ESPACIO TISEC 2005

23 y 24 de noviembre de 2005
Hotel Novotel
Campo de las Naciones
Madrid

# Programa

www.revistasic.com/tisec

# El buen gobierno de la seguridad

Organiza

Revista SIC seguridad en informática y comunicaciones

ESPACIO TiSEC 2005

# El buen gobierno de la seguridad

El devenir de la protección de los activos de información ha ido modelando un panorama en el que para mantener el nivel de riesgo preciso, es decir, para gobernar realmente los procesos de seguridad con eficacia y eficiencia, el responsable de esta actividad estratégica necesita ejercer su labor en el marco de un sistema de gestión contrastable que establezca lo que hay que ir midiendo y cómo.

En esta concepción, que no es en absoluto ajena a otras áreas de gestión de las empresas, ni está aislada de éstas, se hace necesario disponer de herramientas que ofrezcan datos de calidad sobre los estados de la seguridad presentes y, al tiempo, permitan evolucionar su gestión. Estas herramientas son, como se sabe, los cuadros de mando.

Espacio TiSEC 2005 propone un acercamiento diverso a estos conceptos mediante la impartición de conferencias específicas a cargo de expertos de reconocido prestigio.

Al tiempo será marco de dos debates de gran transcendencia, el primero dedicado a la contribución a la gestión de la seguridad de la información de las funciones de auditoría, control y cumplimiento normativo, en tanto que el segundo estará centrado en las nuevas medidas de seguridad en el futuro Reglamento de protección de datos, un asunto de gran actualidad y de muy notable interés para empresas, organismos públicos y profesionales.

Organiza

Revista SIC seguridad en informática y comunicaciones

Copatrocinan

AZERTIA · Indra · KPMG · PRICEWATERHOUSECOOPERS · SGI SOLUCIONES GLOBALES INTERNET

# Programa

## PRIMERA JORNADA | 23 de noviembre

09:00h. Entrega de documentación

09:30h. Acto de inauguración

10:00h. **La gestión integrada de la seguridad de la información y la seguridad tradicional.**
Ponente: **Felipe Alcántara Álvarez**, Subdirector General de Seguridad Corporativa. Telefónica.

10:45h. Coloquio

10:50h. **Hacia una mejora en la eficiencia de la gestión de la seguridad de la información.**
Ponente: **Joaquín Álvarez Pérez**, Coordinador de Seguridad de la Información. Dirección Corporativa de Estrategia. Endesa.

11:35h. Coloquio

11:40h. Pausa-café

12:10h. **La oficina de seguridad como modelo de gestión para las grandes organizaciones.**
Ponentes: **Jesús Romero Bartolomé**, Gestor de Negocio Seguridad TI. Indra, y **Jorge Laredo de la Iglesia**, Consultor Senior de Seguridad TI. Indra.

12:55h. Coloquio

13:00h. DEBATE:
**La contribución a la gestión de la seguridad de la información de las funciones de auditoría, control y cumplimiento normativo.**
Participantes:
- **Carlos Bachmaier Johanning**, Responsable de Seguridad Corporativa y Auditoría IT. Sistemas Técnicos de Loterías del Estado, STL.
- **Carlos Escudero Rivas**, Director del Centro de Calidad, Auditoría y Seguridad de la Gerencia de Informática de la Seguridad Social.
- **Fernando Hervada Vidal**, Presidente de la Asociación de Auditores y Auditoría y Control de Sistemas y Tecnologías de la Información y las Comunicaciones, ASIA (capítulo de Madrid de ISACA).

14:30h. Almuerzo

16:30h. **El día a día en la gestión de un SGSI certificado. El ciclo de vida de los controles.**
Ponente: **Mariano José Benito Gómez**, Director de Seguridad. SGI Soluciones Globales Internet.

17:15h. Coloquio

17:20h. **El impacto de la implantación de la gestión de identidades en una corporación.**
Ponente: **Juan José Míguez Iglesias**, Gerente del Área de Servicios de Seguridad de la Información de la División Advisory de PricewaterhouseCoopers.

