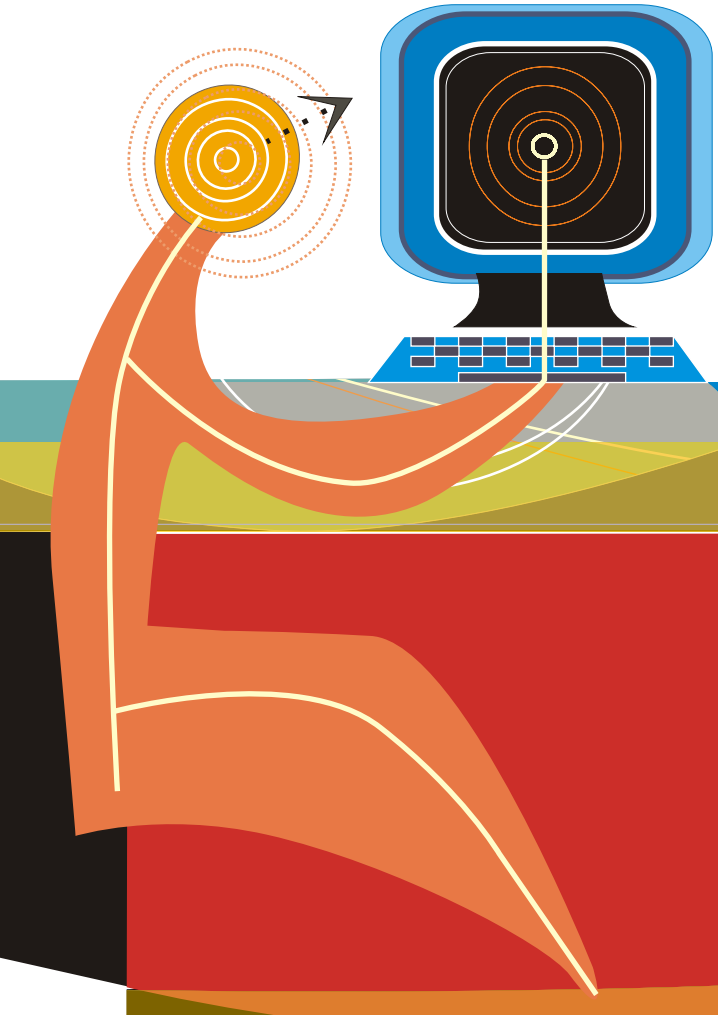
ESPACIO TISEC 2004

24 y 25 de noviembre de 2004
Hotel Novotel
Campo de las Naciones
Madrid

La protección bien entendida:

¿qué hacer con la seguridad?



www.revistasic.com/tisec

Programa

Organiza

REVISTA SIC seguridad en informática y comunicaciones

ESPACIO TiSEC 2004

La protección bien entendida: ¿qué hacer con la seguridad?

Una de las batallas que tienen que librar en sus organizaciones los responsables de ese componente esencial de la gestión del riesgo que es la seguridad de la información, sustantivada hoy de forma casi exclusiva en la parcela multiforme de la seguridad de los sistemas de información y las comunicaciones, es la de su ubicación y competencias en la maquinaria corporativa.

Dicho de un modo más directo: los profesionales de la seguridad de los sistemas de información y las comunicaciones tienen ahora que ganarse su sitio en la empresa, tras haber salido victoriosos del primer asalto: el de la justificación de la necesidad de la existencia permanente de la función específica de seguridad TIC.

Para contribuir a la mejora profesional y con la intención de intentar avanzar con ánimo contructivo en el fortalecimiento de la profesión y de su mejor ejercicio en la empresa, la revista SIC va a organizar los días 24 y 25 de noviembre del presente en Madrid la segunda edición de Espacio TiSEC. En su marco, reputados profesionales de la seguridad TIC van a abordar por primera vez asuntos de gran relevancia presente y futura en línea con lo dicho, tales como, entre otros, las posibilidades de medir el riesgo y la gestión en la seguridad de la información, los conjuntos de indicadores técnicos y de operación, los conjuntos de indicadores organizativos, la auditoría hoy y su papel en la eficacia y la eficiencia de los controles, el día a día de la gestión y la planificación a medio y largo plazo, y la confrontación del modelo de SGSI certificables con el de auditoría externa de SGSI, entre otros.

Igualmente, se llevará a cabo un debate en el que destacados responsables de seguridad TIC de organizaciones confrontarán sus opiniones acerca de las competencias y atribuciones de los departamentos especializados en la protección.

Siempre hay un momento en el desarrollo de un sector profesional en el que para ser competitivo en la empresa, lo esencial es saber encontrarle un sentido transmisible a la función que nos ha sido encomendada, y para ello es necesario dotarla de contenido y utilidad, y saber evolucionarla a los ritmos que marquen las actividades y negocios de la organización. Ese es hoy el gran reto profesional de la seguridad TIC.

Organiza

REVISTA SIC seguridad en informática y comunicaciones

Copatrocinan

AZERTIA

ERNST & YOUNG Quality In Everything We Do

Indra

KPMG

PRICEWATERHOUSECOOPERS

SGI

Programa

24 de noviembre

08:45h. Entrega de documentación.

