cloud security alliance
CSA
SPANISH CHAPTER

cloud security alliance
CSA
SPANISH CHAPTER

I Encuentro Cloud Security Alliance-ES

Governance Risk and Compliance en la Nube

29 de Noviembre de 2010
Barcelona

ISMS Forum Spain
ASOCIACIÓN ESPAÑOLA PARA EL FOMENTO DE LA SEGURIDAD DE LA INFORMACIÓN

Índice

1. CSA Internacional
2. CSA- ES
3. Grupos de Trabajo CSA-ES

CSA Internacional

- Organización internacional sin ánimo de lucro.

- Objetivo
  - Promover un nivel de entendimiento entre consumidores y proveedores de cloud.
  - Promover el desarrollo de guías y buenas practicas independientes.
  - Lanzar campañas de concienciación y sensibilización sobre el uso adecuado y seguro de la nube.

- + 11.000 asociados, +60 empresas.

- 6 capítulos internacionales constituidos y 9 en proceso de constitución.

CSA Internacional

Documentación desarrollada

Security Guidance for Critical Areas of Focus in Cloud Computing Foundational best practices for securing cloud computing Download Version 2.1 (English), released December 17, 2009 Download Identity & Access Management Whitepaper - Released April 27, 2010 Download Application Security Whitepaper - Released July 28, 2010 Go to Guidance page (other languages, deprecated versions)	**Controls Matrix** Security controls framework for cloud provider and cloud consumers Download Version 1.01 (English), released October 20, 2010 Download Version 1.0 (English), released April 27, 2010 Go to Controls Matrix page (other file formats) Sign up for Working Group
Consensus Assessments Initiative Research tools and processes to perform consistent measurements of cloud providers Download Version 1.0 (English), released October 12, 2010 Go to Consensus Assessments Initiative page (more information and other file formats) Sign up for Working Group	**Cloud Metrics** Metrics designed for Cloud Controls Matrix and CSA Guidance Sign up for Working Group
Trusted Cloud Initiative Secure, interoperable identity in the cloud Download Identity & Access Management Whitepaper Go to Trusted Cloud page Sign up for Working Group	**Top Threats to Cloud Computing** Threat research updated twice yearly Download Top Threats Report V1.0 Go to Top Threats page Sign up for Working Group
CloudAudit (10/20/2010: Now a CSA project!) The goal of CloudAudit is to provide a common interface and namespace that allows cloud computing providers to automate the Audit, Assertion, Assessment, and Assurance (A6) of their infrastructure (IaaS), platform (PaaS), and application (SaaS) environments and allow authorized consumers of their services to do likewise via an open, extensible and secure interface and methodology. Go to website	**Common Assurance Maturity Model (partner project)** Provide an objective framework for transparently benchmarking capabilities to deliver information assurance maturity of a selected solutions across ones supply chain. Broad coalition including ENISA and CSA Go to website

Accesible gratuitamente en www.cloudsecurityalliance.org

ISMS Forum Spain
ASOCIACIÓN ESPAÑOLA PARA EL FOMENTO DE LA SEGURIDAD DE LA INFORMACIÓN

CSA Internacional

Top Threats to cloud Computing v1.0

- Threat #1: Abuse and Nefarious Use Of Cloud Computing
- Threat # 2: Insecure Interfaces and APIs
- Threat #3: Malicious Insiders
- Threat #4: Shared Technology Issues
- Threat #5: Data Loss or Leakage
- Threat #6: Account or Service Hijacking
- Threat #7: Unknown Risk Profile

CSA-ES

- Primer capítulo “nacional” del CSA a nivel mundial.

- Constituida el pasado 21 de mayo 2010 bajo el amparo del ISMS Forum y Barcelona Digital.

- Cada capítulo regional tiene un ámbito específico de interés en relación con el cómputo en Nube. En este sentido, el Capítulo Español tendrá, inicialmente, como área de interés el “**Cumplimiento Normativo en la Nube**”.

- 91 asociados fundadores, actualmente 170 asociados.

