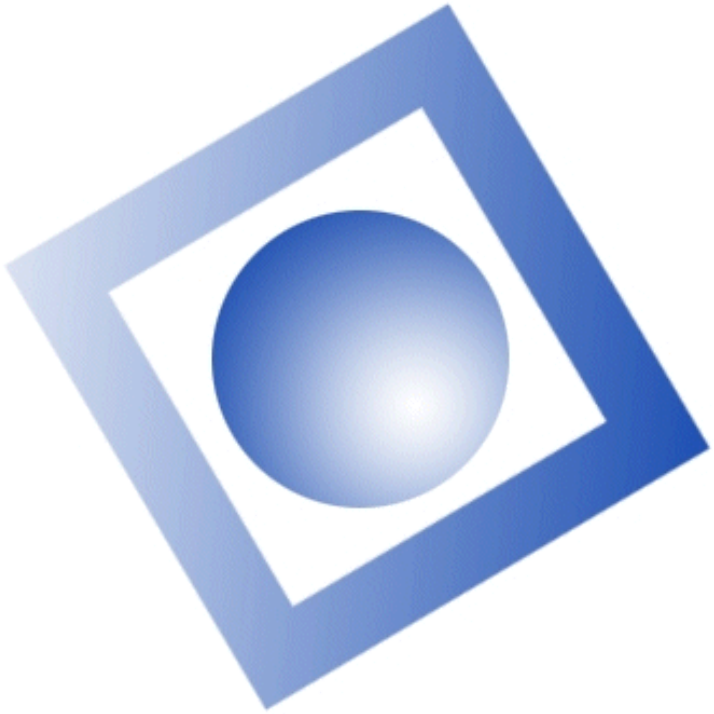


AEMES
asociación española
de métricas del software

VII Conferencia Anual

Indicadores y medición de riesgos en los procesos de negocio

Grupo TQS

C/ Chile 4, edificio II, oficina 20
28290 Las Rozas. Madrid
Tel: 916368020

14 de Noviembre 2006

Seguridad en organizaciones ...

¿Cuál de las siguientes organizaciones tiene mejor protegida su información?

- ***BBVA***
- ***LA CAIXA***
- ***AMADEUS***
- ***EL CORTE INGLES***
- ***MAPFRE***
- ***. . .***

Respuesta: "... depende ..."

Seguridad en tecnología ...

¿Cuál de los siguientes entornos tecnológicos es el más seguro?

- ***IBM AS/400***
- ***Sun Solaris***
- ***Windows 2003***
- ***Linux***
- ***Mac OS/X***
- ***. . .***

Respuesta: "... depende ..."

Conclusión ...

El estado de la seguridad ...

- ***Es dificil definir el concepto de "seguridad buena"***
- ***Es dificil distinguir entre "seguridad" y "suerte"***
- ***No sabemos medir para luego poder mejorar (internamente) o comparar (externamente)***
- ***Una incidencia no significa un fracaso / la ausencia de incidencias no significa un éxito***

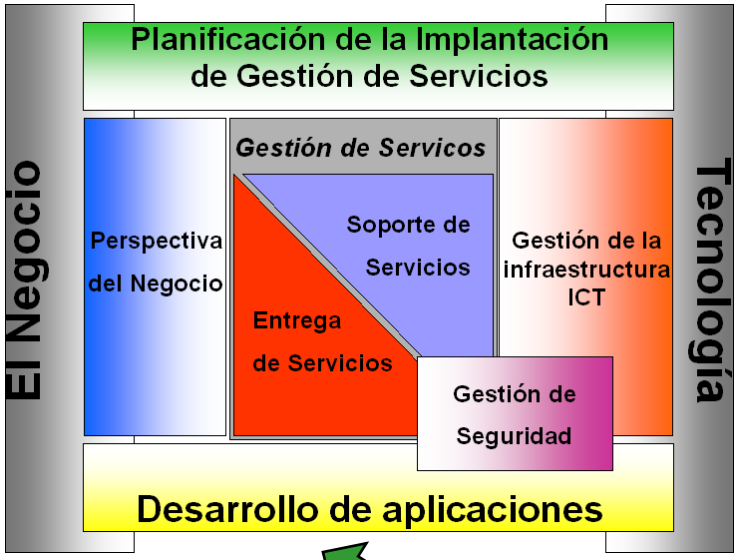
Vamos a trabajar sobre cada uno de estos puntos ...

Distintos enfoques de gestión de riesgos TI

Existen varias metodologías y enfoques con controles y **buenas prácticas** para cubrir parcialmente la gestión de los diferentes aspectos de las nuevas tecnologías en una organización, y consecuentemente los riesgos TI.

ITIL®

- En teoría, no es solamente para la gestión de las operacones TI, tiene dominios referentes a la seguridad y al desarrollo.
- Tiene una estructura de "procesos" de buenas prácticas



- Lo aplicamos a procesos de Desarrollo. Además, hay modulos para la entrega de Servicios y para actividades de adquisición.
- Es "un modelo que describe las características de procesos efectivos" para la mejora de estos procesos, basado en un modelo de madurez

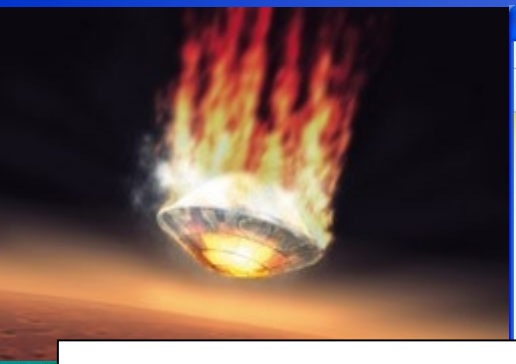
ISO IEC

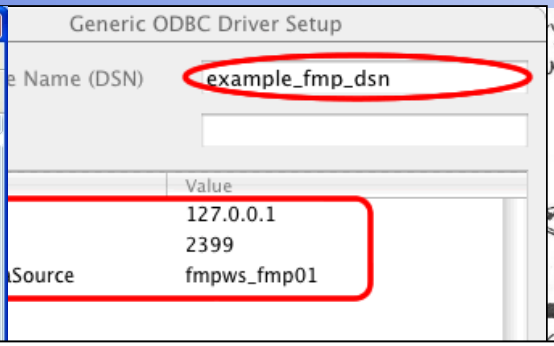
- Enfocado sobre la seguridad, es un conjunto de controles que forman un "Código de Prácticas"

