ESPACIO TISEC 2003

25 de noviembre de 2003
Hotel Novotel
Campo de las Naciones
Madrid

Directrices para la gestión de la seguridad de la información

Programa

Organiza

REVISTA SIC seguridad en informática y comunicaciones

ESPACIO TiSEC 2003

Un espacio profesional para marcar los cauces de la gestión de la seguridad de la información

TiSEC, evento profesional organizado por la revista SIC, auna el conocimiento y la experiencia de destacados expertos para marcar los cauces por lo que está discurriendo la gestión de la seguridad de la información y de la seguridad TIC, y que, obviamente, condicionan su futuro.

La cuestión hoy no se centra tanto en justificar la necesidad de protección –lo que siempre resulta necesario–, como en tener el conocimiento suficiente para enfocar adecuadamente la implantación con garantías razonables de continuidad de dicha función en la empresa, cuyo principal objetivo es el de gestionar los riesgos de seguridad de la información y de seguridad de los sistemas tecnológicos que la tratan.

Existen para ello normas internacionales, cuyo ejemplo más paradigmático lo constituye la ISO 17799. No obstante, el mejor camino para obtener conocimiento directo acerca de este asunto es escuchar a aquellos profesionales que están pudiendo poner en práctica en sus empresas modelos de gestión de la seguridad, y también a los asesores que colaboran en el diseño de iniciativas corporativas de alto nivel.

Esto es, precisamente, lo que aporta Espacio TiSEC 2003, a través de la exposición por parte de muy notables expertos españoles de **Endesa**, **Santander Central Hispano**, **Telefónica** y la **UPM**, de cuatro temas capitales en el mundo de la protección: el análisis de riesgos de seguridad, el plan director de seguridad, el cuadro de mando de seguridad, y el alineamiento de las herramientas técnicas de protección con las necesidades de gestión de riesgos de seguridad.

Igualmente, especialistas de **Deloitte & Touche**, **Ernst & Young**, **KPMG** y **PricewaterhouseCoopers** debatirán en mesa redonda un asunto del máximo interés a todos los efectos: *¿qué líneas de actuación prioritarias van a marcar el rumbo de las inversiones en seguridad de la información?*

Espacio TiSEC 2003 propone también un segundo y paradigmático debate sobre los retos que se plantean hoy los directivos de seguridad de la información y de seguridad TIC, en el que está prevista la participación de gestores expertos de **BBVA**, **Caja Madrid**, **Grupo Ocaso** e **Iberdrola**.

Organiza

REVISTA SIC seguridad en informática y comunicaciones

Copatrocinan

Deloitte. · ERNST & YOUNG Quality In Everything We Do · KPMG · PRICEWATERHOUSECOOPERS

Programa

09:00h. Entrega de documentación.

09:15h. Acto de inauguración.

09:30h. Ponencia: **El arte y la ciencia del análisis de riesgos.**
Ponente: **José Antonio Castro**, Director de Seguridad Informática de Santander Central Hispano.

10:15h. Coloquio

10:30h. Ponencia: **Por el buen camino: el plan director de seguridad de la información.**
Ponente: **Ramón Montes**, Coordinador de Seguridad Informática de Endesa.

11:15h. Coloquio

11:30h. Pausa - café

12:00h. Ponencia: **Una herramienta valiosa: el cuadro de mando de seguridad de la información.**
Ponente: **Manuel Carpio**, Director de Seguridad de la Información y Prevención de Fraude de Telefónica S.A.

12:45h. Coloquio

13:00h. Debate: **¿Qué líneas de actuación prioritarias van a marcar el rumbo de las inversiones en seguridad de la información y seguridad TIC?**
Participantes:

- **Rafael Ortega**, Director de Enterprise Risk Services de Deloitte.
- **Antonio Ramos**, Gerente de Technology and Security Risk Services de Ernst & Young.
- **Ramón Poch**, Gerente de Information Risk Management de KPMG.
- **Diego Sacristán**, Gerente de la práctica de Seguridad de la Información y Privacidad de PricewaterhouseCoopers.

14:30h. Almuerzo

16:30h. Ponencia: **¿Se alinean las funcionalidades de las herramientas técnicas de protección con las necesidades de gestión de seguridad de los usuarios?**
Ponente: **José Antonio Mañas**, Catedrático de Ingeniería Telemática. ETSI de Telecomunicación. Universidad Politécnica de Madrid.

