los Sistemas)?

2120 - Gestión de riesgos

La actividad de auditoría interna debe evaluar la eficacia y contribuir a la mejora de los procesos de gestión de riesgos.

- **2120.A1 -** La actividad de auditoría interna debe evaluar las **exposiciones al riesgo referidas a gobierno, operaciones y sistemas de información de la organización**, con relación a lo siguiente:
- **Fiabilidad de integridad de la información financiera y operativa, Eficacia y eficiencia de las operaciones, Protección de activos, y Cumplimiento de leyes, regulaciones y contratos.**
- **2120.A2 -** La actividad de auditoría interna debe evaluar la posibilidad de ocurrencia de fraude y cómo la organización maneja gestiona el riesgo de fraude.

→ **El "cómo" depende de la evaluación preliminar de los riesgos (*Norma 2210*):**

- Informes de Auditoría y/o Revisiones a disposición de Auditoría Interna.
- Independencia del auditor respecto al auditado. Certificaciones del Auditor.

Normas de Auditoría Interna del IAI (Instituto de Auditores Internos)

- Gobierno ¿Debemos revisar los Planes Estratégicos de Tecnología?

2110 - Gobierno […]

- **2110.A2 -** La actividad de auditoría interna debe evaluar si el **gobierno de tecnología de la información** de la organización sostiene y apoya las estrategias y objetivos de la organización.
- **2110.C1 -** Los objetivos de los trabajos de consultoría deben ser compatibles con los valores y las metas generales de la organización.

→ También entran en nuestro ámbito de actuación

- ¿Debemos hacer la Auditoría bienal de la LOPD, exigida y que queda a disposición de la Agencia Española de Protección de Datos?

→ Se aceptan como válidas las Auditorías Internas.

→ Podemos hacerlo, pero no existe la obligación.

→ Depende de la estructura organizativa, responsabilidades y presupuestos…

- Y por último, ¿Qué papel debe adoptar el auditor cuando los Servicios Informáticos se encuentran externalizados?

2220 - Alcance del trabajo
El alcance establecido debe ser suficiente para satisfacer los objetivos del trabajo.

- **2220.A1 -**El alcance del trabajo debe tener en cuenta los sistemas, registros, personal y bienes relevantes, **incluso aquellos bajo el control de terceros**.

→ Se encuentran también en nuestro ámbito de actuación.

→ Son importantes las condiciones contractuales. Nos deberían permitir evaluar el nivel de control interno y la realización de auditorías en condiciones pactadas.