CMMI®

Grupo TQS

La necesidad de una medición de riesgos IT



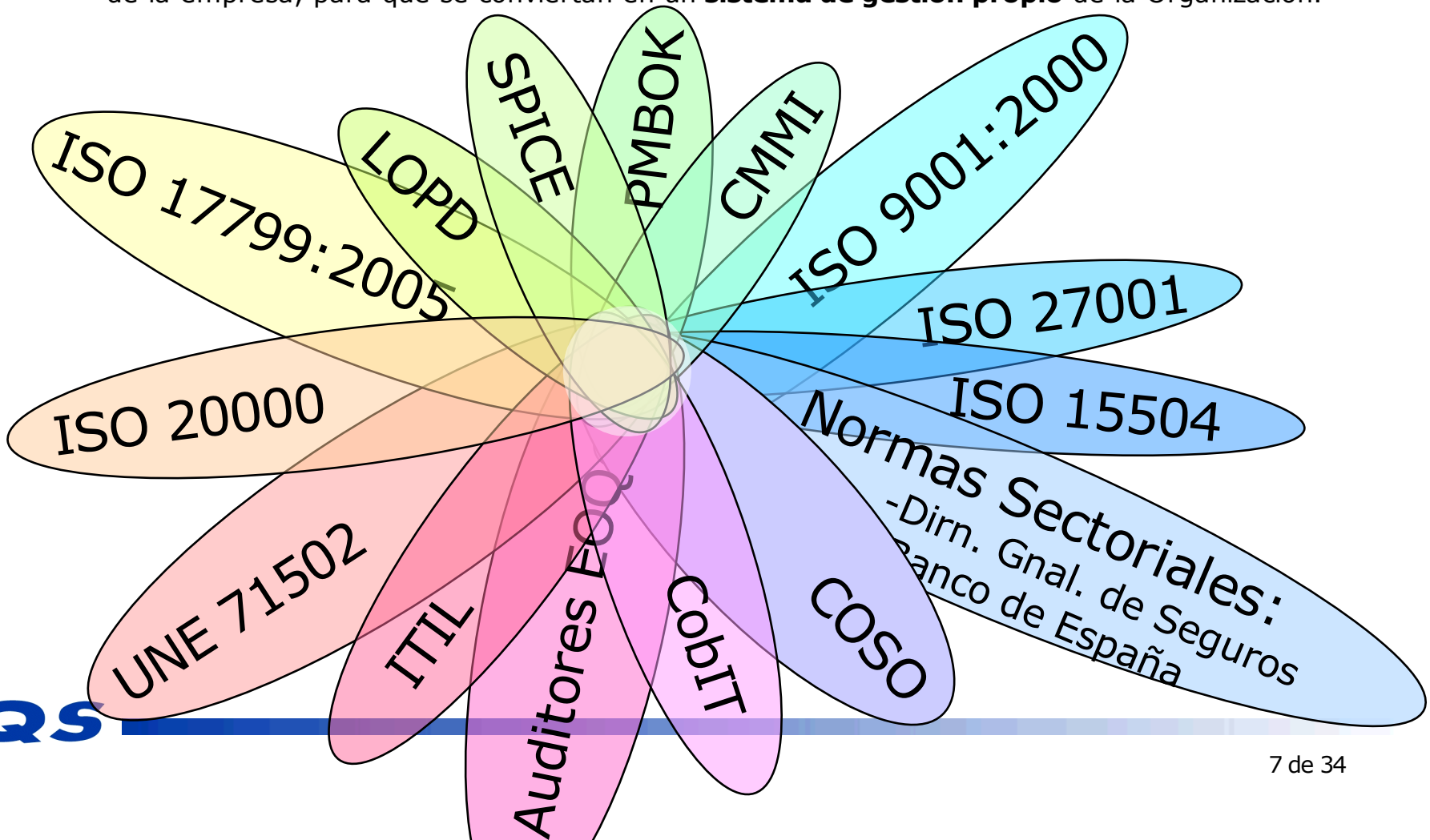


- **La necesidad que existe en integrar los procesos de gestión de TI es obvia, siendo un paso más hacia la búsqueda de calidad y excelencia de servicio, respaldadas por la satisfacción de los usuarios**
  - Por una parte, el proceso de implantación de un enfoque único es más eficaz, que la implantación de varios modelos de gestión específicos.
  - Por otra parte, tanto la gestión de bajo nivel (actividades día-a-día individuales), como la gestión de alto nivel (actividades de gobierno) se benefician de esta visión integrada.

IPN BU 0193/8066 FASTYN MARIAN
IPN BU 0218/3509 FASTYN MARZENNA
IPN BU 0592/3 FASTYN STANISŁAW
IPN BU 0988/95 FASTYNIAK FELIKS
IPN BU 649/99 FASZCZA MARIA
IPN BU 645/286 FASZCZEWSKI ADAM
IPN BU 01013/1241 FASZCZEWSKI STANISŁAW
IPN BU 0193/8612 FASZCZEWSKI STEFAN
IPN BU 00169/50 FASZYŃSKI JERZY I INNI
IPN BU 00611/1457 FATALSKI BRONISŁAW
IPN BU 001198/5199 FATALSKI BRONISŁAW
IPN BU 01013/1242 FATEK STANISŁAW
IPN BU 01133/997 FATYGA BOLESŁAW
IPN BU 00612/2213 FATYGA CZESŁAW
IPN BU 001198/5306 FATYGA CZESŁAW
IPN BU 00612/2538 FATYGA ROBERT
IPN BU 001198/5831 FATYGA ROBERT
IPN BU 00612/2704 FATYGA RYSZARD
IPN BU 001198/5961 FATYGA RYSZARD

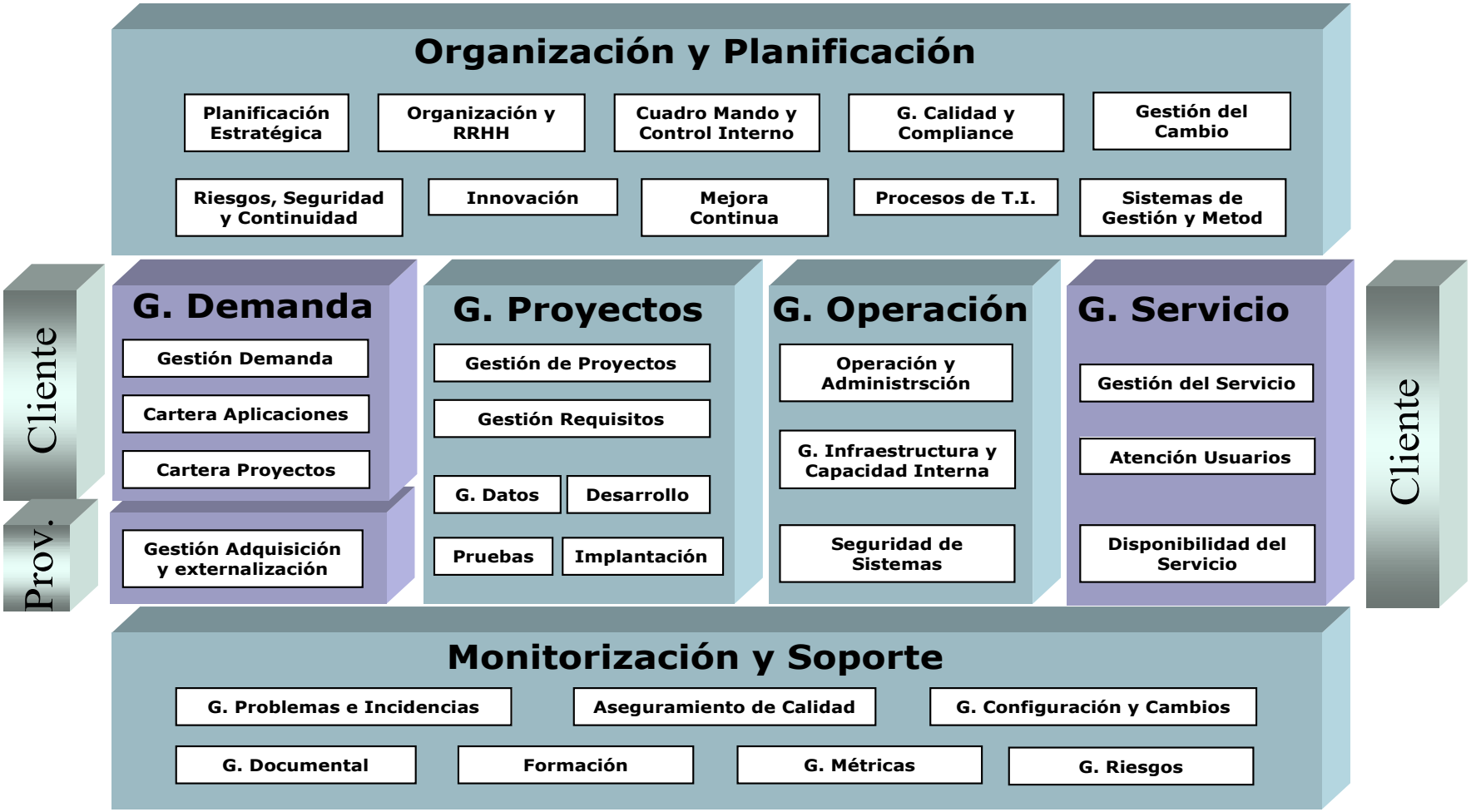
Estándares y normas de buenas prácticas

- **Hay multitud de estándares que podemos aplicar a los procesos de gestión IT**
  - Cada uno tiene su propio enfoque y utilidad, pero en todo caso con solapamiento entre ellos.
  - Todos tratan el riesgo de algún modo, muchos pueden introducir riesgo.
- **Hemos de cuidar la selección "a la carta" de buenas prácticas**
  - Probablemente habrá que adaptarlas para que conformen con las necesidades y la estrategia de la empresa, para que se conviertan en un **sistema de gestión propio** de la Organización.



