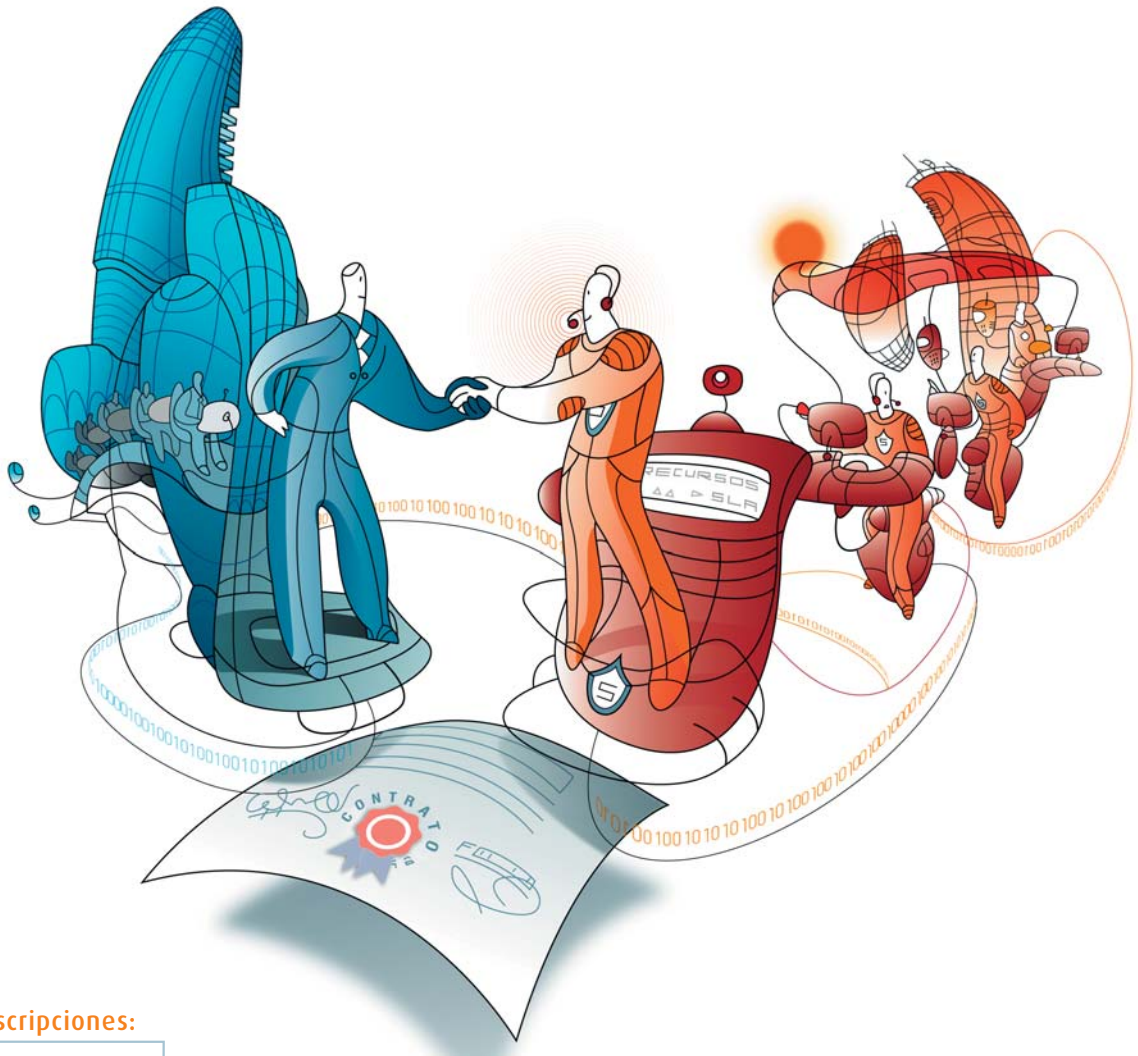
RESPUESTAS SIC

16 de octubre de 2007
Hotel NH Eurobuilding
Madrid

Servicios desde SOC

Seguridad gestionada por terceros en red



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. · Internet Security Systems, an IBM Company · sia · S21sec · VeriSign · symantec. · Telefónica

RESPUESTAS SIC

Seguridad gestionada por

El próximo 16 de octubre tendrá lugar una nueva edición de Respuestas SIC, evento periódico organizado por la publicación en donde se abordan asuntos de la máxima relevancia centrados en el campo de las tecnologías y servicios orientados a la protección de la información. En esta tercera edición de 2007 –sexta ya desde que esta iniciativa fuera convocada por SIC–, centrada en la seguridad gestionada por terceros desde la red, Respuestas SIC volverá a celebrarse en el Hotel Eurobuilding de Madrid en sesión matinal, y estará copatrocinada por las compañías **Accenture**, **Grupo SIA, IBM Internet Security Systems**, **S21sec-VeriSign**, **Symantec** y **Telefónica**.