La Auditoría Interna en los Sistemas de Información

La estructura del Área de Sistemas. Diferentes modelos

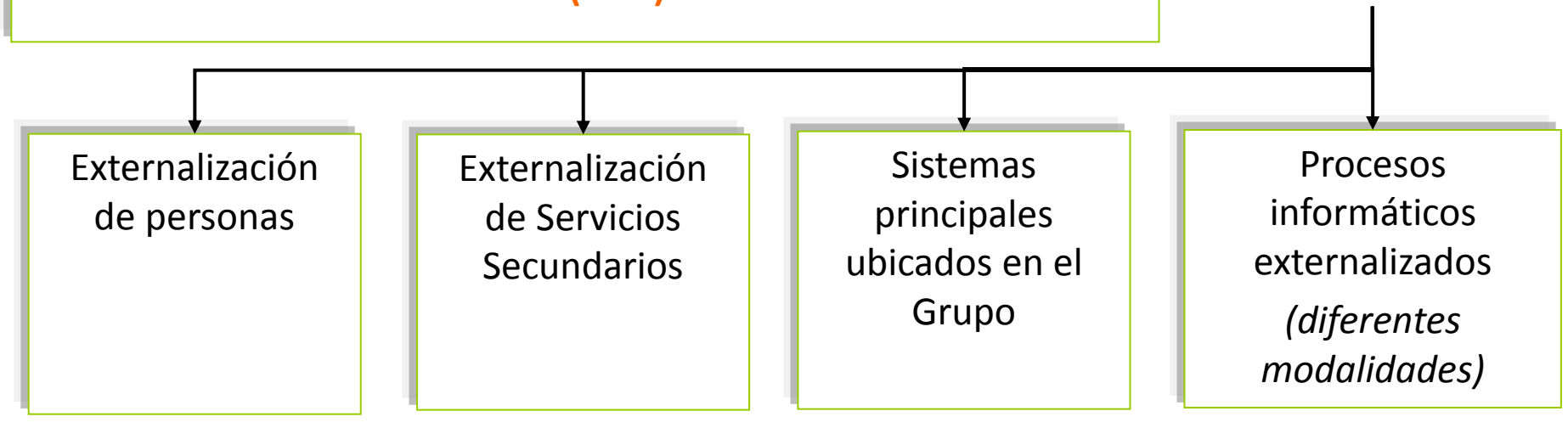
MAZARS

La Gestión de los Sistemas de Información – Estructura Organizativa

Funciones del Servicio de Informática en una Organización:

- **Desarrollo de Sistemas / Integración de Sistemas**
- **Administración de los Sistemas**
- **Administración de las Comunicaciones**
- **Gestión de la seguridad**
- **Micro-informática**
- **Atención a los usuarios (CAU)**

- Alternativas



Pérdida progresiva del control **directo**

No nos exime de nuestras responsabilidades como Auditoría Interna

Primeras preguntas del Auditor frente a un Sistema/Servicio Externalizado

Las 10 preguntas principales que nos debemos formular en Servicios Externalizados *(GTAG Guía de Auditoría de Tecnología Global - Externalización de las TI)*

- 1. ¿Los servicios tercerizados son importantes para el cliente?
- 2. ¿El cliente cuenta con una estrategia de tercerización bien definida?
- 3. ¿Cuál es la estructura de gobierno relacionada con las operaciones tercerizadas? ¿Los roles y responsabilidad están definidos con claridad?
- 4. ¿Se llevó a cabo un análisis de riesgo detallado al momento de la tercerización y se continúa realizando regularmente?
- 5. ¿Existen contratos formales o SLA para las actividades tercerizadas?
- 6. ¿El SLA define claramente los KPI para supervisar el desempeño del proveedor?
- 7. ¿Cómo se supervisa el cumplimiento del contrato o SLA?
- 8. ¿Cuál es el mecanismo utilizado para tratar el incumplimiento del SLA?
- 9. ¿Las responsabilidades de propiedad del sistema de datos, del sistema de comunicación, del sistema operativo, del software utilitario y del software de aplicación se definieron claramente y se acordaron con el proveedor de servicios?
- 10. ¿Cuál es el proceso para obtener aseguramiento de la eficacia operativa de los controles internos del lado del proveedor de servicios?

La Auditoría Interna en los Sistemas de Información

Marcos regulatorios y Estándares.

MAZARS

Marcos regulatorios o propios de Auditoría Interna

- SOX, JSOX, Directivas Europeas, Basilea II, COSO, Solvencia II,…

- GTAG - Guías de Auditoría de Tecnología Global (GTAG) preparadas por el IIA

  - ***1 GTAG -*** *Controles sobre las Tecnologías de la Información*
  - ***2 GTAG -*** *Change and Patch Management Controls: Critical for Organizational Success*
  - ***3 GTAG -*** *Auditoria continua: Implicaciones para el aseguramiento, supervision y evaluacion de riesgos*
  - ***4 GTAG -*** *Management of IT Auditing*
  - ***5 GTAG -*** *Managing and Auditing Privacy Risk*
  - ***6 GTAG -*** *Managing and Auditing IT Vulnerabilities*
  - ***7 GTAG -*** *Externalización de las TI*
  - ***8 GTAG -*** *Auditar Controles de Aplicación*
  - ***9 GTAG -*** *Gestión de Identidades y accesos*

Marcos propios de Gobierno y Gestión de Sistemas de Información

ISO (Organización Internacional para la Estandarización)

Serie 27000 -Contiene las mejores prácticas recomendadas en Seguridad

- ***27000:*** *Términos y definiciones que se emplean en toda la serie 27000.*
- ***27001:*** *Norma principal de la serie y contiene los requisitos del* ***sistema de gestión de seguridad de la información (SGSI)****.*
- ***27002:*** *Es una* ***guía de buenas prácticas*** *que describe los objetivos de control y controles recomendables* ***en cuanto a seguridad*** *de la información.*
- ***27003:*** *Publicación prevista en 2009. Guía de* ***implementación de SGSI*** *e información acerca del uso del modelo PDCA (Modelo "Plan, Do, Control y Act.)*
- ***27004:*** *Publicación prevista en año 2009.* ***Métricas*** *y las técnicas de medida aplicables para determinar la* ***eficacia de un SGSI*** *y de los controles relacionados.*
- ***27005:*** *Establece las* ***directrices para la gestión del riesgo*** *en la seguridad de la información.*
- ***27006:*** *Requisitos para la* ***acreditación de entidades de auditoría*** *y certificación de sistemas de gestión de seguridad de la información.*