La gestión integrada de TI ...

... y de sus riesgos



Identificación e Integración de Procesos de Gestión

Los procesos de gestión IT en el modelo **MPC-TI®** están estructurados en seis áreas e integra todos los procesos críticos de la Gestión de TI:

❑Organización y Planificación

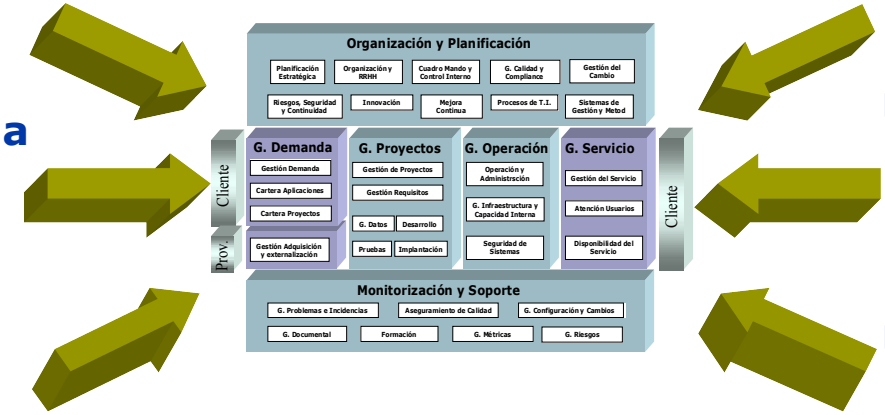
- Planificación estratégica
- Organización y RRHH
- Gestión del Cambio
- Procesos de TI
- Innovación
- Mejora Continua
- Cuadro de Mando y Control Interno
- Gestión de Calidad de SW y Compliance
- Riesgos, Seguridad y Continuidad
- Sistemas de Gestión y Metodologías

❑Gestión de la Demanda

- Gestión de la Demanda
- Cartera de Aplicaciones
- Cartera de Proyectos
- Gestión de Adquisición y externalización

❑Gestión de Proyectos

- Modelos de Gestión de Proyectos
- Gestión de Requisitos
- Gestión de Datos
- Desarrollo
- Pruebas
- Implantación



❑Gestión de Operación

- Operación y Administración
- Gestión de Infraestructura y Capacidad
- Seguridad de Sistemas

❑Gestión del Servicio

- Gestión del Servicio
- Atención a Usuarios
- Disponibilidad del Servicio

❑Monitorización y Soporte

- Gestión de Problemas e Incidencias
- Aseguramiento Calidad
- Gestión de Configuración y Cambios
- Gestión Documental
- Formación
- Gestión de Métricas
- Gestión de Riesgos

La construcción del modelo de métricas de riesgos

Gestión de configuración y cambios	*Soporte y Monitorización*

La construcción del modelo de métricas de riesgos

Gestión de configuración y cambios	*Soporte y Monitorización*

Objetivo

Asegurar la correcta identificación, control y estado de los elementos críticos de TI, como son el software, el hardware, los productos, servicios, documentación **así como el control de los cambios** y la información relacionada a los mismos.

La construcción del modelo de métricas de riesgos

Gestión de configuración y cambios	*Soporte y Monitorización*

Objetivo	**Factores clave**
Asegurar la correcta identificación, control y estado de los elementos críticos de TI, como son el software, el hardware, los productos, servicios, documentación **así como el control de los cambios** y la información relacionada a los mismos.	▪ Identificar y controlar los elementos de configuración y líneas base, la información del estado de la configuración y las auditorías de la configuración. ▪ El Procedimiento de gestión de cambios debe incluir el control de los diferentes tipos de cambio, las solicitudes de cambio, análisis de impacto, aprobación de los cambios, control de la realización de los cambios, control de entregas y un tratamiento especial de los cambios urgentes e información actualizada sobre el proceso de cambio ▪ La Base de Datos de Gestión de Configuración será completa, íntegra y actualizada, dando cabida a elementos de configuración de distinto tipo y formato, ya sea HW, SW, Comunicaciones., productos, servicios ó documentos. ▪ El uso de herramientas automáticas se convierte en un factor clave en entornos complejos. ▪ Construir o proporcionar especificaciones para construir elementos (derivados) a partir de otros desde el sistema de gestión de configuración.

La construcción del modelo de métricas de riesgos

Gestión de configuración y cambios			*Soporte y Monitorización*		
COBIT	ISO 9000	EFQM	CMMI / ISO 15504	ITIL / BS ISO 20000	Otros

Objetivo	**Factores clave**
Asegurar la correcta identificación, control y estado de los elementos críticos de TI, como son el software, el hardware, los productos, servicios, documentación **así como el control de los cambios** y la información relacionada a los mismos.	▪ Identificar y controlar los elementos de configuración y líneas base, la información del estado de la configuración y las auditorías de la configuración. ▪ El Procedimiento de gestión de cambios debe incluir el control de los diferentes tipos de cambio, las solicitudes de cambio, análisis de impacto, aprobación de los cambios, control de la realización de los cambios, control de entregas y un tratamiento especial de los cambios urgentes e información actualizada sobre el proceso de cambio ▪ La Base de Datos de Gestión de Configuración será completa, íntegra y actualizada, dando cabida a elementos de configuración de distinto tipo y formato, ya sea HW, SW, Comunicaciones., productos, servicios ó documentos. ▪ El uso de herramientas automáticas se convierte en un factor clave en entornos complejos. ▪ Construir o proporcionar especificaciones para construir elementos (derivados) a partir de otros desde el sistema de gestión de configuración.

La construcción del modelo de métricas de riesgos

Gestión de configuración y cambios			*Soporte y Monitorización*		
COBIT	**ISO 9000**	**EFQM**	**CMMI / ISO 15504**	**ITIL / BS ISO 20000**	**Otros**
AI6-Manage Changes, DS9-Manage the Configuration	**ISO 90003**		Configuration Managemant	SS 7,8, AM38	**ISO 17799**

Objetivo

Asegurar la correcta identificación, control y estado de los elementos críticos de TI, como son el software, el hardware, los productos, servicios, documentación **así como el control de los cambios** y la información relacionada a los mismos.

Factores clave

- Identificar y controlar los elementos de configuración y líneas base, la información del estado de la configuración y las auditorías de la configuración.
- El Procedimiento de gestión de cambios debe incluir el control de los diferentes tipos de cambio, las solicitudes de cambio, análisis de impacto, aprobación de los cambios, control de la realización de los cambios, control de entregas y un tratamiento especial de los cambios urgentes e información actualizada sobre el proceso de cambio
- La Base de Datos de Gestión de Configuración será completa, íntegra y actualizada, dando cabida a elementos de configuración de distinto tipo y formato, ya sea HW, SW, Comunicaciones., productos, servicios ó documentos.
- El uso de herramientas automáticas se convierte en un factor clave en entornos complejos.
- Construir o proporcionar especificaciones para construir elementos (derivados) a partir de otros desde el sistema de gestión de configuración.