Desde hace años, los agentes que conforman el mercado de TIC han estado profundizando en distintas alternativas de externalización, creando modelos de prestación que han partido de servicios básicos de seguridad en red, como pueden ser los centrados en la administración de cortafuegos y la defensa frente a código malicioso y *spam*, hasta llegar a otros más sofisticados que requieren de una relación contractual y operativa de grano fino entre el cliente y el prestador: gestión de vulnerabilidades, análisis y gestión de *logs*, correlación de eventos, gestión de identidades y acceso seguro, *backup*, respaldo ante contingencias, prevención del fraude...

Es un hecho que el tipo de servicios existentes no es cerrado, y que éstos pueden prestarse en distintos niveles, en distintos grados de amplitud, especialización y "paquetización", y directamente por fabricantes con redes de Centros de Operaciones de Seguridad (SOC - *Security Operations Centers*), o por integradores y operadores globales de TI, que bien mediante acuerdos con fabricantes que disponen de SOC o por disponer ellos de este tipo de centros (sea por creación interna o por la vía de las

Externalización en red

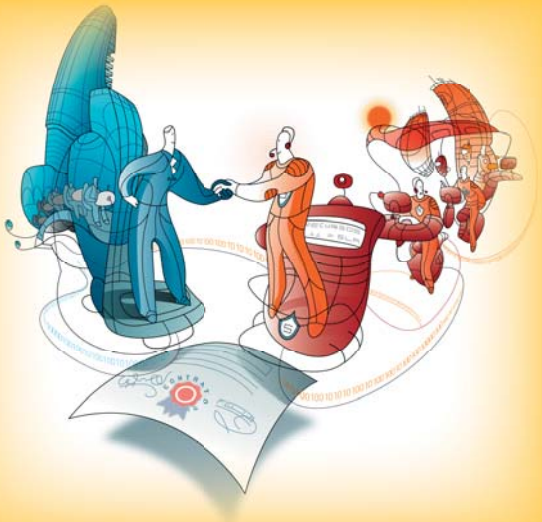
Gestión de la seguridad

Cómo gestiona la seguridad, monitoriza, logs, etc.	SI	NO	NS/NC
• Herramientas freeware o productos OSSIM, NESSUS...	46,2%	38,5%	15,4%
• Las certificaciones y modelos como estándar de gestión de Seguridad ISO 27001, ITIL WebTrust	42,3%	34,6%	23,1%
• Integración de gestión de seguridad - consolas únicas y UTM	61,5%	23,1%	15,4%
• Dispone de métricas y sistema de valoración de riesgo	38,5%	38,5%	23,1%
Identificación de recursos dedicados, internos y externos (outsourcing)			
• Implantación de SOC propio o de terceros	65,4%	15,4%	19,2%
• Recursos dedicados de seguridad o complementarios con Sistemas y Operaciones	76,9%	3,8%	19,2%
• Integración de servicios externos y/o profesionales de empresas terceras	57,7%	15,4%	26,9%
Tendencias			
• Evolución de UTM en appliance	30,8%	26,9%	42,3%
• Utilización de appliance de seguridad	38,6%	23,1%	38,5%
• Implantación de herramientas de correlación y gestión de logs y seguridad	69,2%	15,4%	15,4%
• Virtualización de plataformas de seguridad	34,6%	30,8%	34,6%

Externalización

La externalización como paliativo de la complejidad de la gestión de seguridad	SI	NO	NS/NC
• ¿Estaría dispuesto a externalizar o ya ha externalizado aspectos de seguridad?	53,8%	19,2%	26,9%
De los siguientes aspectos de seguridad, ¿cuál externalizaría?			
• Infraestructuras de seguridad	50,0%	26,9%	23,1%
• Gestión y monitorización de la seguridad	50,0%	26,9%	23,1%
• Administración y operación de la seguridad	57,7%	19,2%	23,1%
• Definición de políticas y estrategia	3,8%	73,1%	23,1%
• Externalización total	3,8%	76,9%	19,2%

Fuente: Estudio Sintra 2006 de Afina sobre la externalización de seguridad en red en el mercado español.



Fuente: Estudio "El estado de la seguridad en el suministro de servicios de las operadoras" de ISS. 2006.

terceros en red desde SOC

adquisiciones), han ido perfilando modelos cuya proyección de futuro es proporcionar una oferta a medida de cada cliente, sea o no en el contexto de servicios más generales de CPD.

