

Conclusiones del VII Encuentro del Capítulo Español de Cloud Security Alliance

28 de noviembre – IE Business School de Madrid (Calle María de Molina, 11)

- **Jim Reavis**, Co-founder and Chief Executive Officer de Cloud Security Alliance presentó la cuarta edición de las “Guías de seguridad de áreas críticas en Cloud Computing”, considerada un documento clave, a nivel internacional para la adopción del cloud.

Madrid, 28 de noviembre. El capítulo español de Cloud Security Alliance celebró su séptimo encuentro de profesionales de la seguridad en Cloud Computing el **28 de noviembre** en el Aula Magna del IE Business School de Madrid (Calle María de Molina, 11. Madrid. Este séptimo encuentro tuvo más de 150 asistentes.

Esta séptima edición del Encuentro de CSA ES contó con los principales representantes institucionales, así como de la Industria y expertos en la materia, para abordar la eminente adopción empresarial de servicios en la Nube, haciendo hincapié en la confiabilidad y seguridad, y en el marco regulatorio que envuelve la Nube.

El acto estuvo inaugurado por **Gianluca D’Antonio**, presidente de ISMS Forum Spain, director académico del IE Master of Cybersecurity y Chief Information Officer del Grupo FCC, acompañado de **Mariano Benito**, coordinador del Comité Técnico Operativo de Cloud Security Alliance y **Teresa Ramos**, directora del área de tecnología del IE Business School.

La ponencia inaugural estuvo a cargo de **Jim Reavis**, Co-founder and Chief Executive Officer de Cloud Security Alliance. Jim fue el encargado de presentar la cuarta edición de las “Guías de seguridad de áreas críticas en Cloud Computing”, considerada una referencia a nivel internacional sobre seguridad y privacidad en la nube. A lo largo de la guía se pueden encontrar dominios tales como Cloud Computing y arquitectura e infraestructura de la nube, un dominio a destacar es el área legal donde el GDPR es un punto muy importante. En el estudio también se abordó el ámbito de Compliance teniendo en cuenta el marco regulatorio que envuelve la nube. Asimismo, se ha estudiado cómo se debe mantener el ciclo de vida del dato sin perder el gobierno de la información ya que hay que entender la información que proviene desde la nube. En cuanto al plan de management y continuidad de negocio se ha buscado crear un nuevo conocimiento de la seguridad. De la misma manera ha ocurrido con la infraestructura de seguridad y en este punto hay que entender un nuevo modelo de cloud y adoptar a la nueva y actual plataforma devOps. En palabras de Jim, “La seguridad en el dato y la encriptación del mismo es primordial en la información almacenada en la nube.” Reavis, concluyó diciendo que “La seguridad como servicio y las tecnologías relacionadas como el Big Data, Internet of Things, mobile computing, entre otras, son el futuro.”

Entre los principales keynotes, **Mauricio Monti**, EMEA Channel & Partner Manager de Cloudflare, presentó los últimos ataques DDoS y el impacto social y económico en la sociedad. Ha presentado varios ejemplos entre los que destaca el ataque que sufrió Hong Kong antes del referéndum y Cloudflare lo detectó. Otro caso práctico fue el de eurovisión en 1965 donde se envió un aviso de ayuda a Cloudflare. Estos ataques DDoS se miden en Mbps. Entre los elementos de los ataques DDoS ha destacado el atasco de información. “Los ataques se han ido incrementando debido a la fuerza y la sofisticación que existe en la actualidad”.

Kai Roer, Security culture specialist, author and speaker y miembro de Cloud Security Alliance Norway, puso de manifiesto la importancia de la cultura de la seguridad como componente indispensable en la gestión empresarial. Roer hizo un énfasis especial en resaltar que el factor humano es muy importante en todos los aspectos y en particular en la computación en la nube. “Es un error pensar que el ser humano no tiene nada que ver con la computación en la nube” concluyó Kai en su ponencia del VII Encuentro de profesionales de la nube.