18:25h. Coloquio

18:30h. Fin de la primera jornada

## SEGUNDA JORNADA | 24 de noviembre

09:30h. Inicio de la jornada

10:00h. **Qué debe y qué no debe tener un cuadro de mando de seguridad de la información.**
Ponente: **José Antonio Mañas Argemí**, Catedrático de Ingeniería Telemática. ETSI de Telecomunicación de la Universidad Politécnica de Madrid.

10:45h. Coloquio

10:55h. **El enfoque de la ISO/IEC WD 27004, Métricas y medidas para la gestión de la seguridad de la información.**
Ponente: **Paloma Llaneza González**, miembro del GT1 del Subcomité de AENOR (AEN/CTN 1/SC27/Wg1 Tecnologías de la Información) y Project Editor de la ISO/IEC WD 27004.

11:40h. Coloquio

11:50h. Pausa-café

12:20h. **La medición del riesgo y la respuesta temprana.**
Ponente: **Pedro Castillo Muros**, Director Técnico de Seguridad Informática. Bankinter.

13:05h. Coloquio

13:15h. **Experiencias en la creación de cuadros de mando de seguridad de la información.**
Ponentes: **Luis Sáiz Gimeno**, Responsable de los Procesos de Seguridad y Control Interno Corporativo. Dirección de Seguridad Lógica Corporativa del Grupo BBVA, y **Rafael Ortega García**, Vicepresidente de Continuidad de Negocio y Seguridad. Azertia.

14:00h. Coloquio

14:10h. Almuerzo

16:15h. **Cómo enlazar la seguridad TIC con los procesos de buen gobierno corporativo.**
Ponente: **Ramón Poch Vilaplana**. Director de IRM Information Risk Management. KPMG.

17:00h. Coloquio

17:10h. DEBATE:
**Las medidas de seguridad en el futuro Reglamento de protección de datos.**
Participantes:
- **Tomás Arroyo Salido**. Experto del sector financiero.
- **María José Blanco Antón**, Subdirectora General del Registro General de Protección de Datos. Agencia Española de Protección de Datos.
- **Francisco Javier García Carmona**, Director del Departamento de Seguridad de la Información y las Comunicaciones de Iberdrola.
- **Rosa María García Ontoso**, Asesora Adjunta al Gerente de Informática de la Comunidad de Madrid (ICM).
- **Mar Sánchez Caro**, Responsable de Seguridad Informática. BT España.

18:30h. Clausura

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

# 23 de noviembre

## La gestión integrada de la seguridad de la información y la seguridad tradicional.

La seguridad tradicional tiene experiencia de decenas de años, en tanto que la seguridad en tecnologías de la información y las comunicaciones empezó a extenderse hace poco tiempo. La primera basa su actividad en procedimientos, normativas y sistemas que la experiencia ha ido adaptando. La segunda ha evolucionado muy ligada a las capacidades técnicas del software y del hardware en cada momento y, sobre todo, a la iniciativa de los técnicos tanto en los laboratorios como en los Centros de Proceso de Datos. La seguridad informática forma parte de los sistemas de gestión en las empresas y también de los equipos informáticos domésticos y, como consecuencia, comienza a tener protagonismo en la cultura actual. La usabilidad de los sistemas informáticos se fundamenta en parámetros de disponibilidad, tiempos de respuesta, continuidad, integridad, confidencialidad y privacidad, variables que están presentes en los procedimientos y formas de hacer del mundo de la seguridad tradicional. La gestión integrada de la seguridad en la empresa es un elemento estratégico para consolidar y aumentar la confianza de los clientes en los productos y servicios que se ofrecen al mercado.

▼ **Felipe Alcántara Álvarez** es, desde octubre de 2004, Subdirector General de Seguridad Corporativa de Telefónica, dependiente de la Dirección General Adjunta de Seguridad Corporativa. Informático y con veinticinco años de servicio en la compañía, Alcántara ha sido en su más reciente trayectoria Director de Sistemas de Información Corporativos y Director de Tecnología y Redes. Entre sus principales responsabilidades ejecutivas actuales se encuentran las de la coordinación del área de Seguridad Corporativa con los Departamentos de Seguridad de las empresas del Grupo; la dirección y supervisión de la Seguridad Física y de la Seguridad de los Sistemas de Información, así como participar en los distintos Comités del Grupo donde debe figurar el área de Seguridad Corporativa.

