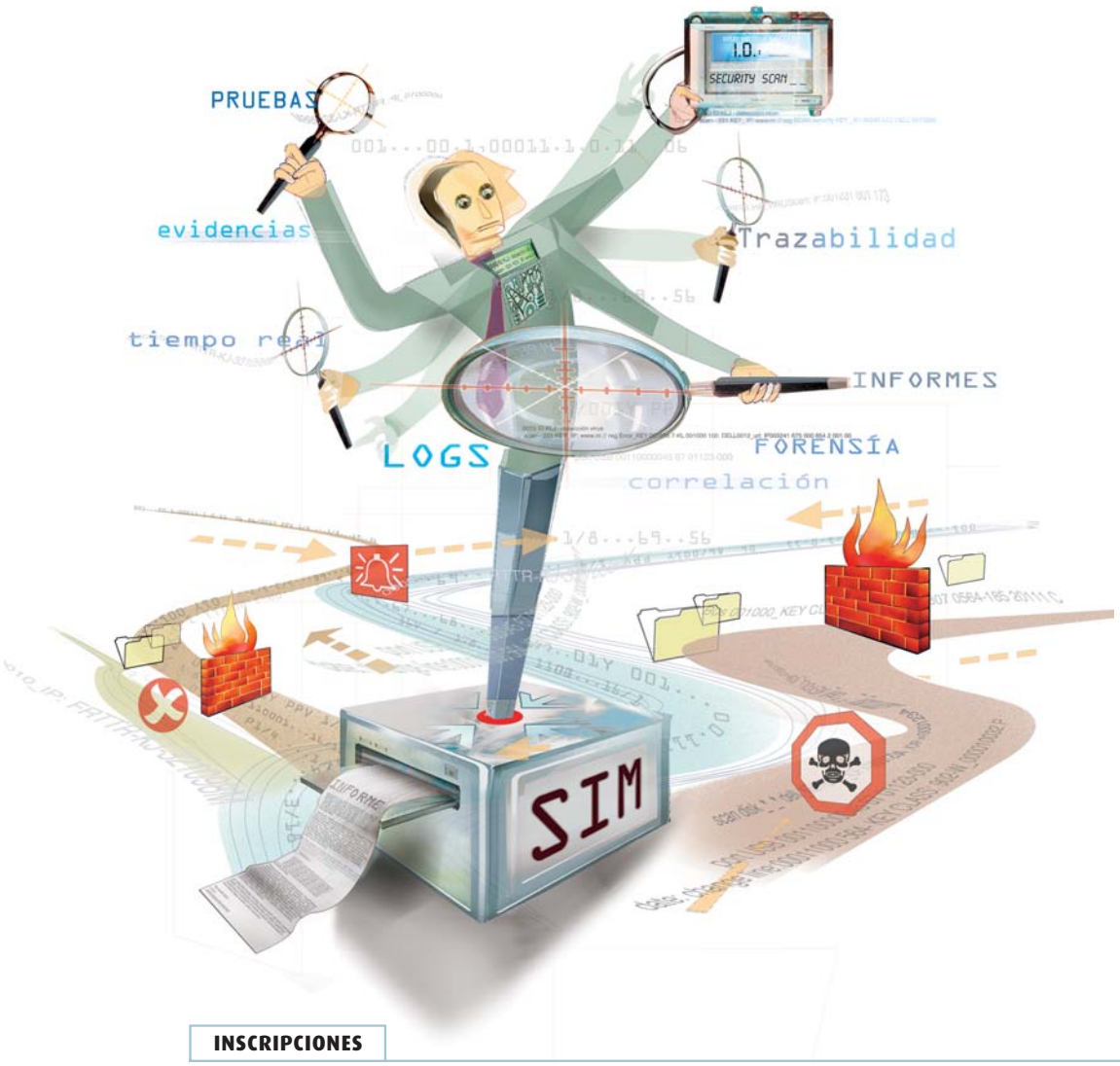
RESPUESTAS SiC

5 de octubre de 2006
Hotel NH Eurobuilding
Madrid

## Seguridad TI

# Qué está pasando en mi Sistema de Información




**INSCRIPCIONES**

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

> **AFORO LIMITADO**

Organiza:

Revista SiC seguridad en informática y comunicaciones

Copatrocinan:

ArcSight · BREYER · ca · IBM · IGA · S21sec · symantec.