Interrelaciones entre Procesos de Gestión de TI

Los procesos de gestión IT en el modelo **MPC-TI®** están estructurados en seis áreas e integra todos los procesos críticos de la Gestión de TI. Las interdependencias entre procesos de Gobierno, Producción, Desarrollo, Seguridad y Monitorización:

❑Organización y Planificación

- Planificación estratégica
- Organización y RRHH
- Gestión del Cambio
- Procesos de TI
- Innovación
- Mejora Continua

- Cuadro de Mando y Control Interno
- Gestión de Calidad de SW y Compliance
- Riesgos, Seguridad y Continuidad
- Sistemas de Gestión y Metodologías

❑Gestión de Operación

- Operación y Administración
- Gestión de Infraestructura y Capacidad
- Seguridad de Sistemas

❑Gestión de la Demanda

- Gestión de la Demanda
- Cartera de Aplicaciones
- Cartera de Proyectos
- Gestión de Adquisición y externalización

❑Gestión del Servicio

- Gestión del Servicio
- Atención a Usuarios
- Disponibilidad del Servicio

❑Gestión de Proyectos

- Modelos de Gestión de Proyectos
- Gestión de Requisitos
- Gestión de Datos
- Desarrollo
- Pruebas
- Implantación

❑Monitorización y Soporte

- Gestión de Problemas e Incidencias
- Aseguramiento Calidad
- Gestión de Configuración y Cambios
- Gestión Documental
- Formación
- Gestión de Métricas
- Gestión de Riesgos

Hay diferentes tipos de métricas

- **Métricas de rendimiento: miden la eficiencia y ejecución de controles de seguridad**
  - Son mediciones sobre la actividad "normal"
  - Pe. tiempo medio para aprovisionar / desprovisionar una cuenta
- **Métricas operativas: miden el funcionamiento de los controles de seguridad**
  - A menudo son mediciones sobre eventos de seguridad
  - Pe. número de mensajes spam bloqueados esta semana
- **Métricas de negocio: miden el impacto en el negocio de los controles de seguridad, y la efectividad del programa de seguridad**
  - Pe. estimación de pérdida económica debida a caídas de la red corporativa

Hay diferentes tipos de métricas

- **Los cuatro "M"'s**
  - "Meaningful" – que sea relevante y tenga sentido para quien lo recibe
  - "Measurable" – comportamiento que se puede medir
  - "Monitorable" – dentro de o asociado con procesos reconocidos
  - "Manageable" – que exista un marco para gestionar lo medido
- **Métricas ≠ medición**
  - Métricas son el conjunto de los cuatro M's

Los roles que necesitan métricas de seguridad

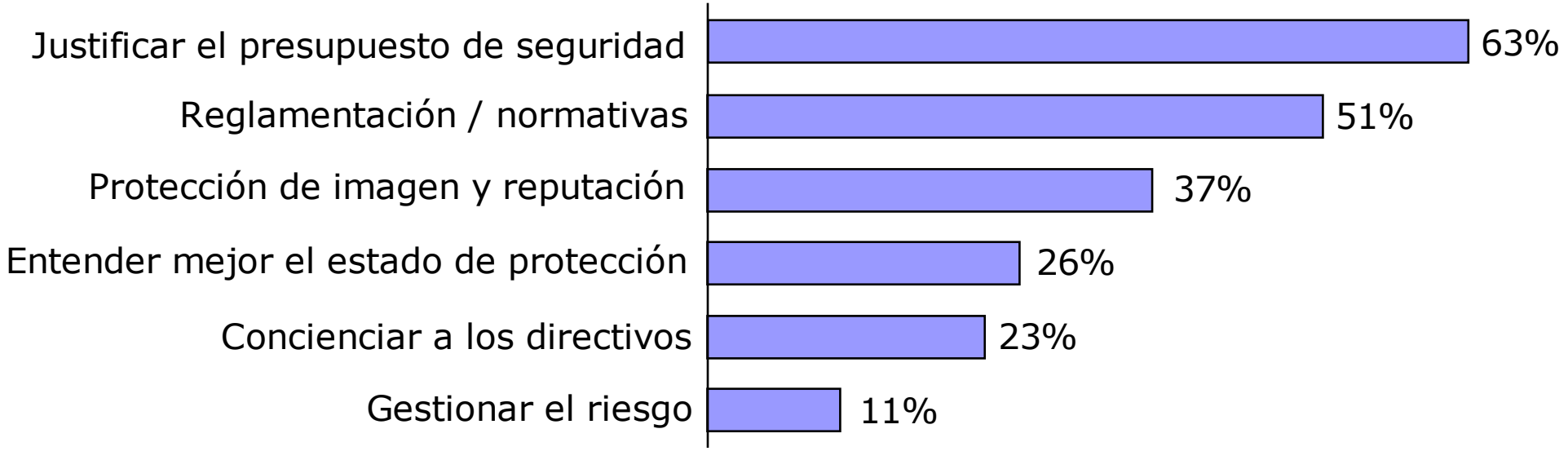
- **Gerentes tecnológicos y de seguridad**
  - Para justificar el presupuesto de seguridad
  - Para saber la evolución en la gestión de seguridad
- **Directores de unidades de negocio**
  - Para comparar el estado de su unidad con otras unidades dentro y fuera de la organización
- **El consejo y los stakeholders**
  - Para asegurar el cumplimiento de normativas y leyes
  - Para asegurar que la información de la organización es segura
  - Para asegurar que se obtenga valor del gasto en seguridad

Factores que impulsan las métricas de seguridad

FORRESTER®

March 2006, Best Practices **"Are We Secure Yet?"**

"¿Cuáles son sus tres principales objetivos en medir la seguridad de la información?"



(Pregunta hecha ante 40 CISO's y gerentes de seguridad, permitiéndose multiples respuestas)

Grupo TQS

El mapa de métricas de la organización

Para construir el mapa de métricas de seguridad propio de nuestra organización, tenemos que identificar las características y eventos que son medibles y que pueden ser determinantes en la toma de decisiones en diferentes niveles organizativos. Cada uno de los factores clave de nuestros procesos TI tendrá una o más métricas asociadas en la siguiente matriz.

	Personas	Procesos	Tecnología
Consejo y Stakeholders			
Dirección de Unidades de Negocio			
Responsables de Tecnología			

Métricas a nivel del consejo y los "stakeholders"

1. Responsabilidad para las iniciativas de Gestión de Riesgos y Cumplimiento de Normativa relacionadas con la seguridad de la información (pe., LOPD, Sarbanes-Oxley, normativa sectorial, etc.)

1.1. (B) Porcentaje de activos claves de información para los cuales se ha implantado una estrategia comprensiva para reducir los riesgos de la seguridad de la información, y mantener estos riesgos dentro de límites aceptables.

1.2. Porcentaje de funciones organizativas claves para las cuales se ha implantado una estrategia comprensiva para reducir los riesgos de la seguridad de la información, y mantener estos riesgos dentro de límites aceptables.

1.3. (B) Porcentaje de requerimientos externos claves que se considera que la organización cumple, en base a una auditoría objetiva u otro medio de comprobación.

2. Aprobación y adopción de los principios de un programa de seguridad de la información, y aprobación de la asignación de responsabilidades para las funciones que prevee el programa

2.1. Porcentaje de principios del programa de seguridad de la información para los cuales la Dirección ha implantado políticas y controles aprobados.

2.2. (B) (PYME) Porcentaje de roles claves de la seguridad de la información para los cuales se han asignado responsabilidades, líneas de reporting y autoridad, y se han identificado capacidades requeridas.

