

# ***Resumen y Conclusiones CSTIC 2012***

### Patrocinadores



### Colaboradores



# Ponencias

## La Continuidad del negocio frente a los riesgos de desastre

Juan Bautista Pérez Mínguez. MINISTERIO DE DEFENSA

- Para garantizar la continuidad de negocio requiere una gestión adecuada de los riesgos durante la vida de un servicio, desde su puesta en marcha, hasta su retirada o su transición.
- Cómo nos podemos apoyar en distintas normas y modelos para conseguir que se consigan los resultados de la organización, sobre todo a nivel empresarial
- Hemos visto el modelo de ciclo de vida de un producto TI en el ministerio de Defensa, en 5 capas.

## Análisis y gestión de Riesgos. Herramienta PILAR

José Luis Quintero Villarroya. MINISTERIO DE DEFENSA

- Hemos visto la evolución histórica de la Seguridad TI, hasta el momento actual en el que el análisis y gestión de riesgos son el juicio fundamental para considerar el adecuado nivel de seguridad.
- Nos ha presentado la metodología MAGERIT y su automatización a través de herramientas.

# Ponencias

## Una visión incremental del riesgo: de MAGERIT a CMMI

Ramiro Carballo CAELUM

- Cómo institucionalizar la gestión de los riesgos en una organización, apoyando la técnica particular de Magerit con las prácticas organizacionales.

## Habilidades humanas para gestionar los riesgos TI

Inmaculada Barea ATOS

- La ponente expone su experiencia profesional sobre la importancia de las capacidades que deben tener los roles asignados a realizar las tareas de gestión de riesgos. Dicho de otra manera, nos ayuda a descubrir os riesgos que tiene asignar inadecuadamente la responsabilidad de gestión de riesgos dentro de una organización TI



# Ponencias

## SOLVENCIA II y Gestión del Riesgo TI en las compañías de seguros Francisco Javier Baena. DIRECCIÓN GENERAL DE SEGUROS

- Es una Directiva que cambia las normas europeas del Seguro para mejorar el control y medición de los riesgos (de mercado, operacionales, de crédito y de liquidez) a los que están expuestas las aseguradoras.
  - Pilar I: Medida de activos, pasivos y capital.
  - Pilar II: Proceso de Supervisión.
  - Pilar III: Requerimientos de transparencia
- Guía de Apoyo a la Supervisión Tecnológica basada en el Gobierno Corporativo TI.



# Mesa Redonda sobre Riesgos en Proyectos

## Concepción Torrijos, Jefe de Proyecto en INSA. Ponencia: Gestión de Riesgos en Proyectos

Conchita ha presentado la metodología de gestión de riesgos en proyectos de INSA, donde se considera como riesgo cualquier tipo de incertidumbre, tanto positivas como negativas. Se consideran distintas fuentes de riesgos tipificadas. Los riesgos se tienen en cuenta desde la fase de la propuesta. Posteriormente se sigue un ciclo de gestión desde la identificación hasta el seguimiento y control.

## Juan Félix Castela, Subdirección General TIC del Ministerio de Defensa. Ponencia: Riesgos detectados en la función inspectora de un Proyecto

Félix ha presentado la actividad de inspección de riesgos durante el ciclo de vida de los proyectos tecnológicos del Mº de Defensa. Cada fase de un proyecto tiene uno o varios hitos de inspección. Los 4 riesgos típicos detectados son los riesgos de financiación, de rotación de recursos humanos, de aprovisionamiento y de ejecución. Félix ha concluido que la calidad final de un proyecto depende de la correcta gestión del riesgo durante el ciclo de vida.





