RESPUESTAS SIC

Barcelona: 16 de noviembre de 2010
(Hotel Rey Juan Carlos I)

Madrid: 18 de noviembre de 2010
(Hotel NH Eurobuilding)

La evolución de los servicios de SOC

Seguridad a medida

Inscripciones:

- Acceso gratuito previa solicitud de inscripción
- Solicitud: www.revistasic.com/respuestassic

> AFORO LIMITADO

Organiza:

Revista SIC seguridad en informática y comunicaciones

Copatrocinan:

accenture High performance. Delivered. · ECIJA Derecho y Tecnología · Ironwall · Symantec. · Telefónica

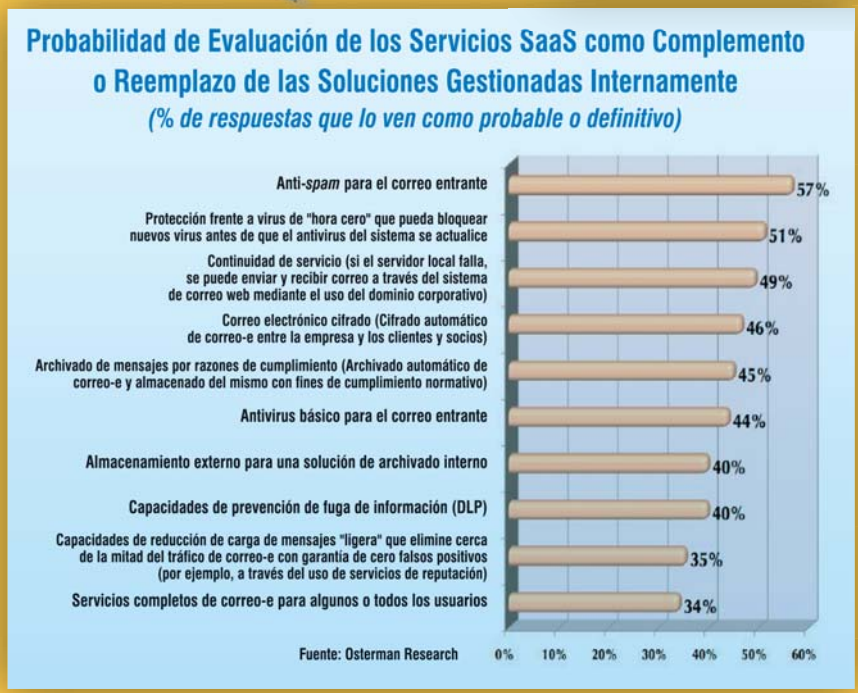
La evolución de los servicios de

El proceso de agrupamiento de funciones de seguridad en Centros de Operaciones específicos *(Security Operations Center-SOC)*, iniciado hace años en los entornos de grandes organizaciones, obedece a la búsqueda de la eficiencia. Las TIC y su uso intensivo, además, han sido el catalizador fundamental de este hecho, y particularmente el control de riesgos de seguridad de la información en red, un entorno endiabladamente dinámico y de protagonismo galopante. De hecho, muchos SOC internos y de prestadores han nacido o son en origen NSOC *(Network Security Operations Centers)*.

Lo cierto es que estos hechos han forzado a la redefinición de lo que se entiende por seguridad en las empresas y de quién o quiénes debe depender su gestión, cuestiones esenciales a la hora de optar por la centralización de funciones y aspectos capitales para entender el alcance real de la denominada convergencia de las seguridades, del papel y perfil profesional de los CSO y los CISO, y factor determinante para fijar e ir evolucionando las funciones y alcances de tal o cual SOC.

Este devenir no ha sido ajeno a la mirada de las firmas proveedoras de servicios de TIC, que a tenor de los tiempos, marcados por la externalización, han ido creando líneas para dar solución a las necesidades de sus clientes (tengan éstos formalmente o no SOC): seguridad en red, servicios de seguridad gestionados, servicios de SOC, servicios de oficina operativa, servicios administrados... que llámense como se llamen abarcan la monitorización de plataformas, el análisis y la gestión de *logs*, la correlación, la detección de vulnerabilidades, el parcheado, el análisis forense, la capacidad de respuesta, la intervención, la gestión de derechos digitales, la gestión de identidades y accesos, la prevención de fraude, la inspección de tráfico... Una lista interminable.