Por su parte, **Adenike Cosgrove**, Cybersecurity Strategy EMEA de Proofpoint, explicó su visión sobre cuál es la mejor manera de securizar todos los aspectos que rodean Office 365. A lo largo de su ponencia explicó que los ataques para robos de identidad se sofistican cada vez más vía email. También los emails fraudulentos han aumentado notablemente desde el tercer trimestre del año anterior hasta el día de hoy. De la misma manera, subrayó que alrededor del 90% de emails con enlaces fraudulentos fueron enviados de manera intencionada para captar información y así, comprometer la privacidad del dato. Adenike concluyó su ponencia diciendo que “la industria no está alineada con las amenazas a las que estamos expuestos y nuestro gran reto es que esto se modifique.”

Una mesa redonda titulada “Security breaches from in house to cloud” reunió a los principales proveedores de seguridad para analizar el nivel de seguridad y confiabilidad, así como los riesgos y amenazas asociados al entorno Cloud, y la necesidad de implementar medidas de seguridad como forma de afrontar las barreras para la adopción de servicios en la Nube. Esta mesa estuvo moderada por Casimiro e integrada por expertos profesionales del sector cloud como **Luis Corrons**, director del Laboratorio de Panda Labs en Panda Security, “sin nube sería inviable el uso y el trato masivo de datos”; **Javier Larrea**, Sr. Sales Engineer en Forcepoint, “Tenemos dos tipos de usuarios, aquellos que de forma malintencionada hacen un uso indebido de la información y aquellos que no. Una ventaja importante de la nube es que se puede utilizar para compartir información y datos. Uso masivo de datos y gran velocidad de actualización”; **José Luis Laguna**, director técnico en Fortinet ha apuntado que las organizaciones están migrando servicios con información menos sensible a la nube para vencer la barrera de falta de confianza con respecto a la nube. “Tenemos que gestionar la seguridad de este modelo híbrido en la nube para satisfacer a nuestros clientes”; **Marc Rodriguez**, experto en ciberseguridad de Trend Micro, “Hay una transición clara a los entornos de la nube. Necesitamos un punto central de gestión de agregación, así como visibilidad y control”; **Alejandro Fernández**, especialista en soluciones de Gestión de Identidades, Gobierno de Datos y Accesos en Sailpoint, “el cliente tiene que elegir cuál es el tipo de plataforma que necesita ya que estamos ante un modelo híbrido.”

El Encuentro continuó con otra mesa redonda titulada “Giving an access to the bad guy” donde se abordó la seguridad centrada en las identidades y accesos, y la gestión de los mismos, como forma de garantizar la protección de la información asegurando que el usuario es quien dice ser y que accede de manera autorizada, facilitando asimismo el cumplimiento normativo y generando mejoras en el servicio e incluso creando nuevas oportunidades de negocio. Esta mesa ha estado compuesta por **Ricardo Rodríguez**, country Manager Spain, Italy and Portugal en CenturyLink, “Todas las empresas utilizan el cloud y el almacenamiento en la nube” **José María Cayuela**, security Specialist Senior en Akamai, “Las redes de bonnets son muy útiles para el robo de identidad y por ello hay que securizar al máximo posible a través de los programas disponibles;” **Roberto Baratta**, global Executive VP and Director of Loss Prevention, Business Continuity and Security en Abanca; “La gestión de identidades es una función muy compleja. Los retos que asume una gran empresa son gestionar cantidades ingentes de identidades y a esto se le suma la identidad que se gestiona con los dispositivos y, por último, la gestión y gobierno de estos dos pasos anteriores.” **Adolfo Hernández**, advance Cyber Defense Manager Banco Sabadell;” Todo va orientado a la gestión de identidades y a sus soluciones habilitadas para la correcta utilización en la nube.” En esta ocasión, la mesa ha estado moderada por **Luis Ballesteros**, CISO de WiZink.

Durante el segundo bloque de contenidos se presentaron dos estudios realizados por Cloud Security Alliance España: **Cloud Control Matrix v3 (versus Esquema de Seguridad Nacional v2 (ENS) (RD 951/2015))** y la **V Edición del Estudio del Estado del Arte de la Seguridad en la Nube**.