CSA-ES

Organización y órganos de gobierno

1. Junta Directiva.
2. Consejo Asesor.
3. Comité Operativo.
4. Asamblea.
5. Grupos de Trabajo

CSA-ES

Junta Directiva

Constituida formalmente el pasado Viernes 21 de Mayo de 2010 con la siguiente estructura:

- Vocales:
  - Carlos Saiz, Ecija
  - Casimiro Juanes, Ericsson
  - Gianluca D´ Antonio, FCC
  - Jesús Luna, Barcelona Digital
  - Nathaly Rey, ISMS Forum
  - Victor Villagrá, UPM
  - Elena Maestre, PWC
  - Ramón Miralles, APDCAT

- Vicepresidente y Secretario:
  - Jesús Milán, Bankinter

- Presidente:
  - Luis Buezo, HP

CSA-ES

Consejo Asesor

Órgano de alto nivel formado por expertos propuestos por la Junta Directiva, cuyo objeto será asesorar y proponer planes de acción e interlocución con las autoridades de control, todo ello enmarcado en el desarrollo de las tres líneas de actividad fundacionales de la asociación.

Constitución del Comité Asesor con la siguiente estructura:

- Máximo de 6 miembros
- Equilibrio entre fabricantes, prestadores de servicios, administraciones públicas y usuarios.

Miembros actuales:

- Marcos Gómez HIdalgo, Subdirector programas de INTECO.
- Olof Sandstrom, DG. Operaciones Arsys
- Pau Contreras, Dir. Innovación y Desarrollo de negocio ORACLE Ibérica

CSA-ES

Comité Operativo

Órgano de gobierno de la asociación cuyo cometido será el diseño, implantación y seguimiento en el día a día de las directrices y acuerdos alcanzados por la Junta Directiva en sus reuniones plenarias.

Constitución del Comité Operativo con la siguiente estructura:

- Presidente y vicepresidente del CSA-ES.
- 1 Representante del Comité Asesor.
- 2 miembros de la Junta Directiva.

CSA-ES

Asamblea

La Asamblea es el órgano supremo de decisión y gobierno del capítulo y está por la totalidad de los miembros.

Grupos de Trabajo

Constitución de 3 grupos de trabajo enfocados al desarrollo del "*Compliance Report*".

- Privacidad y Cumplimiento normativo en la nube (transferencias internacionales de datos, estándares internacionales, auditorias, subcontrataciones, etc.)

- *SGSI y Gestión de Riesgos en la nube* (Continuidad de los servicios, SLA's, Responsabilidades, Mapa de riesgos, certificaciones, etc.)

- *Contratación, evidencias electrónicas y auditoria en la nube (Propiedad intelectual, finalización de la relación, contacto con autoridades, auditorias, responsabilidades, etc.)*

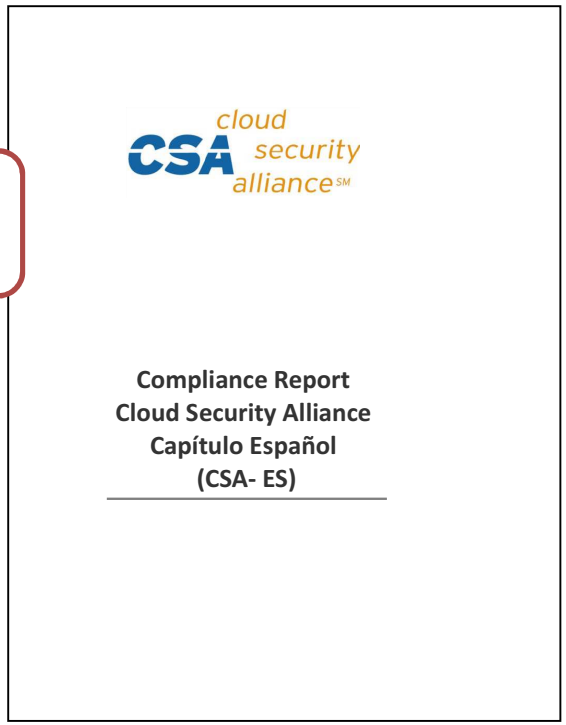
Cada grupo tiene15 miembros y un líder.

CSA-ES

Calendario de Actividades 2010-2011

- Informe anual: **Compliance Report**
  - Español/inglés.

Esquema Report	Primera versión	Publicación
Noviembre 2010	Marzo 2011	Junio 2011



- Eventos anuales:
  - I Encuentro CSA-ES. Governance Risk and Compliance en la nube (29-11-2010 Barcelona)
  - TBC (2011)

- Reuniones trimestrales abiertas.