# Mesa Redonda sobre Riesgos en Proyectos

Antonio Moya, VP del Comité CSTIC AEC. Ponencia: Gestión de Riesgos en Proyectos, un modelo sencillo y eficaz

Para Antonio, gestión de riesgos es lo contrario a gestión de crisis. A través de un caso práctico, nos ha ido explicando de una forma sencilla conceptos de gestión de riesgos como: diferencia entre riesgo y hecho, balance entre riesgo y coste de calidad, gestión cualitativa y cuantitativa, etc. Para Antonio es clave que la alta dirección sea consciente de los riesgos en los proyectos, y para ello los Project Managers deben comunicar los riesgos usando un lenguaje financiero.



# Mesa Redonda sobre Riesgos en Cloud

## Nuevos modelos de servicios Cloud. Impacto en la seguridad

César Franco HP

Nos ha puesto al corriente de las novedades en los modelos de servicio que vienen y donde tenemos que poner el foco a la hora de intentar garantizar la seguridad.

## Principales amenazas en Cloud Computing

Cristina Fernández GRUPO SMS

Con la amplia experiencia internacional de Cristina, esta exposición nos ayudará a identificar los riesgos que supone un proyecto de Virtualización , y donde se han identificado potenciales soluciones que mitiguen el impacto de las amenazas típicas en este tip de proyectos.



# Mesa Redonda sobre Riesgos en Cloud

## Gestión de riesgos energéticos en un Datacenter

Carmen García TISSAT

Cómo se gestionan los riesgos de un datacenter en función de la necesidad de servicio que requiere el negocio de los clientes, considerando costes, agilidad, gestión eficiente y activos. En concreto, se ha tratado la gestión de la energía, no sólo como riesgo, sino como coste del negocio

## Moderniza 6.0: Plan de Modernización de los Ayuntamientos de la provincia de Alicante.

Adrián Ballester DIPUTACIÓN PROVINCIAL DE ALICANTE.

Donde hemos podido valorar las funcionalidades compartidas que estos servicios proporcionan a distintas entidades locales, y que convierten a la Administración Pública española en ejemplo para otros países.





# Mesa Redonda sobre Riesgos en Cloud (análisis)

- 1. Cuándo y cómo vamos al Cloud.** La cuestión cada vez menos es si es útil o aporta valor. La cuestión es elegir correctamente el proveedor de servicios, que ofrezca adaptación a las diferentes necesidades, y la flexibilidad suficiente para variar los balances entre diversas soluciones públicas y privadas y poder revertir decisiones de migración que se hayan tomado.
- 2. Proveedores de servicios Cloud.** Es fundamental medir, a través del cumplimiento de normativas y pruebas por parte del proveedor, su capacidad para satisfacer los requisitos que se planteen, que deberán quedar correctamente reflejados en los SLA,s sin que ello implique caer en la “cautividad” con el proveedor. Además, es fundamental la información de seguimiento de los servicios que, en tiempo real, proporcione el proveedor.
- 3. Cuestiones culturales asociadas al Cloud.** Todavía existen barreras de tipo cultural hacia el Cloud Computing, fundamentalmente derivadas de que se trata de servicios intangibles frente a la realidad tangible de tener el servidor, el CPD o el equipo TIC dentro de la propia empresa.
- 4. Carácter internacional.** Dado que en un servicio Cloud suelen intervenir diversas entidades y es frecuente que su origen sea diverso, hay que tener en cuenta el cumplimiento de todas las normativas nacionales de los clientes por parte de todos los actores independiente de su país de ubicación.
- 5. Regulaciones asociadas al Cloud.** Se está haciendo, a nivel internacional, un importante esfuerzo de unificación de todas las normativas aplicables, tanto surgidas ex novó como ya consolidadas. Es importante mejorar la presencia española en los foros donde se está llevando a cabo esta labor, de modo que nuestras peculiaridades puedan ser escuchadas y tenidas en cuenta.

# CSTIC 2012

Dominando los riesgos se compite mejor

18 de Septiembre de 2012

#CSTIC12



## Patrocinadores



## Organizador



## Patronos de la AEC:



## Colaboradores



## Cooperadores