Marcos propios de Gobierno y Gestión de Sistemas de Información

ISO (Organización Internacional para la Estandarización) (*continúa*)

- ***27007:*** *Publicación prevista en Mayo de 2010.* ***Guía de auditoría de un SGSI****.*
- ***27011:*** *Guía de gestión de seguridad de la información específica para telecomunicaciones.*
- ***27031:*** *Publicación prevista en 2010.* ***Guía de continuidad*** *de negocio en cuanto a tecnologías de la información y comunicaciones.*
- ***27032:*** *Publicación prevista en 2009. Guía relativa a la* ***ciberseguridad****.*
- ***27033:*** *Publicación prevista entre 2010 y 2011. Guía de* ***seguridad en redes****, que estará compuesta por 7 partes.*
- ***27034:*** *Publicación prevista en 2009. Guía de* ***seguridad en aplicaciones****.*
- ***27799:*** *Estándar de gestión de seguridad de la información en el* ***sector sanitario*** *aplicando ISO 27002.*
- ***ITIL - serie ISO/IEC 20000 -*** *Service Management. Es el estándar reconocido internacionalmente* ***en gestión de servicios de TI*** *(Tecnologías de la Información).*
- ***38500 -*** *Norma para el Gobierno de las TIC*

Marcos propios de Gobierno y Gestión de Sistemas de Información

- BSI (British Standards Institution)
  - ***25999*** *– Establece las mejores prácticas, recomendaciones y actividades específicas para lograr la continuidad de negocio teniendo en cuenta los riesgos a los que se enfrenta una organización.*
  - ***10008.*** *Valor probatorio y la admisibilidad legal de la información electrónica.*
- ISACA (Information Systems Audit and Control Association)
  - ***COBIT*** *(Control Objectives for Information and related Technology). Modelo de administración de Tecnologías de Información, que comprende un conjunto de procesos, objetivos, indicadores de madurez y guías de auditoría.*
  - ***ValIT*** *- Relaciona los procesos de COBIT con los procesos de la gerencia requeridos para conseguir un buen valor de las* ***inversiones en tecnologías de la información****.*
  - ***RiskIT*** *- Marco de gobierno de los* ***riesgos corporativos de TI.***
- **ISECOM (Institute for Security and Open Methodologies)**
  - ***OSSTMM*** *(Open Source Security Testing Methodology Manual) – Metodología abierta de Testeo de Seguridad.*
  - ***OWASP*** *(Open Web Application Security Project) – Metodología para garantizar la seguridad en aplicaciones web abiertas al exterior.*

Marcos propios de Gobierno y Gestión de Sistemas de Información (*continúa*)

- *PCI SSC (Payment Card Industry Security Standards Councuil)*
  - *PDCI – DSS (Payment Card Industry Data Security Standard). Estándar de Seguridad de Datos para la **Industria de Tarjetas de Pago**. guía que ayude a las organizaciones que procesan, almacenan y/o transmiten datos de tarjetahabientes (o titulares de tarjeta), a asegurar dichos datos, con el fin de prevenir los fraudes que involucran tarjetas de pago débito y crédito.*
- *Legislación Española*
  - ***LOPD** – L.O. de Protección de los Datos de Carácter Personal*
  - ***RD1720/2007**, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de protección de datos de carácter personal*
  - ***LSSICE** - Ley 34/2002, de Servicios de la Sociedad de la Información y de Comercio Electrónico*
  - ***LISI** - Ley 56/2007, de Medidas de Impulso de la Sociedad de la Información*
  - *Ley 59/2003, de **Firma Electrónica***
  - ***Ley 11/2007**, de **acceso electrónico de los ciudadanos** a los Servicios Públicos.*

La Auditoría Interna en los Sistemas de Información

¿Contratar o subcontratar?