La presentación del primer estudio corrió a cargo de **Miguel Ángel Amutio**, Subdirector Adjunto de Coordinación de Unidades TI de la Secretaría General de Administración Digital, Ministerio de Hacienda y Función Pública, y **Jorge Laredo**, Miembro del Comité técnico operativo de Cloud Security Alliance España. La Tercera Edición de la Cloud Control Matrix ha tenido como objetivo impulsar la adopción de servicios de Cloud en España, permitiendo tanto el cumplimiento normativo como la seguridad efectiva de los datos para las empresas. Esta guía ha recogido los aspectos de seguridad necesarios en la computación en la nube y considera la relación del Esquema Nacional de Seguridad con las normas y estándares de gestión adaptados al mismo. Es un marco de 133 controles cuyo objetivo es impulsar la adopción de servicios de cloud en España. Como conclusiones importantes, Jorge sentenció que tan solo un 10% de los controles de CCM no tienen correlación con los datos previamente mencionados.

El segundo estudio se ha presentado de la mano de la **Mariano J. Benito**, coordinador del Comité Técnico Operativo del Cloud Security Alliance, junto con **Josep Bardallo**, CISO de Grupo Recoletas, Director de Ciberseguridad de SVT Cloud y Miembro del Comité Técnico Operativo de Cloud Security Alliance España. El objetivo de este estudio ha sido explorar y conocer el estado del arte de la adopción de servicios Cloud, y el papel que juega la seguridad en la adopción de esta tecnología, desde la perspectiva de los usuarios. También ha identificado las expectativas en seguridad que tienen los usuarios en los servicios en la Nube, su satisfacción con dichos servicios, la disponibilidad de información y certificaciones a su alcance en la adopción de estos servicios, los modelos y servicios más demandados, así como otros resultados obtenidos por la adopción de servicios en la Nube.

Asimismo, durante la presentación destacaron que “Shadow IT sigue siendo un aspecto de gran interés dentro del estudio habiendo una posición de mayor conocimiento y menor permisividad o tolerancia hacia el fenómeno, se ha impulsado a los Departamentos de TI a mejorar la calidad de sus servicios hasta igualar los percibidos por los usuarios de ShadowIT.” También señalaron que la concienciación en el mundo del cloud computing es baja y continúa la tendencia de años atrás.

Como conclusiones acerca del estudio Mariano y Josep concluyeron diciendo que la satisfacción se debe incrementar, los requisitos relevantes ya han sido identificados, el alto impacto de GDPR, y por último, “tener un conocimiento más exhaustivo acerca del compliance y el marco regulatorio que envuelve la nube.”



Sobre Cloud Security Alliance España

El capítulo español de Cloud Security Alliance (CSA-ES) reúne a miembros representativos de la industria del Cloud Computing en España. Se trata de un foro de debate que promueve el uso de buenas prácticas para garantizar la seguridad y privacidad en el entorno del Cloud Computing, siendo una de sus áreas de interés específico el Compliance en la Nube. CSA-ES contribuye al desarrollo de conocimiento en materia de seguridad y cumplimiento en la nube por medio de estudios propios y de terceros, así como a través de la organización de Encuentros de Cloud Security Alliance España, a la vez que promueve la guía de las mejores prácticas de seguridad cloud que publica el Cloud Security Alliance Global. ISMS Forum y CSA-ES han impulsado la primera certificación profesional en castellano sobre Seguridad de la Información en Cloud Computing, el Certificate Of Cloud Security Knowledge (CCSK).

Sobre ISMS Forum Spain

La Asociación Española para el Fomento de la Seguridad de la Información, ISMS Forum Spain, es una organización sin ánimo de lucro fundada en enero de 2007 para promover el desarrollo, conocimiento y cultura de la Seguridad de la Información en España y actuar en beneficio de toda la comunidad implicada en el sector. Creada con una vocación plural y abierta, se configura

como un foro especializado de debate para empresas, organizaciones públicas y privadas, investigadores y profesionales donde colaborar, compartir experiencias y conocer los últimos avances y desarrollos en materia de Seguridad de la Información. Toda su actividad se desarrolla en base a los valores de transparencia, independencia, objetividad y neutralidad.

ISMS Forum Spain tiene ya a más de 150 empresas asociadas y más de 900 profesionales asociados. La Asociación es ya, por tanto, la mayor red activa de organizaciones y expertos comprometidos con la Seguridad de la Información en España.

Comunicación ISMS Forum

91.563.50.62 – Marta Cueto Martínez-Pontrémuli

comunicacion@ismsforum.es

Síguenos en [@ISMSForumSpain](https://www.instagram.com/ISMSForumSpain) y LinkedIn [ISMS Forum Spain](https://www.linkedin.com/company/ISMS-Forum-Spain)