17:15h. Coloquio.

17:30h. Debate: **¿Cuáles son los retos que se plantean hoy los directivos de seguridad de la información y de seguridad TIC?**
Participantes:

- **Francisco Javier García Carmona**, Director de Seguridad de la Información y Comunicaciones de Iberdrola.
- **David Jorrín**, Responsable de Seguridad Informática del Grupo Ocaso.
- **Santiago Moral**, Director de Seguridad Lógica Corporativa del Grupo BBVA
- **Miguel Ángel Navarrete**, Director de Seguridad Informática de Caja Madrid.

19:00h. Clausura.

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

El arte y la ciencia del análisis de riesgos

En el escenario tecnológico actual, donde los sistemas de información son fundamentales para la operativa y el negocio de las empresas, la gestión del riesgo tecnológico se postula como un componente de gran peso específico en el riesgo operativo y, por tanto, aspecto fundamental a la hora de diseñar la estrategia y los objetivos de las organizaciones. En el mundo empresarial, el alto riesgo es sinónimo de alto porcentaje de fracaso; mediante la adecuada gestión del riesgo tecnológico se pueden determinar claramente acciones preventivas para mitigar o minimizar los riesgos asociados al uso de tecnologías de la información.

En la presentación, se tratará de la gestión de la seguridad desde la filosofía de la gestión del riesgo tecnológico y desde la óptica de una larga experiencia en una compañía, plasmando estrategias, enfoques y aspectos fundamentales a considerar de cara a la implementación y despliegue de un sistema de gestión de riesgo.

José Antonio Castro es Director de Seguridad Informática de Santander Central Hispano. Ha desarrollado la práctica totalidad de su carrera profesional en tecnologías de la información (16 años) en Santander Central Hispano, primero como consultor del área internacional y luego como responsable de diferentes áreas técnicas. Cuenta con 10 años de experiencia en el mundo de la seguridad de la información en áreas como continuidad operativa, seguridad en canales alternativos, infraestructuras de clave pública, arquitecturas de seguridad net, ...

Por el buen camino: el plan director de seguridad de la información

La ponencia se desarrollará en base a dos líneas argumentales, una primera, teórica, en la que de un modo sintético se aportarán ideas conceptuales sobre el Plan Director de Seguridad: base organizativa, apoyo de la dirección, análisis de riesgos, ROSI, cuadro de mando, etc., y una segunda práctica, basada en la experiencia de Endesa, en la que se explicará cómo nació la Unidad de Seguridad Informática y cómo desde un primer momento se detectó la necesidad de generar un Plan Director, haciendo énfasis en los aspectos que lo impulsaron y los posibles riesgos que podían hacerlo fracasar. Para finalizar se expondrán los objetivos generales del Plan Director de Seguridad Informática 2002-2005 de Endesa, y se resumirán las distintas actuaciones que lo conforman.

Ramón Montes ha cursado estudios de Ingeniería Superior en la Universidad Politécnica de Barcelona. En 1974 ingresó en la Escuela de Aprendices de Fecsa, y en 1976 pasó a la Dirección de Sistemas de Información de esta empresa, en la que prestó sus servicios como Operador de Sistemas y como Responsable de Explotación. En 1998 y hasta enero de 2000, dirigió el proyecto de Adaptación al Año 2000 de la infraestructura tecnológica de Endesa. Posteriormente, y ya en esta compañía, fue responsable de la creación de la función de Seguridad Informática con el cargo de Coordinador de Seguridad Informática, que ocupa en la actualidad. En el año 2001, diseñó el Plan Director de Seguridad Informática 2002-2005 de Endesa, actualmente en fase de desarrollo e implantación.

DEBATE ·····>

¿Qué líneas de actuación prioritarias van a marcar el rumbo de las inversiones en seguridad de la información y seguridad TIC?

La inversión en seguridad de la información y en seguridad TIC lleva tiempo creciendo. Las entidades más madrugadoras –por decirlo de algún modo, el grupo de cabeza– tienen ya en fase de ejecución planes directores a varios años en los que se recogen de forma ordenada numerosas acciones y proyectos. Pero, ¿pasará mucho tiempo hasta que esta pauta de comportamiento sea extrapolable al resto de organizaciones empresariales de cierta dimensión, o por el contrario un conjunto importante de las mismas seguirá invirtiendo sólo en función de necesidades coyunturales?