El perfil del Auditor Informático

MAZARS

Debida competencia profesional

¿Contratamos a Auditores Informáticos o Subcontratamos el Servicio?

1200 - Aptitud y cuidado profesional

Los trabajos deben cumplirse con aptitud y cuidado profesional adecuados.

2010 - Planificación

El director ejecutivo de auditoría debe establecer **planes basados en los riesgos**, a fin de determinar las prioridades de la actividad de auditoría interna. Dichos planes deberán ser consistentes con las metas de la organización.

2230 - Asignación de recursos para el trabajo

- Los auditores internos deben determinar los recursos adecuados y suficientes para lograr los objetivos del trabajo, basándose en una evaluación de la naturaleza y complejidad de cada trabajo, las restricciones de tiempo y los recursos disponibles.

Ventajas de la Subcontratación

- Expertos en diferentes materias y con la visión obtenida de las auditorías en otras organizaciones.
- Utilización de metodologías ya desarrolladas por las firmas Auditoras.
- Comunicación de conclusiones realizadas por personal externo a la organización (independencia respecto a sistemas).
- Ante un suministrador en un contrato de externalización, es un ente neutral.
- Rotación de los perfiles informáticos.

→ Depende de la política de contratación de la organización

Debida competencia profesional

Formación Académica

- Ingeniero Técnico, Ingeniero, Diplomado o Licenciado en **Informática, Telecomunicaciones, Industriales o Matemáticas.**
- **Master en Auditoría Informática o Seguridad Informática**, Derecho de Nuevas Tecnologías, o post-grado equivalente.

☑ **Certified Information Systems Auditor (CISA)** es una certificación para auditores respaldada por la Asociación ISACA (Information Systems Audit and Control Association). Los candidatos deben cumplir requisitos establecidos por la ISACA.

☑ **Certified Information Security Manager (CISM)** es una certificación para Responsables de Seguridad respaldada por la Asociación ISACA.

☑ **Certified Information Systems Security Professional (CISSP)** otorgada por la (ISC)2 (International Information Systems Security Certification Consortium, Inc). CISSP es considerada como una de las credenciales de mayor representatividad en el ámbito de la seguridad informática.

Otras:

☑Auditor Interno certificado CIA (Certified Internal Auditor) por el IIA (www.theiia.org)

☑Auditor de Sistemas de Gestión de la Seguridad de la Información - Certificado AENOR

☑Certificate ITIL: Foundation Certificate in IT o superiores

Debida competencia profesional

Conocimientos

Idiomas: Inglés alto, y otros idiomas (según la organización)

Conocimientos desarrollo y administración de sistemas:

- Sistemas Operativos (Windows, UNIX, OS/390, AS/400).
- Programación (Cobol, Visual Basic, Access Basic, SQL, C).
- Bases de Datos: (ORACLE, SQL Server, DB2).
- Conocimientos de seguridad tecnológica (firewalls, VPNs, PKIs, IDS/IPS, etc)
- Herramientas de interrogación de datos: ACL o IDEA
- SAP

Conocimientos de normativas, metodologías, estándares y legislación vigente:

- Normativas y estándares de Seguridad de TI: ISO 17799, ISO 27001, BS25999, NIST, COBIT
- Regulación legal: LOPD, RD1720/2007, LSSI, etc.
- Metodologías de análisis de riesgos: MAGERIT, CRAMM, Octave, etc.
- Regulaciones sectoriales: SOX, Basilea II
- Metodologías de intrusión: OSSTMM / OWASP
- Análisis Forense y evidencias electrónicas
- Mejores prácticas ITIL
- Metodologías de desarrollo: Métrica