CSA-ES

Siguiente sesión

16:15 Conferencia	***"Privacidad, SGSI, Contratación y Evidencias en la Nube. La visión de CSA-ES"*** ***Intervienen:*** **ANTONIO RAMOS**, Líder del grupo de trabajo 'SGSI y Gestión de Riesgos' de **CSA-ES** y Consultor independiente. **MARIA LUISA RODRÍGUEZ**, Líder del grupo de trabajo 'Contratación, Evidencias Electrónicas y Auditorías' de **CSA-ES** y Security Business Manager en **Barcelona Digital Technology Centre**. **MIGUEL ÁNGEL BALLESTEROS**, Líder del grupo de trabajo 'Privacidad y Cumplimiento Normativo' de **CSA-ES** y Auditor en **CEPSA.** **Modera: JESÚS LUNA**, Co-fundador de **CSA-ES** y Security Researcher en **Barcelona Digital Technology Centre.**

CSA-ES

Siguiente sesión

17:30 Mesa Redonda	***"El control de las autoridades de protección de datos en la nube"*** ***Intervienen:*** **EMILIO ACED**, Subdirector General de la **Agencia de Protección de Datos de la Comunidad de Madrid.** **PEDRO ALBERTO GONZÁLEZ**, Responsable del Registro de Ficheros y NNTT de la **Agencia Vasca de Protección de Datos.** **RAMON MIRALLES**, Coordinador de Auditoría y Seguridad de la Información de la **Autoridad Catalana de Protección de Datos.** **Modera: CARLOS ALBERTO SÁIZ**, Área Governance, Risk & Compliance de **ECIJA** y Vicepresidente de **ISMS Forum Spain.**
18:30	**JIM REAVIS**, Director de **Cloud Security Alliance.**

ASOCIACIÓN ESPAÑOLA PARA EL FOMENTO DE LA SEGURIDAD DE LA INFORMACIÓN

CSA-ES

GT 1: Privacidad y Cumplimiento normativo en la nube

Misión:

- Proporcionar una respuesta adecuada a los interrogantes que presenta el uso de la nube respecto de la privacidad de la información.

Visión:

- La privacidad y el cumplimiento normativo no constituyan una barrera.
- Usuarios y los proveedores de servicios tengan una referencia de los deberes y las obligaciones que conlleva utilizar la nube.
- Dar respuesta a las personas físicas afectadas por el uso de la nube en el manejo de sus datos personales.

Objetivos:

- Determinar la legislación aplicable al Cloud Computing.
- Estudiar los problemas y proponer soluciones y buenas prácticas.
- Detectar lagunas legislativas y proponer cambios legislativos.
- Proponer sistemas de verificación de las soluciones adoptadas.

Alcance:

- El alcance inicial será la legislación española sobre protección de datos.

CSA-ES

GT 2: SGSI y Gestión de Riesgos en la nube

Misión:
- Definir unas mejoras prácticas para la realización de análisis de riesgos e implantación de Sistemas de Gestión de la Seguridad de la Información.

Visión:
- Facilitar la implantación de SGSIs y análisis de riesgos a los clientes y proveedores de servicios en la nube
- Los SGSIs dentro del Cloud serán un derecho común y necesario.

Objetivos:
- Desarrollar guías y orientaciones para usuarios y proveedores de servicios

Alcance:
- Introducción a los SGSI y análisis de riesgos en Cloud Computing.
- Análisis de riesgos en entornos de Cloud Computing
- Identificación de procesos y activos
- Identificación y valoración de amenazas
- Análisis y valoración de impactos
- Pilares básicos de los SGSIs y el Cloud Computing

CSA-ES

GT 3: Contratación, evidencias electrónicas y auditoria en la nube

Misión:
- Asesorar a las empresas usuarias de servicios Cloud en los ámbitos relacionados con la contratación, auditoría y gestión de las pruebas electrónicas.

Visión:
- Servir como fundamento a la hora de elegir proveedores y gestionar los contratos de los servicios Cloud

Objetivos:
- Identificar la problemática en materia de contratación, auditoría y gestión de las evidencias electrónicas
- Establecer referencias para las condiciones de contratación.
- Establecer referencias para las tecnologías y metodologías de auditoría.
- Establecer referencias para la gestión de las evidencias electrónicas que pudieran surgir como resultado de algún incidente en los servicios contratados.

Alcance:
- Aspectos legales y normativas relacionadas
- Tecnologías y metodologías de auditoría