3. Esfuerzo para proteger los intereses de todos los "Stakeholders" que dependen de la seguridad de la

3.1. Porcentaje de reuniones de dirección / consejo y/o reuniones de comités donde la seguridad de la información figura en

3.2. (B) Porcentaje de incidencias de seguridad que no causaron daños, compromiso de la seguridad, o pérdidas más allá de los límites establecidos, para los activos, funciones, o stakeholders de la organización.

3.3. Estimación económica de los daños que han causado todas las incidencias de seguridad. (es deseable un valor menor)

4. Revisión de las políticas de seguridad de la información con respecto a socios estratégicos y otros

4.1. (B) Porcentaje de relaciones con socios estratégicos y otros terceros para las cuales se han implantado requisitos de seguridad de la información en los acuerdos y contratos.

5. Esfuerzo para asegurar la continuidad del negocio

5.1. (B) Porcentaje de unidades organizativas con un plan establecido para garantizar la continuidad del negocio

6. Revisión de provisiones para auditorías internas y externas del programa de seguridad de la información

6.1. (B) Porcentaje de auditorías internas y externas obligatorias que se han realizado y revisado por la Dirección / Consejo

6.2. (B) Porcentaje de conclusiones / recomendaciones de auditoría que han sido implantadas / resueltas

Fuente: NIST Corporate Information Security Working Group Report of the Best Practises and Metrics Teams, 2005

Grupo

Métricas a nivel de la dirección de unidades de negocio-1

8. Establecer políticas y controles de gestión de la seguridad de la información, monitorizar su grado de cumplimiento

8.1. (B) Porcentaje de elementos del programa de seguridad de la información para los cuales actualmente existan políticas y controles aprobados y operativos

8.2. (B) (PYME) Porcentaje de responsabilidades asignadas al personal, donde el personal ha reconocido esta responsabilidad para aspectos de las políticas o controles de seguridad, y realizan un reporting regular a sus superiores.

8.3. (B) Porcentaje de revisiones de cumplimiento de seguridad de la información donde no se han detectado incumplimiento

8.4. Porcentaje jefes de unidades de negocio y gerentes quienes han implantado procedimientos operativos para asegurar el cumplimiento con políticas y controles aprobados de seguridad de la información

9. Asignar roles, responsabilidades y capacidades necesarias de seguridad de la información, y asegurar que se utilicen privilegios de acceso basados en roles

9.1. (B) (PYME) Porcentaje de nuevos empleados contratados en este periodo que han realizado formación de concienciación en temas de seguridad antes de concederles acceso a la red corporativa

9.2. (B) (PYME) Porcentaje de empleados que han realizado formación periódica de actualización en temas de seguridad, de acuerdo con las políticas de seguridad

9.3. Porcentaje de descripciones de puestos que definen los roles, responsabilidades, capacidades y certificaciones de seguridad de la información para:

a. Gerentes y administradores de seguridad
b. Personal IT
c. Usuarios finales de sistemas

9.4. Porcentaje de evaluaciones de rendimiento y desempeño laboral que incluyen una valoración de responsabilidades de seguridad de la información y cumplimiento con la política de seguridad de la información

9.5. (B) (PYME) Porcentaje de roles de usuario, sistemas y aplicaciones que cumplan principios de segregación de funciones

9.6. (B) Porcentaje de individuos con acceso a software de seguridad que son administradores autorizados y formados de

9.7. (B) Porcentaje de individuos que pueden asignar privilegios de seguridad en sistemas y aplicaciones, que son administradores autorizados y formados de seguridad

9.8. Porcentaje de individuos cuyos privilegios de acceso han sido revisados durante el presente periodo

a. (B) (PYME) Empleados con privilegios que conceden un alto nivel de acceso a sistemas y aplicaciones
b. (B) (PYME) Empleados dados de baja en la organización

9.9. Porcentaje de usuarios para los cuales se han comprobado sus antecedentes laborales antes de contratarles o concederles acceso a la red y los sistemas

10. Valorar los riesgos para la información, establecer límites aceptables de riesgo, y gestionar activamente

Fuente: NIST Corporate Information Security Working Group Report of the Best Practises and Metrics Teams, 2005

Grupo

Métricas a nivel de la dirección de unidades de negocio-2

10. Valorar los riesgos para la información, establecer límites aceptables de riesgo, y gestionar activamente los riesgos

10.1. (B) (PYME) Porcentaje de activos críticos de la información y funciones dependientes en la información para las cuales se ha realizado y documentado algún tipo de valoración de riesgos, de acuerdo con las políticas de seguridad

10.2. Porcentaje de activos y funciones críticas para los cuales el coste de compromiso (pérdida, daño, no disponibilidad ...) ha sido cuantificado

10.3. (B) (PYME) Porcentaje de riesgos identificados que tienen definido un plan de reducción de riesgos cuyo estado está informado periódicamente, de acuerdo con políticas de seguridad

11. Asegurar la implantación de requisitos de seguridad de la información para socios estratégicos y otros

11.1. Porcentaje de riesgos conocidos para la información que están relacionados con relaciones con terceros (es deseable un valor menor)

11.2. (B) (PYME) Porcentaje de funciones o activos de la información críticos para los cuales no se permite acceso por parte de terceros

11.3. (B) (PYME) Porcentaje de personal de organizaciones terceras que actualmente tienen privilegios de acceso a la información, y cuya continuidad de acceso ha sido revisada y aprobada por la autoridad correspondiente en la organización, de acuerdo con la política de seguridad

11.4. (B) (PYME) Porcentaje de sistemas con funciones o activos de la información críticos para los cuales la conectividad por parte de sistemas de terceros no está permitida.

11.5. Porcentaje de incidencias de seguridad donde están involucrado personal de organizaciones terceras (es deseable un

11.6. Porcentaje de acuerdos con terceros que incluyen / demuestran la verificación independiente de políticas y

11.7. (B) (PYME) Porcentaje de relaciones con terceros que han sido revisadas para asegurar su cumplimiento de requisitos de seguridad de la información

11.8. Porcentaje de debilidades detectadas y áreas de no-cumplimiento en revisiones y auditorías, que han sido corregidas desde la última revisión

12. Identificar y Clasificar los Activos de la Información

12.1. (B) (PYME) Porcentaje de activos de información que han sido revisado y clasificado por el propietario asignado, de acuerdo con el esquema de clasificación establecido por la política de seguridad

12.2. Porcentaje de activos de la información con privilegios definidos de acceso que han sido asignados, basándose en roles y de acuerdo con las políticas de seguridad

p12.3. Porcentaje de inventarios programados de activos que ocurren según el calendario previsto, de acuerdo con las políticas de seguridad

Fuente: NIST Corporate Information Security Working Group Report of the Best Practises and Metrics Teams, 2005

Grupo

Métricas a nivel de la dirección de unidades de negocio-3

13. Implantar y probar los planes de continuidad de negocio

13.1. (B) Porcentaje de unidades organizativas con un plan de continuidad de negocio documentado para los cuales se han asignado responsabilidades específicas

13.2. (B) Porcentaje de planes de continuidad de negocio que han sido revisados, probados y actualizados, de acuerdo con las políticas de seguridad

14. Aprobar la arquitectura de sistemas de información, durante su adquisición, desarrollo, operaciones y mantenimiento

14.1. Porcentaje de riesgos para la seguridad de la información relacionados con la arquitectura de sistemas, que han sido identificados en la valoración más reciente de riesgos, y que han sido adecuadamente tratados / solucionados / limitados /

14.2. (B) Porcentaje de cambios en la arquitectura de sistemas que han sido revisados en cuanto a su impacto en la seguridad, aprobados por la autoridad correspondiente y documentados mediante formularios de solicitud de cambios

14.3. Porcentaje de funciones o activos críticos de información que estén instalados en sistemas que actualmente cumplen con la arquitectura aprobada de sistemas

15. Proteger el entorno físico

15.1. (B) (PYME) Porcentaje de funciones o activos críticos de información que han sido revisados desde la perspectiva de riesgos físicos tales como el control de acceso físico y la protección física de media de copias de respaldo

15.2. Porcentaje de funciones o activos críticos de información de la organización expuestos a riesgos físicos para los cuales se han implantado medidas de mitigación de riesgos

15.3. (B) (PYME) Porcentaje de activos críticos que han sido revisados desde la perspectiva de riesgos ambientales, como temperatura, fuego, inundación, etc.