Conocimientos propios del sector

Debida competencia profesional

Habilidades

- ☑ **Competencias sociales:**
  - ☑ **Trabajo en equipo:** Capacidad para desempeñar un rol dentro de un equipo de trabajo, con responsabilidad y en colaboración.
  - ☑ **Comunicación.** Capacidad de informar, recibir información y transmitir una idea claramente, tanto a nivel escrito como verbal.
  - ☑ **Resolución de problemas**. Análisis y toma de decisiones en situaciones no resueltas.
- ☑ **Competencias de apoyo al crecimiento.**
  - ☑ **Análisis:** Capacidad de ver diferentes partes o aspectos de una misma información.
  - ☑ **Síntesis:** Capacidad de llegar a una conclusión tras el análisis de una serie de datos.
  - ☑ **Autoaprendizaje**. Habilidades para analizar y adquirir nuevos conocimientos de manera autónoma.
  - ☑ **Adaptabilidad**. Adaptación a los cambios organizacionales. Capacidad para realizar diferentes tareas, asumiendo diferentes roles.
- ☑ **Competencias personales:**
  - ☑ **Inteligencia emocional.** Aptitudes para controlar las emociones dentro de las relaciones sociales. Autocontrol.
  - ☑ **Integridad**. Coherencia en las actitudes e ideas transmitidas.
  - ☑ **Motivación**. Auto-motivación para desempeñar un trabajo con responsabilidad y entusiasmo.

La Auditoría Interna en los Sistemas de Información

¿Por dónde empezamos?

MAZARS

¿Por dónde empezamos para iniciar las Auditorías Informáticas?

- ¿Cómo implantar la Función de Auditoría Informática en Auditoría Interna?

Recomendación: Implantación gradual.

- Inicialmente sub-contratar servicios de Auditoría Informática, que permitan: auditar los controles automatizados de los procesos, y obtener el conocimiento sobre los Sistemas de Información y su Gestión. Permitirá romper resistencias del personal informático, en algunos casos.
- Contratar al coordinador de la Función de Auditoría Informática, con el objeto de que:
  - Participe en las reuniones de los servicios subcontratados de Auditoría Informática (por el Área de Auditoría Interna, o por otras áreas) con el Área de Sistemas.
  - Gestione el conocimiento sobre el control de los Sistemas.
  - Participe en la elaboración del Plan de Auditoría Interna, respecto a los Sistemas de Información.
- Según la política de contratación / subcontratación de la organización, incorporar gradualmente personal para tareas repetitivas y recurrentes.
- Subcontratar los servicios de Auditoría más especializados.

La Auditoría Interna en los Sistemas de Información

Un ejemplo de alcance siguiendo la ISO 27002

MAZARS

Ejemplo de alcance de una Auditoría Interna de Seguridad

Metodología ISO 27002:2005

Código de buenas prácticas para la gestión de la Seguridad de la Información

MAZARS

Ejemplo de alcance de una Auditoría Interna de Seguridad

√ **1. Política de Seguridad**

- ❖ **1.1. Política de seguridad de la información**
  - Documento de la política de seguridad de la información
  - Revisión de la política de seguridad de la información

√ **2. Organización de la seguridad de la información**

- ❖ **2.1. Organización interna**
  - Compromiso de la gerencia con la seguridad de la información
  - Coordinación de la seguridad de la información
  - Asignación de las responsabilidades de la seguridad de la información
  - Autorización de proceso para facilidades procesadoras de información
  - Acuerdos de confidencialidad
  - ✕ Contacto con las autoridades
  - Contacto con grupos de interés especial
  - Revisión independiente de la seguridad de la información
- ❖ **2.2. Grupos o personas externas**
  - Identificación de los riesgos relacionados con los grupos externos
  - ✕ Tratamiento de la seguridad cuando se lidia con clientes
  - Tratamiento de la seguridad en acuerdos con terceros

Ejemplo de alcance de una Auditoría Interna de Seguridad

✗ **3. Gestión de activos**

- ❖ 3.1. Responsabilidad por los activos
- ❖ 3.2. Clasificación de la información

√ **4. Seguridad de recursos humanos**

- ✗ ❖ 4.1. Antes del empleo
- ❖ **4.2. Durante el empleo**
  - ✗ • Responsabilidades de la gerencia
  - • Conocimiento, educación y capacitación en seguridad de la información
  - ✗ • Proceso disciplinario
- ❖ **4.3. Terminación o cambio de empleo**
  - • Responsabilidades de terminación
  - • Devolución de los activos
  - • Retiro de los derechos de acceso

√ **5. Seguridad física y ambiental**

- ❖ **5.1. Áreas seguras**
  - • Perímetro de seguridad física
  - • Controles de ingreso físico
  - ✗ • Asegurar las oficinas, habitaciones y medios
  - • Protección contra amenazas externas e internas
  - ✗ • Trabajo en áreas aseguradas
  - ✗ • Áreas de acceso público, entrega y carga
- ✗ ❖ 5.2. Seguridad de los equipos