El reto del conocimiento



Servicios gestionados

¿Nube?

SOC compartido

MSSP

Contrato

Convergencia

A medida

Industrialización

XaaS

SOC: Seguridad a medida

Pero, ciertamente, dichos servicios, no pocos generales y de "primera" generación, han de evolucionar conforme madura la función de gestión de riesgos de seguridad en las organizaciones y conforme aparecen nuevos escenarios (XaaS y "La Nube", por ejemplo). Y ello implica una labor activa por parte de cada proveedor especializado para diferenciar su oferta y para adaptarse al usuario en su totalidad, en cada una de sus partes y en sus relaciones con socios y clientes, sean cuales sean los mercados en donde opere.

Éste es el asunto que se plantea en esta sesión: ni más ni menos que la evolución de los servicios de SOC para alcanzar el objetivo de una seguridad a medida.

Contenido

El Respuestas SIC se estructurará en base a sus tres bloques tradicionales. En el primero, dos expertos en la materia, en este caso de las firmas **Ernst & Young** y **blueliv**, enfocarán el tema propuesto, intentando aportar claves para el desarrollo de nuevos servicios de interés en base a varias concepciones de la seguridad.

En el segundo bloque se profundizará en los actuales catálogos de servicios y en los planes para su evolución de cinco jugadores destacados: **Accenture**, **Ecija**, **Ironwall (Grupo Mnemo)**, **Symantec** y **Telefónica**.

En el tercer y último bloque, tres expertos en seguridad del **CTTI de la Generalitat de Cataluña**, **Mapfre** y **RSI-Rural Servicios Informáticos** darán su visión y debatirán sobre el asunto propuesto.

Programa

09:00h. Acreditación y entrega de documentación.

LAS CLAVES DEL FUTURO

09:30h. **El papel de los SOC en la búsqueda de la eficiencia en la gestión de seguridad.**

Rafael Ortega García, Socio de Advisory. **Ernst & Young.**

10:10h. **SOC: nuevos servicios, servicios inteligentes.**

Daniel Solís Agea, Director de Operaciones. **blueliv.**

10:40h. Coloquio.

APROXIMACIONES DE LOS PRESTADORES Y PROVEEDORES

10:50h. **Accenture**.

Javier Martín Barroso, Security Senior Manager.

11:10h. **Ecija**.

Abel González Lanzarote, Director de Desarrollo de Negocio.

11:30h. Pausa-café.

12:00h. **Ironwall (Grupo Mnemo)**.

Fernando García Vicent, Director General.

12:20h. **Symantec**.

David Fernández Granado, Responsable de Desarrollo de Negocio de Servicios de Seguridad Gestionada.

12:40h. **Telefónica**.

Juan Miguel Velasco López-Urda, Director Asociado de Servicios y Proyectos de Seguridad de Telefónica España.

13:00h. Coloquio general.

MESA REDONDA

13:15h. **La visión de los usuarios. Escenarios actuales, limitaciones y necesidades.**

Participantes:

Tomás Roy Catalá, Director del Área de Calidad, Seguridad y Relaciones con Proveedores. Centro de Telecomunicaciones y Tecnologías de la Información (CTTI). **Generalitat de Cataluña.**

Daniel Largacha Lamela, Subdirector del Centro de Control General (CCG) y Análisis Forense. **Mapfre.**

Pedro Pablo López Bernal, Gerente de Infraestructura de Seguridad, Auditoría y Normalización. **Rural Servicios Informáticos.**

14:30h. Almuerzo para todos los asistentes.

* Revista SIC se reserva el derecho a modificar el contenido o los ponentes de este programa si las circunstancias así lo requieren.