En todo caso, la externalización de servicios de seguridad en red y desde la red es una de las grandes vías del mercado de protección TIC, a la que los analistas vaticinan un crecimiento espectacular y por la que están apostando fuertemente grandes prestadores y fabricantes.

Como es habitual, esta edición de Respuestas SIC se dividirá en tres bloques: en el primero, y mediante una conferencia de un consultor especializado de **GMV Soluciones Globales Internet**, se tratará de realizar una taxonomía de lo que hoy se entiende por servicios de seguridad prestados por terceros en red, se intentará definir qué hay que entender por SOC y qué operaciones de seguridad le son propias, se procederá a la discusión del siempre espinoso asunto de la fijación de criterios para el establecimiento bilateral de acuerdos de nivel de servicio y tratamiento de excepciones, y se expresarán las diferencias que pudieran existir entre los servicios ofrecidos por fabricantes, por integradores/consultores y por operadores.

A continuación tendrá lugar un segundo bloque, en el que seis especialistas de las compañías copatrocinadoras expondrán sintéticamente las características más relevantes de su oferta y pondrán algunos ejemplos de acuerdos vigentes en España.

Finalmente, el tercer y último bloque lo conformará una mesa redonda en la que profesionales de organizaciones usuarias –en esta ocasión expertos en seguridad de **Cepsa**, **Ministerio de Defensa** y **Vodafone**– brindarán su opinión profesional acerca del asunto propuesto.

Programa

CLAVES PARA DECIDIR

09:00h. Acreditación y entrega de documentación.

09:30h. **Servicios gestionados por terceros desde SOC: tipologías, especialización y prescripción de servicios.**

Ponente: **Mariano J. Benito Gómez**,
Director de Seguridad de GMV Soluciones Globales Internet.

10:20h. Coloquio.

APROXIMACIONES DE LOS PRESTADORES

10:25h. **Accenture.**

Javier Martín Barroso,
Senior Manager del área de Seguridad Gestionada. Accenture Technology Consulting.

10:45h. **Grupo SIA.**

Eduardo López Rebollal,
Director de Marketing de Producto.

11:05h. **IBM Internet Security Systems.**

Vicente Gozalbo Moragrega,
Gerente de Desarrollo de Negocio para España y Portugal. Servicios de Seguridad Gestionados.

11:25h. Pausa-café.

11:55h. **S21sec - VeriSign.**

Alfonso del Castillo Jurado,
Director de Operaciones.

12:15h. **Symantec.**

Alfredo Reino Romero,
Consultor Senior de Seguridad y Responsable de la Práctica Security Assurance.

12:35h. **Telefónica España.**

Juan Miguel Velasco López-Urda,
Director Asociado de Servicios y Soluciones de Seguridad. Servicios desde la RED-A.M.Seguridad. UN Grandes Empresas.

12:55h. Coloquio general.

MESA REDONDA

13:05h. **La visión de los usuarios. Escenarios actuales, limitaciones y necesidades futuras.**
Participantes:

Rafael Hernández González,
Responsable de Seguridad Informática de Cepsa.

Miguel Ángel Rego Fernández,
Área de Seguridad. Inspección CIS. Ministerio de Defensa.

Javier del Riego Fernández,
Jefe de Seguridad Lógica de Vodafone.

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.

La externalización de la seguridad TIC desde la red se ha convertido en una opción a considerar por parte de las corporaciones. Pero no es oro todo lo que reluce: todavía es necesario saber identificar a aquellos prestadores con conocimientos en protección y experiencia en *outsourcing*.

- ¿Qué hay que entender por externalización de servicios de seguridad en red ofrecidos desde un Centro de Operaciones de Seguridad?
- ¿Qué tipologías de servicios externalizados se identifican en el mercado en función de la naturaleza de los prestadores (operadores de TIC, fabricantes, consultores-integradores)?
- ¿Qué factores se identifican hoy como limitadores del crecimiento de la externalización de servicios de seguridad desde la red?
- ¿Se requiere un conocimiento especializado para dar servicios competentes de SOC o cualquier proveedor de servicios externalizados de CPD que disponga de acuerdos con grupos de prevención e investigación de incidentes puede ofrecer de forma fiable la administración de la seguridad desde la red?
- ¿Es factible para los usuarios pactar acuerdos de nivel de servicio contrastables en los que prepondere su opinión frente a la del prestador, y en cuyo contexto el impacto económico no sea disuasorio?
- ¿Hasta qué punto los prestadores pueden diseñar a medida servicios externalizados de seguridad en red a precios de mercado?