Ejemplo de alcance de una Auditoría Interna de Seguridad

6.Gestión de las comunicaciones y operaciones

- **6.1. Procedimientos y responsabilidades operacionales**
  - Procedimientos de operación documentados
  - Gestión del cambio
  - Segregación de los deberes
  - Separación de los medios de desarrollo, prueba y operación
- **6.2. Gestión de la entrega del servicio de terceros**
- **6.3. Planeación y aceptación del sistema**
- **6.4. Protección contra el código malicioso y móvil**
  - Controles contra códigos maliciosos
  - Controles contra códigos móviles
- **6.5. Respaldo o Back-Up**
- **6.6. Gestión de seguridad de la red**
  - Controles de redes
  - Seguridad de los servicios de la red
- **6.7. Gestión de medios**
- **6.8. Intercambio de información**
- **6.9. Servicios de comercio electrónico**
- **6.10. Monitoreo**
  - Registro de auditoría
  - Uso del sistema de monitoreo
  - Protección del registro de información
  - Registros del administrador y operador
  - Registro de fallos
  - Sincronización de relojes

Ejemplo de alcance de una Auditoría Interna de Seguridad

✓ **7. Control del acceso**

- ❖ **7.1. Requerimiento del negocio para el control del acceso**
- ❖ **7.2. Gestión de acceso del usuario**
- ❖ **7.3. Responsabilidades del usuario**
- ❖ **7.4. Control de acceso a la red**
  - Política sobre el uso de los servicios de la red
  - Autenticación del usuario para las conexiones externas
  - ✗ Identificación del equipo en las redes
  - ✗ Protección del puerto de diagnóstico y configuración remoto
  - Segregación en redes
  - ✗ Control de conexión a la red
  - ✗ Control de routing de la red
- ✗ ❖ **7.5. Control del acceso al sistema operativo**
- ❖ **7.6. Control de acceso a la aplicación y la información**
  - Restricción del acceso a la información
  - ✗ Aislar el sistema confidencial
- ✗ ❖ **7.7. Computación y tele-trabajo móvil**

Ejemplo de alcance de una Auditoría Interna de Seguridad

√ 8. Adquisición, desarrollo y mantenimiento de los SS.II.

- **8.1. Requerimientos de seguridad de los sistemas de información**
  - Análisis y especificación de los requerimientos de seguridad
- ✗ **8.2. Procesamiento correcto en las aplicaciones**
- ✗ **8.3. Controles criptográficos**
- ✗ **8.4. Seguridad de los archivos del sistema**
- **8.5. Seguridad en los procesos de desarrollo y soporte**
  - Procedimientos del control del cambio
  - Revisión técnica de la aplicación después de cambios en el sistema
  - Restricciones sobre los cambios en los paquetes de software
  - Filtración de información
  - Desarrollo de software abastecido externamente
- ✗ **8.6. Gestión de la Vulnerabilidad Técnica**

√ 9. Gestión de incidentes en la seguridad de la información

- **9.1. Reporte de los eventos y debilidades de la seguridad de la información**
  - Reporte de eventos en la seguridad de la información
  - Reporte de las debilidades en la seguridad
- **9.2. Gestión de los incidentes y mejoras en la seguridad de la información**
  - Responsabilidades y procedimientos
  - ✗ Aprender de los incidentes en la seguridad de la información
  - ✗ Recolección de evidencia