Rafael Ortega es director responsable de Seguridad y PKI del Área de Enterprise Risk Services en Deloitte España, S.L. Ha dirigido y participado en numerosos proyectos de seguridad de los Sistemas de Información, proyectos de planificación estratégica de sistemas de información, proyectos relacionados con Infraestructura de Clave Pública, Planes Estratégicos de Seguridad, Desarrollo y Soporte a Planes de Contingencia, Diagnósticos de Seguridad y Análisis de Riesgos.

Antonio Ramos es Gerente de Technology and Security Risk Services (TSRS) de Ernst & Young. Licenciado en Ciencias Económicas –especialidad Cuantitativa– por la Universidad Complutense de Madrid y Master en Auditoría por la Universidad Pontificia de Salamanca, desde su incorporación a Ernst & Young se especializó en Auditorías de Seguridad Informática, obteniendo la certificación CISA de la Isaca en el año 2000. Actualmente es responsable del área de CyberProcess Certificación (auditorías de cumplimiento), realizando proyectos tipo WebTrust y, adicionalmente, participando en proyectos relacionados con firma digital y toda la normativa existente en relación con ella) y con ISO 17799 / BS7799.

Ramón Poch, economista por la Universidad de Barcelona y por la Universidad Central Lancashire de UK, es Master en Auditoría Informática y CISA así como Vocal de la ISACA en Barcelona. Inició su carrera profesional en Nestle, siendo trasladadado como responsable de Auditoría Interna Informática a la sede mundial de Nestle en Suiza. Posteriormente se incorporó a KPMG como Gerente del grupo de Information Risk Management en Barcelona, donde desarrolla actualmente su actividad. Poch también es ponente habitual en materia de Auditoría Informática en el Instituto de Auditores Censores Jurados de Cuentas de España, asi como del Instituto de Auditores Internos. Finalmente es profesor de Auditoría Informática de la Universidad de Barcelona, así como en otros foros.

Diego Sacristán. Gerente de la práctica de Seguridad de la Información y Privacidad de PricewaterhouseCoopers. Su trayectoria profesional se inició en el desarrollo de sistemas de información, especializándose posteriormente en la seguridad de la información y sistemas asociados. Cabe destacar su experiencia internacional, habiendo desarrollado y dirigido proyectos de seguridad en las principales entidades financieras inglesas durante su traslado a la oficina de PwC en Londres. Diego Sacristán es Licenciado en Ciencias Económicas y Empresariales por la UCM y CISSP.

Una herramienta valiosa: el cuadro de mando de seguridad de la información

El aumento de la financiación de la seguridad informática ha crecido significativamente en los últimos años y todo indica que esta tendencia se puede mantener en el futuro próximo, para alborozo de los responsables de seguridad. Pero cualquier día, al igual que ha ido ocurriendo con otras preocupaciones consideradas como de alta prioridad para el negocio, los equipos directivos de las grandes empresas se preguntarán sobre la eficacia, la eficiencia, el retorno de la inversión y cómo esas inversiones están contribuyendo a los objetivos globales de la organización. Una respuesta profesional a esta inquietud puede consistir en un conjunto de métricas de seguridad englobadas en un cuadro de mando. Durante la conferencia se procurará clarificar algunos conceptos alrededor de métricas y cuadros de mando, su valor para la organización así como las dificultades para su establecimiento y continuidad.

Manuel Carpio. Ingeniero Superior de Telecomunicaciones por la UPM, Programador de Sistemas por la Escuela Superior de Informática PDD IESE (Universidad de Navarra) y miembro de Isaca (EE.UU.) con la certificación CISA. Inició su carrera profesional en 1988 como Ingeniero de Desarrollo en Telefónica Sistemas y Jefe de Proyecto de Seguridad de la Información y las Comunicaciones. En 1992 fundó el Área de Consultoría de Seguridad, dedicada a la integración de soluciones de seguridad para 'Grandes Clientes' de Telefónica. Más adelante, y desempeñando el cargo de Gerente de Seguridad Lógica, realizó las especificaciones y dirigió diversos proyectos. Igualmente, desarrolló la normativa de seguridad para los ficheros con datos de carácter personal de acuerdo con la legalidad vigente. Desde noviembre de 2001 ocupa el cargo de Director de Seguridad de la Información y Prevención de Fraude en Telefónica S.A., dependiendo de la Subdirección General de Seguridad Corporativa de la entidad. Su actividad se centra en las tareas de organización de seguridad, normalización de seguridad y prevención del fraude, establecimiento y homogeneización de herramientas de control de gestión, monitorización continua y supervisión de cumplimiento.