## Hacia una mejora en la eficiencia de la gestión de la seguridad de la información.

La profusión de medios electrónicos en los entornos empresariales agiliza y hace más eficientes a nuestros negocios; como contrapartida, introducen un factor de riesgo operativo que debe minimizarse mediante la implantación de modelos de seguridad, que no siempre se gestionan de la manera más eficiente. Esta ponencia está enfocada a dar una visión del proceso de gestión de la seguridad de la información, haciendo hincapié en aquellas palancas que permiten variar su eficiencia. Se completará haciendo una revisión de lo que en los modelos actuales se presenta como poco eficiente y se propondrán varios enfoques destinados a optimizar la eficiencia en la gestión de la seguridad de la información.

▼ **Joaquín Álvarez Pérez** es Coordinador de Seguridad de la Información del Grupo Endesa. Parte de su carrera profesional la ha desarrollado en el mundo de los sistemas de información, donde ha dirigido proyectos relacionados con diversas áreas de la empresa. Durante los últimos ocho años ha centrado su actividad profesional en el desarrollo organizativo, en el diseño de los procesos de negocio y en el desarrollo de la función de seguridad de la información. Es Coordinador de Seguridad de la Información del Grupo Endesa y dirige el área de normativa de la Compañía. Además de en el sector de la energía, que es donde está actualmente, ha trabajado en el sector de las telecomunicaciones y en el de la electromedicina. Es Licenciado en Derecho, Ingeniero de Telecomunicaciones y Master en Consultoría Estratégica de las Organizaciones.

## La oficina de seguridad como modelo de gestión para las grandes organizaciones.

A lo largo de la presentación se expondrán los diferentes modelos organizativos y operativos a la hora de acometer la gestión de la seguridad TI, prestando especial atención a las Oficinas de Seguridad como el órgano encargado de gestionar la seguridad de la información mediante el diseño, implantación, monitorización y mejora continua del sistema de gestión. Además, se estudiarán los escenarios en los que resulta de interés la externalización del diseño e implantación de la Oficina de Seguridad, o incluso de su operación; y se ilustrarán los conceptos expuestos con casos prácticos.

▼ **Jesús Romero Bartolomé** es Ingeniero Superior de Telecomunicación y ha desarrollado toda su carrera profesional en el área de la Seguridad TIC. En la actualidad es el Gestor de Negocio de Seguridad TI de Indra, habiendo desempeñado con anterioridad funciones de responsabilidad en Bull España y en el Grupo Altran. A lo largo de esta trayectoria, ha participado en el desarrollo de algunas de las iniciativas emblemáticas de nuestro país en áreas tan diversas como la consultoría y gestión de seguridad, las arquitecturas técnicas de seguridad, la certificación y firma electrónica o la gestión de identidades. Romero es ponente habitual en conferencias y seminarios sobre seguridad TIC y colabora con publicaciones generalistas y especializadas.

▼ **Jorge Laredo de la Iglesia** es Consultor Senior de Seguridad TI en Indra. Ingeniero de Telecomunicaciones por la Universidad Politécnica de Madrid (UPM) y Master en Dirección de Sistemas de Información y Comunicaciones por la Universidad Politécnica de Madrid, ocupa el cargo de Consultor Senior de Seguridad TI en Indra desde el año 1999, habiendo participado y dirigido múltiples proyectos en materia de seguridad, adecuación a la legislación de protección de datos, certificación electrónica y planes de contingencia en diferentes empresas y administraciones públicas.