Ejemplo de alcance de una Auditoría Interna de Seguridad

√ **10. Gestión de la continuidad del negocio**

❖ **10.1. 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

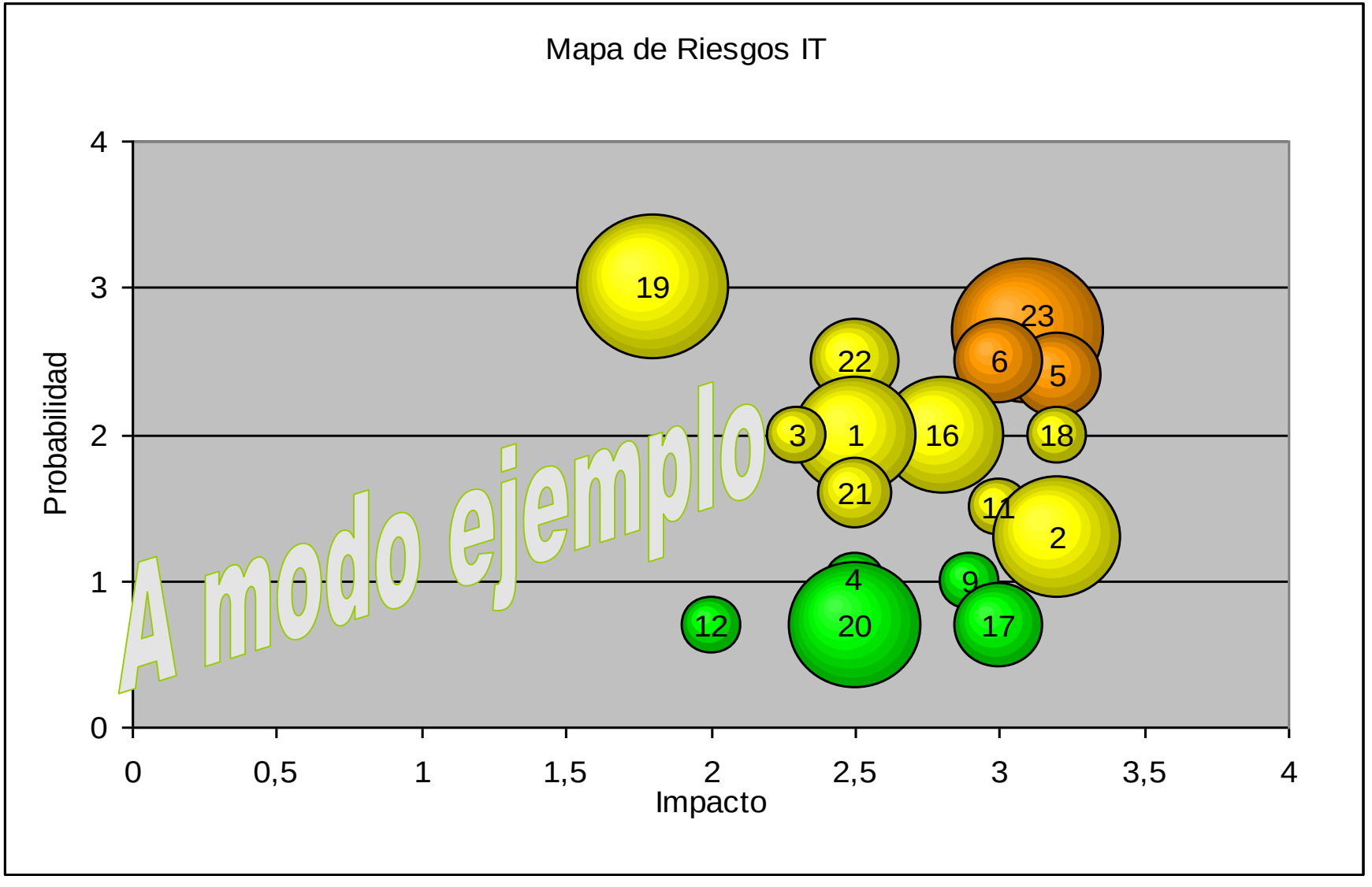
√ **11. Cumplimiento**

❖ **11.1. Cumplimiento de los requerimientos legales**

- Identificación de la legislación aplicable
- ✗ Derechos de propiedad intelectual (IPR)
- ✗ Protección de registros organizacionales
- Protección de la data y privacidad de la información personal
- ✗ Prevención del mal uso de los medios de procesamiento de la información
- ✗ Regulación de controles criptográficos

✗ ❖ **11.2. Cumplimiento de las políticas y estándares de seguridad, y cumplimiento técnico**

Resultados de la Auditoría Informática de Seguridad



MAZARS

Resultados de la Auditoría Informática de Seguridad

Riesgo Muy Alto:

No se ha detectado ningún riesgo muy alto

Riesgo Alto:

	Áreas de Mejora	Impacto	Probabilidad	Esfuerzo
23	Metodología del ciclo de vida de desarrollo	3,1	2,7	2,5
5	Gestión de Riesgos asociados a personal externo	3,2	2,4	1,5
6	Planes de Calidad y Seguridad en Servicios externos	3	2,5	1,5

Riesgo Medio:

	Áreas de Mejora		abilidad	Esfuerzo
18	Prueba periódica de las copias de seguridad		2	1
22	Revisión periódica de usuarios y reg	5	2,5	1,5
16	Uso de portátiles, equipos móviles	2,8	2	2
19	Política de per sos en	1,8	3	2,5
1	Actualización Polí	2,5	2	2
3	Comisión de S uimi	2,3	2	1
11	Revisión de u ios	3	1,5	1
2	Análisis de ri sg s para las diferentes aplicaciones	3,2	1,3	2,1
21	Política de calidad de las contraseñas	2,5	1,6	1,2

Riesgo Bajo:

	Áreas de Mejora	Impacto	Probabilidad	Esfuerzo
9	Acceso a áreas de acceso limitado	2,9	1	1
4	Compromiso de confidencialidad en externos	2,5	1	1
17	Normativa de desechado y reutilización de soportes	3	0,7	1,5
20	Registro centralizado de permisos autorizados	2,5	0,7	2,2
12	Test de seguridad física	2	0,7	1

Prioridades y pautas para elaborar el Plan de Auditoría Informática

MAZARS

Prioridades y presupuestos

1. AUDITORÍA DE PROCESOS AUTOMATIZADOS

- → Sub-contratación de personal para revisión de controles automatizados, en los procesos a auditar dentro del plan de auditoría.
- → Análisis de Datos. Análisis SCAN-D para SAP.

Presupuesto (jornadas): 5 - 10 días por proceso y 15 días para análisis SCAN-D.

2. AUDITORÍA DE SEGURIDAD GENERAL

- → Auditoría de Buenas Prácticas de Seguridad (ISO 27002).

Presupuesto (jornadas): de 20 a 30 días.

3. AUDITORÍAS ESPECÍFICAS EN FUNCIÓN DEL RIESGO

- → Auditoría de Seguridad de Servicios Web / Plan de Continuidad / LOPD, ….

Presupuesto para cada tipo (jornadas): de 30 a 40 días.

4. AUDITORÍA DE CALIDAD DE SERVICIOS EXTERNALIZADOS

- → Auditoría de verificación de cumplimiento con el contrato

Presupuesto (jornadas): de 30 a 40 días.

Nuestros servicios de Gestión de Riesgos Tecnológicos

1. Cumplimiento legal (pág. 15)

- 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. 29)

- 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. 47)

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

4. Governance IT (pág. 50)

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

5. Soporte a Auditoría/Control Interno (pág. 54)

- Herramientas de Análisis de Datos. Forensic
- Análisis SCAN-D para SAP
- Implantación de Proaudit Advisor como soporte al Control Interno

La Auditoría Interna en los Sistemas de Información

Conclusiones

MAZARS

Conclusiones

- La Auditoría Informática juega un papel cada vez más importante dentro de la Auditoría Interna.
- La contratación o subcontratación de Auditores Informáticos debe garantizar unas Competencias Profesionales.
- Conveniencia de la implantación gradual de la función de Auditoría Informática Interna.
- La importancia del análisis de datos y las revisiones multidisciplinares (auditor informático y auditor interno)
- No inventar la rueda: Auditar los Sistemas en base a Marcos y Estándares conocidos.

La Auditoría Interna en los Sistemas de Información

Preparación del próximo desayuno

MAZARS

Preparación de la próxima sesión

Fecha :

- 29 de enero de 2010 en Madrid
- 5 de febrero de 2010 en Barcelona

Tema propuesto inicialmente:

- Control Interno. Cómo integrar el Mapa de Riesgos Tecnológicos con el Mapa de Riesgos Corporativo. La gestión del Riesgo Tecnológico.

Otros temas interesantes:

- Cómo comprobar la validez de documentos firmados digitalmente. DNI-e. e-Factura.
- Auditoría de procesos que se encuentran automatizados. El riesgo oculto al auditor.
- Investigaciones internas y evidencias electrónicas. Qué podemos hacer y qué no.
- El buen gobierno de la Auditoría: Octava Directiva

- Contribuciones eventuales

auditoria.it@mazars.es

www.mazars.es

C/ Aragón, 271

08007 Barcelona

España

Tel : +34 934 050 855

Fax: +34 934 050 770

c/ Claudio Coello, 124

28006 Madrid

España

Tel. : +34 915 624 030

Fax: +34 915 610 224

GRACIAS