15.4. Porcentaje de servidores en ubicaciones con control de acceso físico

16. Asegurar auditorías regulares internos y externos del programa de seguridad de la información, con un seguimiento asiduo

16.1. (B) Porcentaje de requisitos de seguridad de la información aplicables que figuran en legislación y regulaciones, y que están incluidos en programas de auditoría interna y externa

16.2. (B) Porcentaje de auditorías internas o externas de seguridad de la información realizadas con programas de trabajo

16.3. (B) Porcentaje de acciones de la Dirección acordadas en respuesta a recomendaciones de auditoría, que fueron implantadas de acuerdo dentro del calendario previsto y de manera completa

Fuente: NIST Corporate Information Security Working Group Report of the Best Practises and Metrics Teams, 2005

Grupo

Métricas a nivel de áreas técnicas - 1

18. Identificación y autenticación de usuarios

18.1. (B) (PYME) Número de identificativos activos de usuarios que están asignados a una sola persona física

18.2. (B) (PYME) Porcentaje de sistemas y aplicaciones que realizan verificación de contraseñas contra la política o normativa de contraseñas

18.3. (B) (PYME) Porcentaje de contraseñas que están configurados para expirar de acuerdo con las políticas de seguridad

18.4. Porcentaje de sistemas con activos de información críticos que utilizan una autenticación más fuerte que simplemente una verificación de identificativo y contraseñas, de acuerdo con la política

19. Gestión de Cuentas de Usuarios

19.1. (B) (PYME) Porcentaje de sistemas donde los datos de conexión (cuentas y contraseñas) de por defecto han sido desactivados o modificados

19.2. (B) (PYME) Porcentaje de cuentas asignadas a personal que se ha dado de baja en la organización o que ya no tiene necesidad de acceso a los sistema, y que han sido cerradas

19.3. (B) Porcentaje de sistemas con parámetros de bloqueo de cuentas configurados, de acuerdo con la política de

19.4. Porcentaje de cuentas inactivas de usuario que han sido desactivadas de acuerdo con la política de seguridad

19.5. (B) (PYME) Porcentaje de estaciones de trabajo con controles de bloqueo de sesión o de desconexión automática en base a tiempo de inactividad, y de acuerdo con la política de seguridad

20. Privilegios de Usuario

20.1. (B) (PYME) Porcentaje de cuentas activas de sistemas, que han sido revisadas para justificar los privilegios actuales de acceso, de acuerdo con la política de seguridad

20.2. (B) (PYME) Porcentaje de sistemas donde se limita la posibilidad de instalar software no-estándar, de acuerdo con la política de seguridad

20.3. Porcentaje de sistemas y aplicaciones donde la asignación de privilegios de usuario cumple con la política que especifica los privilegios de acceso a la información en base a roles.

21. Gestión de Configuraciones

21.1. Porcentaje de sistemas para los cuales se han implantado parámetros autorizados y aprobados de configuración, de acuerdo con la política de seguridad

21.2. (B) (PYME) Porcentaje de sistemas con configuraciones que no se desvían de estándares autorizados o aprobados

21.3. (B) (PYME) Porcentaje de sistemas cuyo cumplimiento con la política de configuración se monitoriza de manera continua, generando – en su caso – alarmas o informes sobre situaciones de incumplimiento

21.4. Porcentaje de sistemas cuya configuración se compara con valores de referencia reconocidos y establecidos previamente, de acuerdo con la política de seguridad

21.5. (B) Porcentaje de sistemas donde la autoridad para realizar cambios a las configuraciones se limita, de acuerdo con la política de seguridad

Fuente: NIST Corporate Information Security Working Group Report of the Best Practises and Metrics Teams, 2005

Grupo

Métricas a nivel de áreas técnicas - 2

22. Registro en logs y monitorización de eventos y actividad

22.1. (B) Porcentaje de sistemas para los cuales se ha implantado el registro en logs de eventos y actividad, de acuerdo con la política de seguridad

22.2. (B) (PYME) Porcentaje de sistemas para los cuales se monitoriza y se revisan los logs de eventos y actividad, acuerdo con la política de seguridad

22.3. Porcentaje de sistemas para los cuales se ha implantado un determinado volumen de información y ciclo de retención, de los logs

22.4. (B) Porcentaje de sistemas que generan alertas sobre actividad anómala o potencialmente no autorizada

23. Comunicaciones, Correo electrónico, y Seguridad en el Acceso Remoto

23.1. (B) (PYME) Porcentaje de portátiles y dispositivos móviles que requieran una comprobación de cumplimiento con una política aprobada de configuración, antes de concederles acceso a la red corporativa.

23.2. Porcentaje de canales de comunicaciones controlados por la Organización que han sido securizados, de acuerdo con la política de seguridad

23.3. Porcentaje de servidores host que están protegidos contra su explotación para el reenvío de comunicaciones no

23.4. Porcentaje de usuarios itinerantes y remotos que accedan a recursos telemáticos de la organización mediante comunicaciones protegidas

24. Protección contra Código Malicioso, incluyendo Virus, Gusanos y Troyanos

24.1. (B) (PYME) Porcentaje de puestos de trabajo (incluyendo portátiles) con una protección automática contra código malicioso, de acuerdo con la política de seguridad

24.2. (B) (PYME) Porcentaje de servidores con protección automática contra código malicioso, de acuerdo con la política de

24.3. (B) (PYME) Porcentaje de dispositivos móviles con protección automática contra código malicioso, de acuerdo con la política de seguridad

25. Gestión de Cambios en Software, incluyendo Parcheos

25.1. (B) (PYME) Porcentaje de sistemas con todos los parcheos oficiales actuales instalados

25.2. Tiempo medio desde la notificación por parte de un proveedor de la disponibilidad de un parcheo, hasta su instalación, por entorno tecnológico (es deseable un valor menor)

25.3. (B) Porcentaje de cambios en software, cuyos impactos de seguridad han sido estudiados antes de efectuar el cambio

Fuente: NIST Corporate Information Security Working Group Report of the Best Practises and Metrics Teams, 2005

Grupo

Métricas a nivel de áreas técnicas - 3

26. Cortafuegos

26.1. (B) (PYME) Porcentaje de cortafuegos personales, en servidores host, entre segmentos de red interna, y de perímetro, que han sido configurado de acuerdo con la política de seguridad

27. Encriptación de Datos

27.1. (B) Porcentaje de activos de información críticos que se almacenan en dispositivos accesibles desde la red, y que están encriptados con algoritmos criptográficos públicos que han sido comprobados extensivamente

27.2. (B) (PYME) Porcentaje de dispositivos informáticos móviles que emplean encriptación para los activos de información críticos, de acuerdo con la política de seguridad

27.3. Porcentaje de contraseñas y PIN's que se encriptan (con una función "one-way hash"), de acuerdo con la política de

28. Respaldo y Recuperación

28.1. (B) (PYME) Porcentaje de sistemas con activos o funciones de información críticas para las cuales se confeccionan copias de respaldo, de acuerdo con la política de seguridad