## El día a día en la gestión de un SGSI certificado. El ciclo de vida de los controles.

Quizás los aspectos más conocidos y *"glamourosos"* de los Sistemas de Gestión de Seguridad de la Información se encuentran en sus procesos de implantación y certificación. Sin embargo, la auténtica efectividad del Sistema sólo se obtiene por aquellas organizaciones que entienden la seguridad como un proceso más de la compañía, y conceptúan el SGSI como la herramienta básica para ese proceso, dentro del ciclo PDCA. En estas organizaciones, las fases "Verificar" y "Actuar" (las letras "C" y "A" del ciclo) están en la base de su operativa de seguridad cotidiana. Y, a pesar de ello, son las fases menos conocidas y tratadas del ciclo marcado por la normativa de referencia.

La ponencia se centrará precisamente en estos dos estados del ciclo de vida de un SGSI, analizando la operativa real del Sistema de Gestión de Seguridad de la Información de SGI, y su evolución desde la fecha de su puesta en explotación. Una evolución que puede ser medida y registrada desde un punto de vista tan práctico como el de los controles de seguridad implantados y gestionados por el Sistema.

▼ **Mariano J. Benito Gómez** es Director de Seguridad de Soluciones Globales Internet S.A. Ingeniero de Telecomunicaciones por la Universidad de Valladolid, CISA por ISACA y CISSP por (ISC)², ha desarrollado su carrera profesional en su actual compañía. En 2004 asume las funciones de Director de Seguridad de Soluciones Globales Internet, dirigiendo el proceso de implantación y certificación en diciembre de 2004 del Sistema de Gestión de Seguridad de la Información de la compañía, basado en la norma UNE 71502:2004 y la explotación del SGSI con posterioridad a esa fecha. Ha participado también en la implantación de los SGSIs de otras compañías. Anteriormente, Benito fue director de la Unidad de Negocio de Seguridad Lógica, y Responsable del Área de Seguridad Perimetral y Auditoría de Soluciones Globales Internet. Participa activamente como colaborador en medios escritos, diversas tribunas de opinión y otros foros de seguridad lógica.

DEBATE

## La contribución a la gestión de la seguridad de la información de las funciones de auditoría, control y cumplimiento normativo.

Mantener una óptima gestión de los riesgos de seguridad de la información en una entidad requiere el concurso de varias funciones vinculadas con el concepto amplio de control, entre las que ocupan un lugar relevante las de auditoría y cumplimiento normativo. La primera tiene por finalidad señalar con independencia y competencia profesional las deficiencias en la seguridad detectadas, a fin de contribuir a su mejora, en tanto que la segunda, la de cumplimiento normativo, resulta especialmente necesaria en estos tiempos de gran profusión de leyes, reglamentos y otras normas que afectan a las organizaciones y a la protección de su información y de la de terceros. En el debate se tratará de establecer la esfera de relación de estas funciones entre sí y con los departamentos de gestión de la seguridad TIC.

▼ **Carlos Bachmaier Johanning** es Responsable de Seguridad Corporativa y Auditoría IT en Sistemas Técnicos de Loterías (STL). Dr. Ingeniero Aeronáutico (1984) y profesor titular universitario, fue socio fundador de GMV y SGI Soluciones Globales Internet, compañías en las que ha desarrollado 20 años de actividad profesional. En 1998 se incorpora a Sistemas Técnicos de Loterías, entidad en la que viene ejerciendo actividades de Tecnología y Seguridad. Bachmaier es CISA y CISM por ISACA.

▼ **Carlos Escudero Rivas** es Director del Centro de Calidad, Auditoría y Seguridad de la GISS –Gerencia de Informática de la Seguridad Social–. Licenciado en Ciencias Físicas y postgrado en informática por la Universidad de Zaragoza y master DISTIC por el INAP y la UPM, ha desarrollado su carrera profesional en el ámbito TIC de la administración pública. Encuadrado en la estructura de la SGI, ha trabajado en distintos departamentos, incorporándose a su último cargo desde la dirección de Producción y Sistemas.