# Qué está pasando en mi

## SIM: el camino hacia la protección

Saber en tiempo real qué está pasando en los sistemas que pueda ser relevante para la seguridad de la información de las organizaciones, y, en consecuencia, poder tomar decisiones de prevención y defensa, constituye hoy el objetivo principal de los Responsables de Seguridad de la Información y, obviamente, de la Dirección de Sistemas de Información de cualquier entidad, pública o privada.

Pero crear procesos altamente automatizados tendentes a disponer de información sobre eventos completa, útil y de calidad en el momento justo, y que, además, permitan la implantación de mecanismos para la extracción, preservación y conservación de evidencias no es tarea fácil, ya que obliga de modo rotundo a considerar al sistema de información en su globalidad –incluyendo en él los sistemas de protección TIC en operación– y a definir a efectos corporativos qué es un evento de seguridad, clasificarlos y crear procedimientos de actuación.

Estas son las razones por las que el proyecto SIM (Security Information Management) se convierte en el más ambicioso y complejo de cuantos afectan a la base misma de la gestión de la seguridad de la información y de la seguridad TIC, ya que conjuga en una suerte de sistema heterogéneo información en el nivel de los registros de conexión, definición de eventos, correlación de eventos, bases de datos de vulnerabilidades, análisis de comportamientos, herramientas avanzadas de informes, definición de indicadores y elección de medidas, establecimiento de procedimientos de reacción, punto único de gestión, forensia...

Y estas son también las razones por las que las propuestas tecnológicas de mercado en el entorno SIM mantienen en la actualidad las suficientes diferencias como para convertir la decisión de optar por unas u otras en un quehacer solo apto para los buenos profesionales de la seguridad de la información.

Así pues, para profundizar en este hecho, la revista SIC convoca una sesión matinal –tercera de las organizadas por la publicación bajo el lema **Respuestas SIC**–, que tendrá lugar el próximo **5 de octubre** en el hotel NH Eurobuilding de Madrid.

## SIM, el proyecto ineludible


Fuente: Encuesta sobre Seguridad y Delito Informático del CSI/FBI de 2006. Computer Security Institute.

**Uso apropiado de *logs* (adaptado de NIST 800-92)**

| Categoría | Ataque | Mal uso | Fraude |
|---|---|---|---|
| **Sistemas de seguridad** | | | |
| Filtrado de paquetes (conmutadores, enrutadores) | S | | |
| Cortafuegos | S | | |
| IDS / IPS (sistema, red, integridad) | P | P | S |
| *Antimalware* (virus, troyanos, spyware, rootkits...) | P | P | |
| Detector de vulnerabilidades | S | | |
| Servidores de autenticación | P | P | P |
| Sistemas de cuarentena, honeypots/honeynets | P | S | |
| **Sistemas operativos y servicios de red** | | | |
| Eventos de sistema | P | | |
| Eventos de auditoría | P | P | P |
| Servidor web / servidor de aplicaciones | S | P | P |
| Servidor de correo-e | S | P | P |
| Servidor de ficheros | S | P | S |
| **Aplicaciones / bases de datos** | | | |
| Eventos de auditoría | S | P | P |
| Otros registros de actividad (login/logoff, etc) | S | P | S |

Fuente: Luis Rodríguez (SIC nº71, septiembre de 2006).