28.2. (B) (PYME) Porcentaje de sistemas con activos o funciones de información críticas, cuya recuperación a partir de copias de respaldo ha sido probado exitosamente

28.3. (B) (PYME) Porcentaje de medios de almacenaje de respaldo que se almacenan fuera del centro de cálculo, en condiciones seguras

28.4. Porcentaje de medios de almacenaje que, tras su utilización, la organización les "sanea" (sobrescribir a bajo nivel) antes de reutilizarlos o desahacerse de ellos

29. Detección y Respuesta a Incidencias y Vulnerabilidades

29.1. (B) Porcentaje de tiempo operativo con indisponibilidad de servicios críticos para usuarios / clientes, debido a incidencias de seguridad (es deseable un valor menor)

29.2. (B) (PYME) Porcentaje de incidencias de seguridad que explotan vulnerabilidades existentes, existiendo soluciones conocidas, parches o arreglos ("workarounds"). (es deseable un valor menor)

29.3. Porcentaje de sistemas afectados por incidencias de seguridad donde se han explotado vulnerabilidades existentes, existiendo soluciones conocidas, parches o arreglos ("workarounds"). (es deseable un valor menor)

29.4. (B) Porcentaje de incidencias de seguridad que han sido gestionadas y resueltas de acuerdo con políticas, procedimientos y procesos establecidos

29.5. (B) (PYME) Porcentaje de sistemas con activos o funciones de información críticas, y cuyas vulnerabilidades han sido valorados, de acuerdo con la política de seguridad

29.6. (B) (PYME) Porcentaje de recomendaciones generadas a partir de valoraciones de vulnerabilidades, que han sido tratados desde el último periodo de reporting

Fuente: NIST Corporate Information Security Working Group Report of the Best Practises and Metrics Teams, 2005

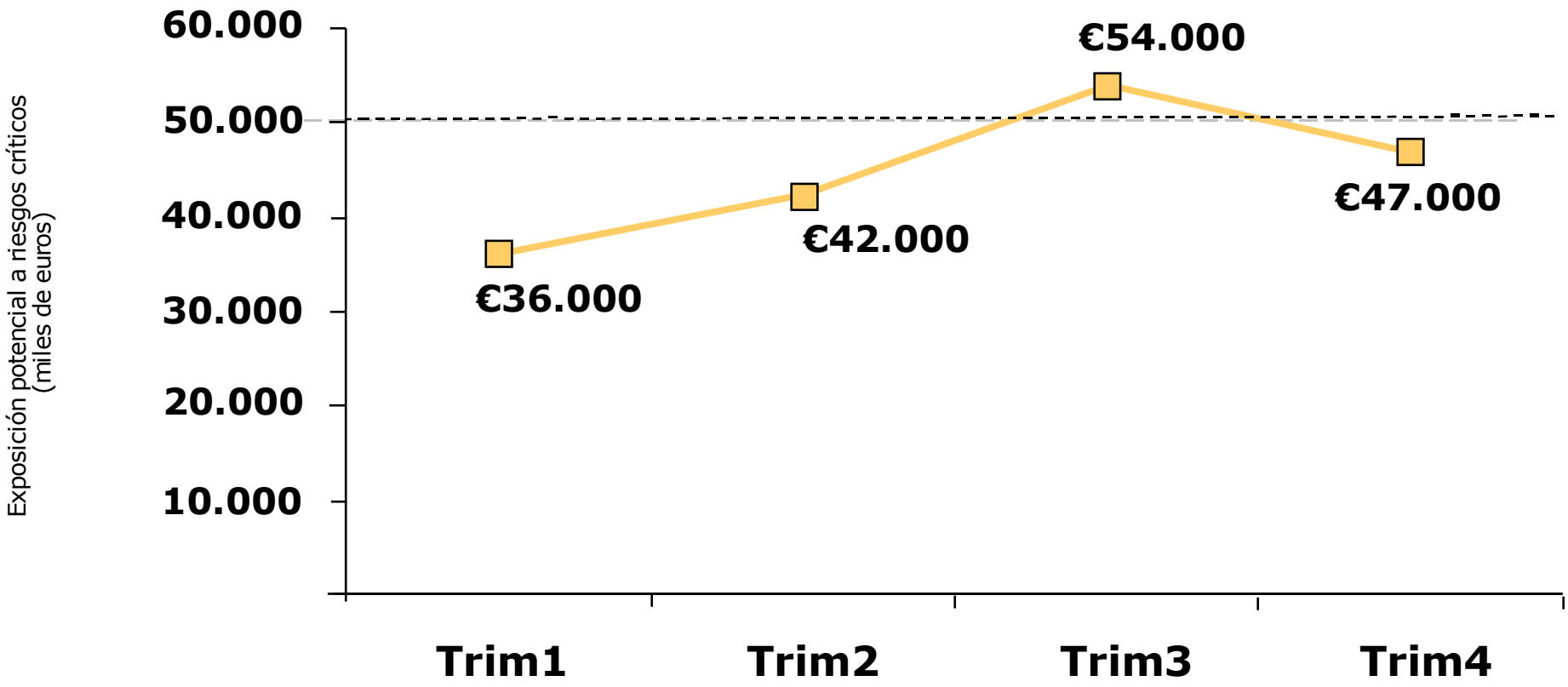
Grupo

Métricas como input a un cuadro de mando

Métrica: Impacto en el negocio de todos los riesgos críticos

3. Objetivo:
   - Mantener la suma de los riesgos críticos < €50,000
4. Medición:
   - Suma del impacto de todos los riesgos críticos (prob. * exposición)
   - Riesgo1 (€4,000) + Riesgo2 (€24,000) + Riesgo3 (€13,000) + . . .
5. Tendencia:
   - Trim1 = €36,000
   - Trim2 = €42,000
   - Trim3 = €54,000
   - Trim4 = €47,000

Métricas como input a un cuadro de mando



Justificación: no se consiguió el objetivo de riesgo aceptable en el tercer trimestre, debido a la implantación de la nueva aplicación de RRHH, que no se sometió (por razones de mercado) a los debidos controles de seguridad.

La gestión integrada de TI y de sus riesgos ...

La gestión integrada de TI y de sus riesgos ...

Gestión de Riesgos, Seguridad y Continuidad				*Organización y Planificación*	
COBIT	**ISO 9000**	**EFQM**	**CMMI / ISO 15504**	**ITIL / ISO 20000**	**ISO 17799:2005**
PO9- Assess Risk, DS4-Ensure Continuous Service, DS5-Ensure Systems Security	ISO 90003 Secciones 7.2.2.2 y 7.3.2		Risk Management	6.3 Gestión de contiuidad 6.6 Gestión de la seguridad	Controles en secciones 5 - 15

Objetivo

Identificar, prevenir y mitigar los riesgos que afectan al logro de los objetivos de TI, para **asegurar que las actividades de TI se realizan de forma continua y segura** pudiendose reestablecer tras la activación de un riesgo y que éste no afecte al logro de los objetivos de TI ni de la empresa, proporcionando confianza, credibilidad y ventajas competitivas.