▼ **Fernando Hervada Vidal** es Presidente de ASIA (Asociación de Auditores y Auditoría y Control de Sistemas de Información), capítulo de Madrid de ISACA. Licenciado en Ciencias Matemáticas por la Universidad Complutense de Madrid y CISA por la ISACA, ha trabajado como analista de aplicaciones en el Departamento de Sistemas de la Bolsa de Madrid y posteriormente en el de Endesa como jefe de proyectos, desarrollando e implantando diferentes aplicaciones de gestión. Actualmente es Subdirector de Auditoría de Sistemas de Información de Endesa, perteneciente a la Dirección de Auditoría Interna de esta compañía. Hervada participa como ponente en diferentes cursos y seminarios relacionados con la Auditoría de Sistemas en la UCLM, Instituto de Auditores Internos e Instituto de Empresa, entre otros.

## El impacto de la implantación de la gestión de identidades en una corporación.

Las ventajas de la implantación de sistemas de gestión de identidades son muchas y conocidas. Por ello, existen organizaciones que se han lanzado frenéticamente a recorrer el ansiado camino de la implantación de complejos sistemas de *Single Sign-On*, creyendo que de esta forma su modelo de gestión de identidades quedaría resuelto. Desde una perspectiva global, el paraguas de soluciones de los proyectos de IdM son mucho más amplias que el SSO, pasando por la implantación de un modelo de perfiles, roles y autorizaciones de acceso a la información. En algunas ocasiones, un enfoque meramente tecnológico ha llevado a errar en las previsiones, prolongando los proyectos en el tiempo e incluso llegando al fracaso. Un factor crítico de éxito clave en este tipo de proyectos consiste en tener siempre presentes a los principales involucrados en dichos proyectos: las personas. Un proyecto de estas características no sólo consiste en la implantación de medidas técnicas, sino mayoritariamente organizacionales, procedimentales y de convencimiento y venta interna hacia los usuarios de las mismas. El éxito, pues, radica en trabajar conjuntamente con tres pilares básicos: los procesos, las personas y la tecnología. En la ponencia se pondrán de relieve los diferentes factores a valorar para llevar a "buen puerto" una implantación de IdM.

▼ **Juan José Míguez Iglesias** es Gerente del Área de Servicios de Seguridad de la Información de la División Advisory de PricewaterhouseCoopers. Ingeniero de Telecomunicación (especialidad Telemática), su trayectoria profesional ha discurrido durante más de ocho años realizando proyectos relacionados con la seguridad, el control y auditoría de los sistemas de información. Mantiene las certificaciones CISM, CISA y Lead Auditor BS 7799-2 y es miembro de ASIA.

## Qué debe y qué no debe tener un cuadro de mando de seguridad de la información.

Un cuadro de mando es una herramienta de gestión. La información es un bien precioso y no precisamente escaso que soporta muchas actividades empresariales y servicios a sus usuarios. Para el tratamiento de la información dependemos de medios técnicos, a menudo incontables, frecuentemente complejos y no siempre bajo nuestra directa responsabilidad. El cuadro de mando, como la cabina del piloto, permite al gestor saber cómo estamos actualmente, si progresamos adecuadamente y si hay nubes en lontananza; para que las decisiones no sean ciegas sino informadas y los peligros no nos sorprendan sino que nos encuentren prudentemente preparados. Los niveles de gestión dentro de una organización son múltiples: desde la gestión de la carrera profesional de cada trabajador hasta la dirección general; pero todos los que tienen opciones necesitan una estrategia para decidir y una información adecuada a las decisiones que deben tomar. Y no olvidemos que los sistemas de información son cada vez menos independientes y la confianza en que la información necesaria esté en el sitio adecuado en el momento adecuado, el de la decisión, se ve amenazada por mis decisiones y por las de los demás, interconectados, a los que habrá que exigir responsabilidad, calidad y prudencia, quizás verificando que, efectivamente, hay alguien al mando.

▼ **José Antonio Mañas Argemi.** 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 en el 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), ha participado igualmente en el desarrollo de la metodología para el análisis y la gestión de riesgos Magerit y en el de la herramienta de apoyo Pilar.