**¿Qué porcentaje del tiempo emplea su plantilla, a diario, en recopilar y analizar manualmente los datos?**

| ESPAÑA | | SECTOR | | | | | | | | EMPLEADOS | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | TOTAL | Finanzas | Fabricación | Servicios Profesionales y Empresariales | Minorista o mayorista | Transporte o distribución | Servicios Públicos | Industria farmacéutica y sanitaria | Sector público | Entre 500 y 2.000 | Entre 2.001 y 5.000 | Más de 5.000 |
| 60% o más | 3% | 9% | | | | | 17% | 13% | | 3% | 8% | |
| 50% | 5% | 15% | 7% | | | 8% | 17% | 13% | | 2% | 15% | 13% |
| 40% | 10% | 9% | 14% | 2% | | 17% | 33% | | 29% | 9% | 15% | 9% |
| 30% | 41% | 36% | 57% | 39% | 100% | 58% | 33% | 38% | 29% | 48% | 31% | 35% |
| Nota | 41% | 27% | 21% | 59% | | 17% | | 38% | 43% | 38% | 31% | 43% |
| EUROPA | | | | | | | | | | | | |
| 60% o más | 5% | 12% | 1% | 3% | 7% | 3% | 16% | 11% | 7% | 2% | 10% | 11% |
| 50% | 8% | 12% | 4% | 2% | 11% | 10% | 15% | 20% | 21% | 4% | 18% | 14% |
| 40% | 13% | 10% | 9% | 13% | 19% | 10% | 18% | 20% | 13% | 12% | 21% | 10% |
| 30% | 44% | 31% | 66% | 53% | 22% | 47% | 12% | 23% | 15% | 55% | 19% | 25% |
| Nota | 30% | 36% | 20% | 28% | 41% | 30% | 38% | 25% | 44% | 26% | 23% | 40% |

NOTA: La cantidad de datos de eventos generada es demasiado grande para examinarla

Fuente: Estudio "Definición y establecimiento de prioridades frente a las amenazas de seguridad". Informe de Varson Bourne. Mayo de 2006.

# Sistema de Información

### Contenido

La estructura prevista de la sesión incluirá tres bloques de interés: el propósito del primero, conformado por dos ponencias –impartidas por expertos de **Ernst & Young** y **GMV Soluciones Globales Internet**–, será realizar una aproximación a las principales claves que definen la mencionada necesidad de proveerse de este tipo de plataformas.

El segundo bloque consiste en mostrar cuáles son, hoy día, las aproximaciones tecnológicas de la industria en este campo, para lo cual seis de las principales compañías especializadas en la materia (**ArcSight**, **CA**, **IBM**, **ICA**, **S21Sec** y **Symantec**) mostrarán las principales características de sus sistemas, encaminados a convertir las grandes cantidades de datos procedentes de sistemas y aplicaciones dispares en información procesable y relevante. Igualmente, los representantes de estas compañías mostrarán ejemplos de este tipo de proyectos llevados a cabo internacionalmente y en España con sus respectivas tecnologías y herramientas.

Finalmente, el tercer y último epígrafe lo conformará una mesa redonda en la que usuarios de organizaciones de nuestro país con experiencia en el tema –en esta ocasión cualificados expertos del área de seguridad de la información de **acens, Bankinter** e **Iberdrola**, debatirán sobre su visión al respecto, tanto en lo concerniente a la posibilidades actuales de conformar este tipo de soluciones de inteligencia empresarial procesable, como a las necesidades futuras, que, a su entender, el devenir de la actividad empresarial demandará en los departamento de seguridad TI para mejorar la eficiencia administrativa, reducir costes y ayudar a cumplir las leyes y normativas imperantes.

# Programa

09:00h. Acreditación y entrega de documentación.

## CLAVES PARA DECIDIR

09:30h. **Proyectos SIM: estado del arte, prescripciones de uso y escenarios previstos de aplicación.**

Ponente: **Francisco Javier Santos Ortega,** Senior Manager de T&SRS (Technology & Security Risk Services) de Ernst & Young.

10:00h. Coloquio.

10:05h. **Consideraciones en el despliegue de herramientas SIM.**

Ponente: **Rodrigo Bermúdez Soto,** Consultor de la División de Auditoría y Planificación de Seguridad de GMV Soluciones Globales Internet.