¿Se alinean las funcionalidades de las herramientas tecnicas de protección con las necesidades de gestión de seguridad de los usuarios?

Gestionar la seguridad es invertir con retorno. O debería serlo. Y para ello es necesario que las herramientas, que cuestan dinero y mucho tiempo, respondan de forma verificable al objetivo (de seguridad) que justificó su adquisición y justifica su mantenimiento. ¿Es así? El problema de integración requiere una respuesta sólida pero evolutiva para responder a las necesidades del día a día, de la lucha reactiva y de la venta a la dirección, del responsable de seguridad y de los usuarios que operan o disfrutan del servicio que es, en última instancia, la métrica definitiva del éxito. ¿Qué hay que pedir? ¿Cuál es nuestra cuota de responsabilidad?

José Antonio Mañas. Ingeniero de Telecomunicación, Doctor en informática, Catedrático de Ingeniería de Sistemas Telemáticos en la E.T.S.I. Telecomunicación de la Universidad Politécnica de Madrid, está especializado en redes de comunicaciones (Internet en particular) y seguridad (criptografía y protocolos seguros para comunicaciones y medios de pago). Participó en la creación del servicio de banca por Internet de BCH y Bankinter, en la definición de la arquitectura de sistemas para los JJOO de Salt Lake City, y análisis de seguridad del canal Internet de Loterías del Estado. Miembro del SC27 (seguridad) de ISO y editor de la norma internacional 18014 (fechado electrónico).

DEBATE ·····>

¿Cuáles son los retos que se plantean hoy los directivos de seguridad de la información y de seguridad TIC?

Aunque la historia de la seguridad de la información y de la seguridad TIC sea relativamente corta, sí pueden diferenciarse en España distintas etapas en su evolución, marcadas por la mayor o menor atención en los planes empresariales a los aspectos tecnológicos, organizativos o de cumplimiento legal en función de plazos de adaptación establecidos. Pero, ¿en qué fase nos encontramos ahora? ¿Qué se está haciendo? ¿Qué retos específicos se plantean en la actualidad los directivos de seguridad TIC?

Francisco Javier García Carmona. Inicia su actividad en 1982 en el sector de las Telecomunicaciones, pasando a dirigir este departamento en diversas empresas del ramo, incorporándose al mundo de la Seguridad en el año 96, simultaneando la Dirección de Operaciones con funciones técnicas. En el año 2001 se incorpora a Iberdrola como Director del Departamento de Seguridad de la Información y Comunicaciones.

David Jorrín es Responsable de Seguridad Informática del Grupo Ocaso. Licenciado en Informática por la Universidad Politécnica de Madrid, comenzó su carrera profesional hace nueve años, dedicado inicialmente a la administración y técnica de sistemas (en entornos unix y servicios Internet). Desde hace seis años está especializado en el área de seguridad lógica, actividad que ha desarrollado en diversas empresas del sector de Telecomunicaciones. Hace un año se incorporó al Grupo Ocaso como responsable de Seguridad Informática de la División de Seguridad Informática, donde se encarga de la coordinación, supervisión e implantación de la seguridad en los sistemas de información del Grupo.

Santiago Moral comienza a trabajar para el Grupo BBVA en mayo del año 2000 como Responsable de Seguridad de Sistemas de Información de la entidad financiera Uno-e Bank. En marzo del año 2001, Moral pasa a ser Responsable de Seguridad Lógica de BBVA Europa, siendo actualmente Director de Seguridad Lógica Corporativa del Grupo BBVA.