## El enfoque de la ISO/IEC WD 27004, Métricas y medidas para la gestión de la seguridad de la información.

El proyecto de Norma 27004 pretende facilitar la gestión de un SGSI proporcionando una metodología para definir los objetivos de implantación y los criterios de eficacia, trazando y midiendo su evolución en el tiempo como parte del sistema de gestión. Se trata de una norma que especifica métricas (Information Security Management Metrics and Measurements), técnicas de medida y un programa de métricas que tiene por objetivo medir la eficacia del ISMS, sus procesos y los controles implantados. En el momento presente de edición, la norma forma parte del grupo de normas de gestión de la seguridad SI 27000 y, en consecuencia, se considera referencia para la implantación de un SGSI ex 27002.

▼ **Paloma Llaneza González** es miembro del GT1 del Subcomité de Aenor (AEN/CTN 71/SC27/Wg1 Tecnologías de la Información) y Project Editor de la ISO/IEC WD 27004. Abogado en ejercicio y socio de Llaneza y Asociados Abogados, es asimismo Secretaria de la Junta Directiva de la Asociación de Auditores y Auditoría y Control de los Sistemas y Tecnologías de la Información y Comunicaciones (ASIA) y del capítulo de Madrid de la ISACA. Es Miembro del Subcomité 27 de Aenor (AEN/CTN 71/SC27 Tecnologías de la Información), donde se estudian y aprueban las normas NE en esta materia. En la reunión internacional de ISO de octubre de 2004 en Fortaleza (Brasil) fue nombrada co-editora de la norma internacional ISO de Métricas de seguridad de gestión de sistemas de información.

DEBATE

## Las medidas de seguridad en el futuro Reglamento de protección de datos.

Todo indica que la legislación española sobre protección de datos personales va a experimentar un cambio transcendente toda vez que se apruebe y entre en vigor el denominado Reglamento de Protección de Datos de Carácter Personal, en el que se contemplan, entre otras, nuevas medidas de seguridad de gran calado y modificaciones en las actualmente vigentes. En el debate propuesto se tratará de establecer el alcance de la futura adaptación a los cambios esperados, y su impacto en los planes de gasto e inversión de las organizaciones y en sus áreas organizativas más concernidas, como son las de gestión de las tecnologías de la información y las comunicaciones y las de gestión de la seguridad de la información.

▼ **Tomás Arroyo Salido** es Responsable de Calidad de Servicio y Control Interno de Sistemas Europa en BBVA. Cuenta con más de 28 años de experiencia en informática, de los cuales 20 se han desarrollado en puestos de Control en BBVA. Auditor CISA por la ISACA, Diplomado en Auditoría de la Información y en Dirección de Seguridad de la Información por la UAM, posee diversos estudios de Derecho en la UNED y es Evaluador de Calidad (modelo EFQM). Arroyo es miembro fundador de ASIA y Secretario General del Grupo de Usuarios de IBM, además de colaborador, articulista y ponente en mesas redondas, grupos de usuarios y presentaciones de diversos foros, así como en cursos de verano y programas de formación de la UNED y la UPM.

▼ **María José Blanco Antón** es Subdirectora General del Registro General de Protección de Datos de la Agencia Española de Protección de Datos. Licenciada en Ciencias Matemáticas por la Universidad Autónoma de Madrid, pertenece al Cuerpo Superior de Sistemas y Tecnologías de la Información de la Administración del Estado. Blanco Antón ha desempeñado diferentes puestos en la Agencia Española de Protección de Datos, ocupando en la actualidad el de Subdirectora General del Registro General de Protección de Datos.

▼ **Francisco Javier García Carmona** es Director del departamento de Seguridad de la Información y las Comunicaciones de Iberdrola. 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 1996, simultaneando la dirección de Operaciones con funciones técnicas. En el año 2001 se incorporó a Iberdrola como Director del departamento de Seguridad de la Información y las Comunicaciones.

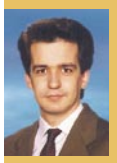
## La medición del riesgo y la respuesta temprana.