Seguridad a medida

La concepción que cada organización tenga de la gestión de riesgos y de la seguridad es, junto al sector de actividad en el que opera, factor determinante para que en ella se establezca y evolucione un modelo específico de SOC con un catálogo de servicios determinado y una mayor o menor propensión a la apuesta por fórmulas de externalización.

- ¿Qué concepción de la seguridad sustenta la consolidación de funciones de seguridad en un SOC único corporativo?
- ¿Es posible alcanzar una convergencia efectiva de las "seguridades" que ofrezca eficiencia y valor a una organización sin consolidar funciones en un SOC gestionado por profesionales de distintas áreas, y muy especialmente de TIC?
- ¿Es necesario para cualquier gran organización disponer de un SOC en el que se centralicen las funciones de seguridad?
- ¿Se vislumbran hoy necesidades que aconsejen evolucionar la naturaleza, alcance, calidad y particularización de los servicios de SOC actuales?
- ¿Qué papel han de jugar los fabricantes y desarrolladores de herramientas tecnológicas en la construcción de nuevos servicios de seguridad que puedan prestarse desde SOC externos?

El SOC como punto único de servicio

La fina observación del proceso de maduración de la función de gestión de riesgos de seguridad en las organizaciones debería permitir a los prestadores avezados vislumbrar la pertinencia de ir investigando nuevos servicios de SOC que puedan rentabilizarse, y que en contraposición a los actuales, lógicamente generales y básicos, deberían ser muy específicos, acotables y a medida de cada entidad en su totalidad y de cada una de sus partes, sean éstas unidades, direcciones, áreas o departamentos.

Los enfoques de SOC de usuarios finales coinciden en tratar información que haga posible controlar riesgos de actividad y de negocio. Ese es su valor primigenio. Y por ahí parece que hay que ir, en la medida en que [illegible] mente son los profesionales de [illegible] llevar cachiporra) los que [illegible] sando la tan cacareada conver[illegible] haciendo efectivos en mu[illegible] las disciplin[illegible] de contro[illegible] gestión.

- ¿Qué efectos puede tener "La Nube" como catalizadora de la evolución de los servicios de SOC?
- ¿Qué modelos de SOC internos hay? ¿Hasta qué punto puede "marcar" el modelo el sector de la economía en el que opere el usuario?
- ¿Qué nuevas necesidades de protección van a ir apareciendo con el avance de la Red y cómo van a afectar a la evolución y creación de servicios de seguridad prestados desde SOC externos?
- ¿Obligará a los proveedores la evolución del mercado a tener que especializar sus SOC de servicios en áreas concretas de la seguridad?
- ¿Qué nuevos actores pudieran tomar cuerpo en la prestación de servicios de seguridad en red y gestionados a tenor de la evolución de las TIC?
- ¿Qué efectos tendrá la legislación sobre protección de infraestructuras críticas en orden a potenciar la existencia de SOC sectoriales con servicios concretos o la interconexión de SOC?

RESPUESTAS SIC

La evolución de los servicios de SOC

LUGAR Y FECHAS

- **BARCELONA: 16 de noviembre de 2010**
  Hotel Rey Juan Carlos I.
  Avda. Diagonal, 661-671. 08028 Barcelona
- **MADRID: 18 de noviembre de 2010**
  Hotel NH Eurobuilding.
  C/ Padre Damián, 23. 28036 Madrid

ORGANIZA

Revista SIC. Ediciones CODA.
C/ Goya, 39. 28001 Madrid
Tel.: 91 575 83 24
info@revistasic.com www.revistasic.com

SOLICITUD DE INSCRIPCIÓN GRATUITA

El procedimiento para la solicitud de la inscripción es vía web mediante la cumplimentación de un formulario. Al ser el aforo limitado, la inscripción se cursará por riguroso orden de fecha de entrada de solicitud.

Sitio web: www.revistasic.com/respuestassic

- Una vez realizada la solicitud, la organización le informará –por razones de limitación del aforo– si ha quedado inscrito o no.
- En ningún caso se admitirán más de dos inscripciones de profesionales de una misma compañía.
- La sesión incluye documentación, café y almuerzo.