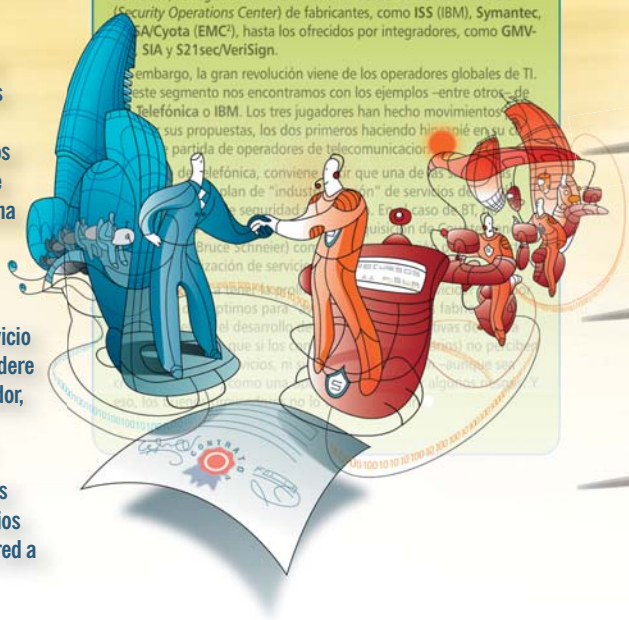
Externalización de servicios gestionados de seguridad: tonto el último

El sector de TIC –y, claro, el ramo de seguridad– han entrado en una etapa evolutiva apasionante, caracterizada, de una parte, por la aceleración de adquisiciones de compañías especializadas en protección por los grandes fabricantes generalistas, y de otra por una reacción de los "clásicos vivos" de la seguridad, que están comprando otras firmas especializadas para ofrecer un portafolio que se adapte a la evolución de las amenazas y del mercado.

A esta fase de madurez de los fabricantes de tecnología –que pelean por conservar el reparto de lo conocido y conquistar lo nuevo– se está superponiendo otra, que si representa un paradigma: la conformación de propuestas de externalización de servicios de seguridad, que afecta en distinta medida a fabricantes, mayoristas, integradores, consultores, asesores, auditores, ISP, operadores globales de TI, grandes organizaciones, pymes y personas.

El mercado no ha definido todavía con exactitud qué debe incluir una oferta completa y/o especializada de externalización de seguridad; de hecho, se registra una oferta variada: desde los servicios de SOC (*Security Operations Center*) de fabricantes, como **ISS** (IBM), **Symantec**, **SA/Cyota** (**EMC²**), hasta los ofrecidos por integradores, como **GMV-SIA** y **S21sec/VeriSign**.

Sin embargo, la gran revolución viene de los operadores globales de TI. En este segmento nos encontramos con los ejemplos –entre otros– de **Telefónica** o **IBM**. Los tres jugadores han hecho movimientos [illegible] sus propuestas, los dos primeros haciendo hincapié en su [illegible] partida de operadores de telecomunicaciones [illegible] Telefónica, conviene [illegible] que una de las [illegible] plan de "industrialización" de servicios de [illegible] seguridad. [illegible] caso de BT, [illegible] Bruce Schneier) con [illegible] vación de servicios [illegible] optimos para [illegible] el desarrollo [illegible] que si los [illegible] servicios, ni [illegible] como un [illegible] sólo, los [illegible]



- ¿Es determinante para los posibles usuarios contratantes saber en qué tecnologías de fabricantes se basan los servicios ofrecidos por prestadores?
- ¿Hay que marcar límites a los prestadores acerca de la extensión de la cadena de subcontratación de intermediarios/proveedores para el servicio contratado?
- ¿Qué factores intervienen para calcular la rentabilidad económica, la buena sintonía en la gestión y la eficacia en la resolución de incidentes de la modalidad de seguridad externalizada desde la red frente a otras opciones?
- ¿Existen herramientas para el usuario eficientes cuya finalidad sea el control de la seguridad en la externalización de los servicios de protección contratados?
- ¿Es más o menos fiable a los efectos de servicio y auditoría que el externalizador disponga de certificaciones contra normas reconocidas: ISO 27001, ITIL...?
- ¿Ofrecen los externalizadores alternativas viables para hacerse cargo del sistema tecnológico de seguridad creado "*in house*" por el usuario durante años?

RESPUESTAS SIC

Seguridad gestionada por terceros en red desde SOC

FECHA
16 de octubre de 2007

LUGAR
Hotel NH Eurobuilding de Madrid.
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.