La medición del riesgo es, en sí misma, un labor no exenta de dificultades y, en muchas ocasiones, un objetivo con entidad propia. Esta medida no arroja como dato un único valor, sino que se trata de una medida multidimensional en la que cada dato puede incluso corresponder al riesgo medido para cada uno de nuestros clientes. Desde un punto de vista más amplio, el riesgo puede ser considerado un indicador que regula la respuesta que la organización ha de dar ante él mismo. Este proceso hace que nos encontremos preparados para actuar en todos y cada uno de los supuestos de riesgo. Por tanto, la combinación de "medida del riesgo", de la forma más granular y automática posible, y la adecuación de la respuesta (técnica, logística, organizativa, comunicativa, etc) de toda la organización ante el mismo, nos abren la puerta hacia una gestión integral de la seguridad, en la que las respuestas son función directa de los incidentes, minimizando la improvisación a lo justo y necesario como proceso creativo.

▼ **Pedro Castillo Muros** es desde enero de 2000 Director Técnico de Seguridad Informática en Bankinter. Estudió Ciencias Químicas en la Universidad Complutense de Madrid. Desde 1992 hasta 1996 trabajó en los servicios de Informática de la Universidad Complutense como administrador de sistemas. Desde 1996 hasta diciembre de 1999 trabajó en Webline S.L. empresa fundada junto a otros compañeros y dedicada al desarrollo de aplicaciones Internet y consultoría de sistemas y seguridad.

## Experiencias en la creación de cuadros de mando de seguridad de la información.

El Cuadro de mando integral (CMI), o también conocido como *Balanced Scorecard* (Robert Kaplan y David P. Norton), consiste en un sistema de gestión estratégica que permite y soporta el proceso de toma de decisiones de una organización en base a la monitorización periódica de indicadores clave. Referido a la seguridad de TI, los principales objetivos buscados en un CMIS serían: evaluar y justificar el valor de la función de seguridad dentro de la organización, actuar como herramienta de soporte a la toma de decisiones y servir como herramienta de control interno para la mejora continua de los aspectos relativos a la gestión de la seguridad.
Esta ponencia abordará, desde la propia experiencia en proyectos, los aspectos más importantes en la creación de un CMIS: identificación de perspectivas, definición de la estrategia, identificación de objetivos e indicadores, identificación de iniciativas y métricas, elaboración del mapa estratégico y de la red causal. Dada la gran cantidad de información manejada, es imprescindible para el éxito de un proyecto de cuadro de mando de seguridad el empleo de infraestructura automatizada específica (p.e., *Metriges*, análisis estadístico para identificar correlaciones entre componentes).



▼ **Luis Sáiz Gimeno.** Con una década de experiencia en protección de la información, este Ingeniero de Telecomunicaciones, poseedor de las certificaciones CISA y CISSP, inició su andadura profesional en el Grupo BBVA en octubre de 2000 en el departamento de Seguridad Lógica de uno-e Bank. Seis meses después, entró a formar parte del equipo responsable de Seguridad Lógica en BBVA. Actualmente en Responsable de los Procesos de Seguridad y Control Interno Corporativo dentro de la Dirección de Seguridad Lógica Corporativa del Grupo BBVA.

▼ **Rafael Ortega García** es desde noviembre de 2004 Director de Continuidad de Negocio y Seguridad de la compañía Azertia Consulting. Ortega tiene una larga experiencia en el sector de seguridad TIC, ámbito en el que 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.

▼ **Rosa María García Ontoso**

es Asesora Adjunta al Gerente de Informática de la Comunidad de Madrid (ICM). Licenciada en Ciencias Matemáticas, durante los tres últimos años ha dado asesoramiento técnico y organizativo, y en seguridad y en materia de protección de datos a las Direcciones Generales de Informática Sanitaria e Innovación Tecnológica y de Farmacia y Productos Sanitarios. Con anterioridad fue la primera mujer directora de una Agencia de Protección de Datos en España y la primera directora de una Agencia de Protección de Datos autonómica, la de Madrid. Forma parte de ASIA/ISACA Capítulo de Madrid, en donde es vocal de la Junta Directiva, y desde noviembre de 2004 preside el Subcomité Técnico de Seguridad JTC1/SC27, del que ha formado parte durante los últimos diez años.