Factores clave

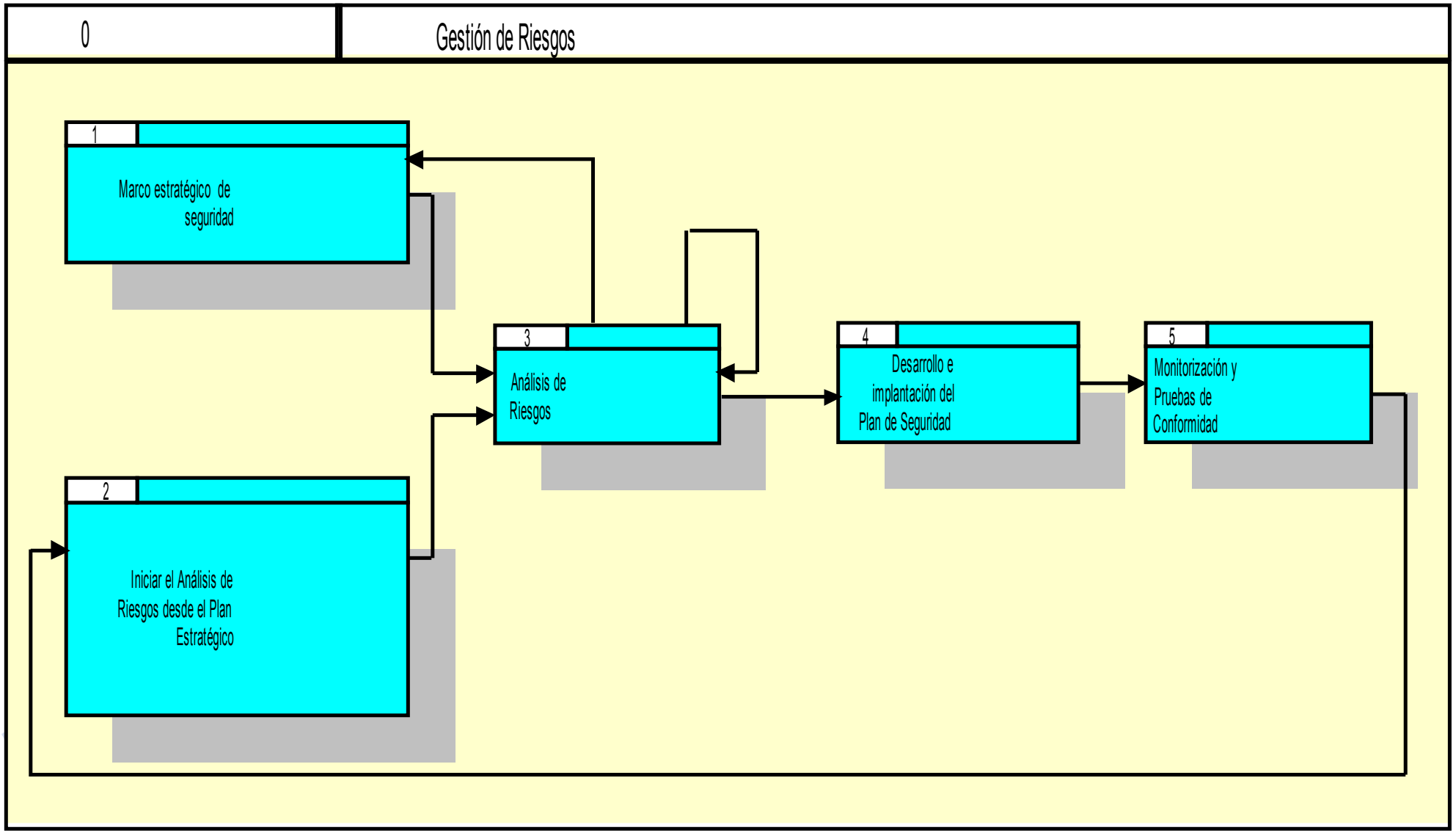
- Considerar la identificación, evaluación, priorización y monitorización de los riesgos posibles en todos los ámbitos incluyendo la seguridad y continuidad.
- Identificar el origen de los riesgos, sus categorías e impacto sobre los objetivos de TI y la prestación de servicios al negocio.
- Valorar el impacto global en el negocio de los principales riesgos de servicios IT.
- Determinar acciones de prevención y mitigación de los riesgos, así como de recuperación tras la activación del riesgo si llegase a producirse.
- Incluir niveles de tolerancia y aceptación de riesgos, así como la asignación de las funciones y responsabilidades en los procedimientos de actuación.
- Revisar periódicamente el estado de los riesgos, identificando nuevos riesgos y actualizando procedimientos y acciones.

... es un circulo cerrado

Grupo TQS

El lugar de las métricas en la gestión de los riesgos

Los procesos de gestión de los riesgos empiezan con la piedra angular que es el marco estratégico de seguridad de la organización. La realización de actividades de análisis de riesgos da lugar a las acciones contínuas de mejora y control de los riesgos. Es en el proceso de monitorización que se ubican la utilización de métricas de seguridad



Conclusión

El estado de la seguridad ...

- ***Es dificil definir el concepto de "seguridad buena"***
- ***Es dificil distinguir entre "seguridad" y "suerte"***
- ***No sabemos medir para luego poder mejorar (internamente) o comparar (externamente)***
- ***Una incidencia no significa un fracaso / la ausencia de incidencias no significa un éxito***

Se puede trabajar sobre cada uno de estos puntos ...

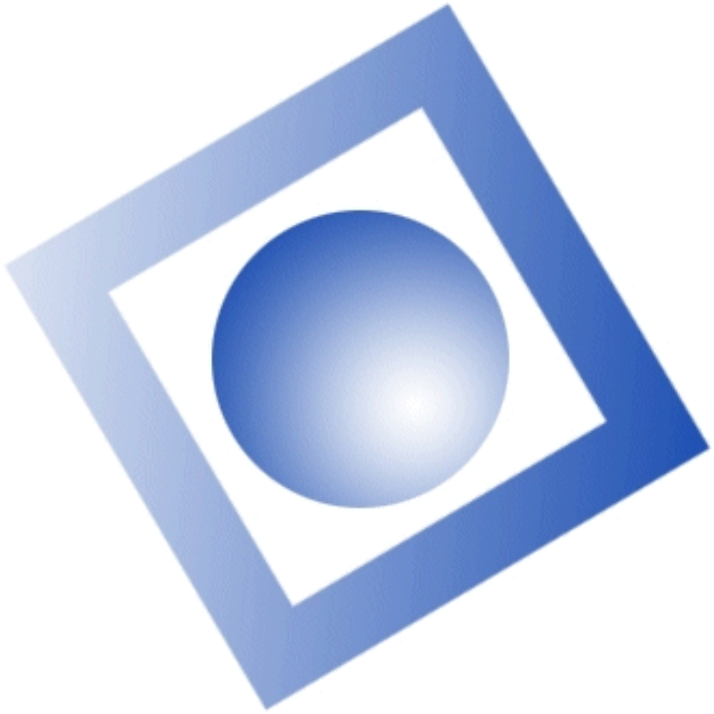
Grupo TQS

Próximos pasos ...

- **El Grupo de Seguridad de AEMES va a realizar una encuesta sobre métricas de seguridad**
- **Se distribuirá a empresas interesadas en participar**
- **Se analizará y publicará los resultados**
  - **En todo momento asegurando la confidencialidad y anonimidad de la información aportada**
- **Estaríamos encantados contar con la participación de organizaciones miembros y no miembros de la AEMES**

Grupo TQS

Para más información ...



En TQS contamos con el "know how" y la experiencia adecuada para ayudar a integrar la gestión de los servicios tecnológicos de su organización.

Nuestro reto es de facilitar que nuestros clientes puedan dedicar todo el tiempo necesario a sus negocios, y que los servicios que dan soporte a los procesos de negocio funcionan de la manera más eficaz posible.

Quedamos a su entera disposición para cualquier pregunta o información relacionada con nuestros servicios.

Douglas Wagner

Grupo TQS

C/ Chile 4, edificio II, oficina 20
28290 Las Rozas. Madrid
Tel: 916368020

tqs@tqs-es.com

w w w . tqs-es . c o m

Cámara Madrid
Servicio de Certificación
EMPRESA CERTIFICADA
ISO 9001
EC - 1.470.0603