10:35h. Coloquio.

## APROXIMACIONES TECNOLÓGICAS DE LA INDUSTRIA

10:40h. **ArcSight.**

**Pablo Crespo Figuera,** Director de Postventa de Breyer.

11:00h. **CA.**

**Inma Terol Nieto,** Responsable Comercial de Seguridad.

11:20h. **IBM.**

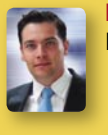
**José Luis Berrocal,** Especialista en Soluciones Netcool. SPGIT.

11:40h. Pausa-café.

12:10h. **ICA.**

**Victorino Martín Jorcano,** Director de Seguridad TIC.

12:30h. **S21sec.**



**David Barroso Berrueta,** Director de Investigación.

12:50h. **Symantec.**

**Timoteo Menezes,** Consultor Senior de Seguridad.

13:10h. Coloquio general.

## MESA REDONDA: La visión de los usuarios. Escenarios actuales, limitaciones y necesidades futuras.

13:25h. Participantes:

**Pedro Castillo Muros,** Director de Innovación Tecnológica de Bankinter.

**Manuel Palau Rolduá,** Jefe de la Unidad de Políticas y Normativa de la Dirección de Sistemas de Iberdrola.

**Gustavo San Felipe Lobo,** Responsable de Seguridad de acens.

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.

# Los responsables de seguridad gastan un tercio de su jornada laboral recopilando, leyendo y analizando informes generados por sus aplicaciones y dispositivos de seguridad...

- ¿Qué es un SIM y para qué sirve?
- ¿Qué fuentes de información de seguridad interesan a mi empresa?
- ¿Tiene mi organización una política definida de gestión de registros de actividad?
- ¿Qué información debe consignarse en los *logs* para fines de seguridad y auditoría?
- ¿Ofrece el mercado herramientas para facilitar la extracción, filtrado, detección y transporte de *logs*?

El 70% de las compañías encuestadas sólo cuenta con un responsable para analizar estos registros

## Saturación de *logs* y registros de seguridad, un problema para las empresas europeas

Como cabía prever, según el estudio *Definición y establecimiento de prioridades entre amenazas de seguridad*, una nutrida muestra de empresas europeas encuentran graves dificultades para gestionar la elevadísima cantidad de datos que generan sus dispositivos tecnológicos de seguridad, del tipo cortafuegos, software antivirus y de propósito complementario.

Para el 30% de estos encuestados, la cantidad de datos de seguridad generados en sus empresas es tan grande que no pueden examinarlos detenidamente con el fin de identificar potenciales amenazas para la seguridad interna. Curiosamente, este porcentaje se eleva al 40% en el caso de España.

Más llamativo resulta el hecho de que casi el 70% de las organizaciones que han respondido reconocen contar con un único responsable TI en este campo para revisar y examinar todos los registros y *logs* de incidencias de seguridad. Por este motivo, deben basarse en su experiencia y conocimiento para identificar los comportamientos sospechosos o amenazas, dado que no cuentan con el tiempo necesario para evaluar todos los da... se deben reprimir en primer lugar. En el caso d... el dato se dispar... el 80%, lo que compli... mismas de alcan... Administración Electró... número de s... on line pero ... mayor...


- ¿Estoy en disposición de atender hoy un requerimiento sobre registro de actividad, emitido por un organismo de control como la AEPD?
- ¿Qué he de priorizar, el seguimiento y control de la seguridad TIC en tiempo real o el manejo de *logs* con fines forenses?
- "La consola de consolas", ¿sueño o realidad?
- ¿Cómo dimensionar los medios necesarios para ir tratando el creciente volumen de datos SIM?
- ¿Hacia dónde evolucionarán las actuales soluciones SIM?

RESPUESTAS SIC

## Qué está pasando en mi Sistema de Información

**FECHA**
5 de octubre de 2006

**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.