▼ **Mar Sánchez Caro** es

Responsable de Seguridad de BT Global Services España. Con una experiencia de más de diez años vinculada a las tecnologías de la información, actualmente ocupa el cargo de Country Security Manager en BT Global Services España. Entre sus responsabilidades están la coordinación del Comité de Seguridad corporativo, la implantación de proyectos de seguridad, la coordinación del Gabinete de Crisis, la responsabilidad en materia de Protección de Datos y la relación internacional con la empresa matriz.

## Cómo enlazar la seguridad TIC con los procesos de buen gobierno corporativo.

Aunque el gobierno corporativo está definido y regulado de manera diferente en distintas parte del mundo, su objetivo final es el mismo: ayudar a gestionar organizaciones perdurables, capaces de responder ante sus grupos de interés, generar valor y ser merecedores de confianza en el mercado.
En este sentido, la seguridad de los sistemas de información se convierten en un elemento clave, que como un reto de buen gobierno, debe permitir un marco más amplio relativo a: 1) cumplir con la regulación creciente; 2) mejorar los procesos de gobierno, dirección estratégica, gestión de riesgos, supervisión y evaluación; 3) comunicar la cultura corporativa, y 4) proteger los intereses de los *"stakeholders"*.
A través de estos retos, se intentarán despejar las directrices de hacia dónde se dirigen los requerimientos de las organizaciones en materia de seguridad informática, y lo que es más interesante, en qué dirección quieren avanzar.

▼ **Ramón Poch Vilaplana**, 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 Nestlé, siendo trasladado como responsable de Auditoría Interna Informática a la sede mundial de Nestlé en Suiza. Posteriormente, se incorporó a KPMG como Gerente del grupo de Information Risk Management en Barcelona. Actualmente es Director de la actividad en España. Poch es ponente habitual en materia de Auditoría Informática en el Instituto de Auditores Censores Jurados de Cuentas de España, así como del Instituto de Auditores Internos. Finalmente, es profesor de Auditoría Informática de la Universidad de Barcelona, así como de otros foros.

ESPACIO TiSEC 2005

AFORO LIMITADO

## Fecha y lugar

Espacio TiSEC 2004 tendrá lugar los días 23 y 24 de noviembre de 2005 en el Hotel NOVOTEL*. Campo de las Naciones de Madrid.

## Derechos de inscripción

Los asistentes inscritos en Espacio TISEC 2005 recibirán la carpeta de documentación con las ponencias así como un CD-Rom con la información en formato digital.

Almuerzos y cafés.

Diploma de asistencia.

## Cuota de inscripción

| | |
|---|---|
| Hasta el 5 de noviembre | **661 € + 16% IVA** |
| Después del 5 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 91 575 83 24 |
| | +34 91 575 83 25 |
| Por fax: | +34 91 577 70 47 |
| 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
Goya, 39 - 28001 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 Espacio TiSEC que deseen alojarse en el hotel Novotel con motivo de su asistencia a Espacio TiSEC. Este particular deberá ser comunicado a la entidad organizadora con la debida antelación.

Las inscripciones sólo se considerarán formalizadas una vez satisfecho el importe de las mismas antes de la celebración de Espacio TiSEC.

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 Espacio TiSEC 2005

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 en Espacio TiSEC 2005
Firma:

Forma de pago: ❑ Talón ❑ Transferencia

Los datos personales que se solicitan, cuya finalidad es la formalización y seguimiento de su inscripción en Espacio TiSEC 2005, 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/. Goya, 39. 28001 Madrid.

>>> Información e inscripciones:

Revista SIC seguridad en informática y comunicaciones

**Ediciones CODA / Revista SIC**
Goya, 39 · 28001 Madrid (España)
Tel: 91 575 83 24 / 25 · Fax: 91 577 70 47
Correo-e: info@revistasic.com / info@codasic.com
Sitio: www.revistasic.com/tisec