Miguel Ángel Navarrete. Director de Seguridad Informática de Caja Madrid, ha trabajado como informático desde hace 20 años en diferentes entidades financieras. Desde su primer contacto en Explotación y hasta su llegada al mundo de la seguridad de la información, ha recorrido un buen número de áreas de las TI como Técnica de Sistemas, Gestión Presupuestaria, de Recursos y Proyectos, Metodología, Arquitectura y más recientemente Desarrollo de Software, donde ha dirigido los equipos y proyectos de infraestructura de oficinas y autoservicio, del centro de informática personal y de soluciones internet. Actualmente se enmarca en Planificación e Innovación Tecnológica, donde se ubica el Departamento de Seguridad Informática del Grupo Caja Madrid, con la responsabilidad y la oportunidad de potenciar la seguridad del Grupo.

ESPACIO TiSEC 2003

AFORO LIMITADO

Fecha y lugar

TISEC 2003 tendrá lugar el día 25 de noviembre de 2003 en el Hotel NOVOTEL*. Campo de las Naciones de Madrid.

Derechos de inscripción por módulo

- Los asistentes inscritos en TISEC 2003 recibirán la carpeta de documentación con las ponencias así como un CD-Rom con la información en formato digital
- Almuerzo y cafés
- Diploma de asistencia

Cuota de inscripción

- Hasta el 7 de noviembre **661** + **16% IVA**
- Después del 7 de noviembre **760** + **16% IVA**

Descuentos:

– Dos inscripciones de una misma empresa: 10% dto. cada una.
– Tres inscripciones y siguientes: 15% dto. cada una.
– Universidades: 25% dto. cada una.

Contacto para inscripción

- Por teléfono: +34 91 401 06 26
  +34 91 309 04 99
- Por fax: +34 91 401 09 90
- Por correo electrónico: info@revistasic.com
  info@codasic.com
- Por sitio web: www.revistasic.com/tisec
- Por correo convencional: envíe el Boletín adjunto o fotocopia del mismo a:

EDICIONES CODA / REVISTA SIC
Lombía, 3 - Bajo derecha
28009 Madrid (España)

- Abone la cantidad correspondiente mediante cheque nominativo a favor de Ediciones CODA, S.L., que deberá ser remitido a la dirección de Ediciones CODA, o
- Transferencia bancaria, cuya fotocopia deberá ser remitida vía fax o correo, a nombre de:

EDICIONES CODA, S.L.
CAJA DE MADRID
Oficina: Avda. de Felipe II, 15
28009 Madrid (España)
C.C.C.: 2038 1726 67 6000477427

- * Existen descuentos para los asistentes a TiSEC que deseen alojarse en el hotel Novotel con motivo de su asistencia a TiSEC. Este particular deberá ser comunicado a la entidad organizadora con la debida antelación, ya que el número de habitaciones es limitado.
- Las inscripciones sólo se considerarán formalizadas una vez satisfecho el importe de las mismas antes de la celebración deTiSEC.
- Las cancelaciones de inscripción sólo serán aceptadas hasta 7 días antes de la celebración del evento y deberán comunicarse por escrito a la entidad organizadora. Se devolverá el importe menos un 10% por gastos administrativos.

Boletín de inscripción a TiSEC 2003

Nombre y apellidos _____

Nombre y apellidos _____

Nombre y apellidos _____

Empresa _____ C.I.F. _____

Cargo _____

Dirección _____ Población _____

Código Postal _____ Teléfono _____ Fax _____

Persona de contacto, Departamento y teléfono para facturación _____

_____

❑ Deseo inscribirme a TiSEC 2003
Firma:

Forma de pago: ❑ Talón ❑ Transferencia

Los datos personales que se solicitan, cuya finalidad es la formalización y seguimiento de su inscripción en TiSEC 2003, serán objeto de tratamiento informático por Ediciones Coda, S.L. Usted puede ejercitar sus derechos de acceso, rectificación, cancelación y oposición, expresados en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en el domicilio del responsable del fichero: Ediciones Coda, S.L., C/. de Lombía, 3. Bajo derecha. 28009 Madrid.

>>> **Información e inscripciones:**

REVISTA SIC seguridad en informática y comunicaciones

Ediciones CODA / Revista SIC
Lombía, 3 - Bajo derecha · 28009 Madrid (España)
Tel: 91 401 06 26 / 91 309 04 99 · Fax: 91 401 09 90
Correo-e: info@revistasic.com / info@codasic.com
Sitio: www.revistasic.com/tisec