09:00h. Acto de inauguración.

09:15h. Presentación: **Seguridad TIC: dónde estamos hoy.**
Ponente: **José de la Peña Muñoz.**
Director de la Revista SIC.

09:45h. **¿Qué información requiere el director de sistemas para gestionar los riesgos de seguridad del sistema tecnológico que gobierna?**
Ponente: **Jesús Marquina.** Director de Sistemas de Información. Bankinter.

10:15h. Coloquio.

10:25h. **Límites a la externalización de la operación de los sistemas tecnológicos de protección.**
Ponente: **Manuel Palau.** Responsable de Seguridad Informática y Proyectos Especiales.
Dirección de Sistemas. Iberdrola.

11:10h. Coloquio.

11:20h. Pausa-café.

11:50h. **El riesgo como métrica de las decisiones de gasto en seguridad TIC.**
Ponente: **José Antonio Mañas.** Catedrático de Ingeniería Telemática. ETSI de Telecomunicación de la Universidad Politécnica de Madrid.

12:35h. Coloquio.

12:45h. DEBATE:
¿Debe el departamento de seguridad TIC operar los sistemas de protección de la empresa?
Participantes:
- **Raúl Bretón Pérez.** Gerencia de Seguridad de Redes y Servicios. Telefónica Móviles España.
- **Javier del Riego.** Jefe de Seguridad Lógica. Vodafone España.
- **Diego Sacristán.** Responsable de Seguridad y Calidad de la Información. Pfizer.

14:30h. Almuerzo.

16:30h. **Seguridad TIC: de la gestión por impulsos a la planificada, o cómo conseguir que lo urgente no desplace a lo importante.**
Ponente: **Pedro Pablo López Bernal.** Gerente de Infraestructura y Seguridad. R.S.I. - Grupo Caja Rural.

17:15h. Coloquio.

17:25h. **La auditoría como pieza indispensable en el ajuste continuo de la eficacia y la eficiencia de los controles.**
Ponente: **Marc Martínez.**
Director de Technology and Security Risk Services de Ernst & Young.

18:10h. Coloquio.

18:20h. Fin de la primera jornada.

25 de noviembre

09:15h. Inicio de la jornada.

09:30h. **Seguridad TIC: ¿qué hay que medir?**
Ponente: **Daniel Barriuso.** Director de Seguridad de la información. Credit Suisse España.

10:15h. Coloquio.

10:25h. **Conjuntos de indicadores técnicos y de operación.**
Ponente: **Javier Osuna.** Jefe de la División de Auditoría y Planificación de la Seguridad. Soluciones Globales Internet.

11:10h. Coloquio.

11:20h. Pausa-café.

11:50h. **Conjuntos de indicadores organizativos.**
Ponente: **Rafael Ortega.** Director de Continuidad de Negocio y Seguridad. Azertia.

12:35h. Coloquio.

12:45h. **La venta interna de iniciativas de seguridad: métricas, indicadores y otros argumentos.**
Ponente: **Jesús Romero.** Gestor de Negocio de Seguridad TI. Indra.

13:30h. Coloquio.

13:40h. **La integración de la seguridad TIC en los procesos de negocio.**
Ponente: **Elena Maestre García.** Responsable de los Servicios de Seguridad de la información de PricewaterhouseCoopers.

14:25h. Coloquio.

14:35h. Almuerzo.

16:30h. **SGSI: modelo de certificación vs modelo de auditoría externa.**
Ponente: **Ramón Poch.** Director de Information Risk Management. KPMG.

17:15h. Coloquio.

17:25h. **Datos personales: riesgos asociados en sistemas y aplicaciones.**
Ponente: **Tomás Arroyo.** Responsable de Calidad de Servicio y Control Interno. BBVA.

18:10h. Coloquio.

18:20h. Clausura.

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

Seguridad TIC: ¿dónde estamos hoy?

Durante el último decenio, el fulgurante desarrollo de las TIC y su papel indiscutible como soporte de los negocios y las actividades de las empresas, han ido acompañados de una creciente necesidad de gestionar los riesgos de seguridad de la información y de los sistemas tecnológicos que la tratan. En este contexto, se ha desarrollado una industria específica y puntera en I+D+i, que las grandes compañías generalistas de TIC tratan de fagocitar para ser más competitivas. Al tiempo, ha florecido una nueva especialización profesional, la de los expertos en seguridad, que ya como miembros de equipos estables en departamentos de sistemas de empresas y administraciones públicas, ya en el ámbito de la consultoría y la integración, se han convertido en insustituibles. Sus retos, hoy, pasan por ajustar permanentemente la gestión de los riesgos de seguridad a la dinámica de las organizaciones en la que prestan sus servicios, un objetivo esencial para conseguir la mayoría de edad.

José de la Peña Muñoz es Licenciado en Ciencias de la Información, rama de Periodismo, por la Universidad Complutense de Madrid. Desde 1992 es director de la revista española SIC Seguridad en Informática y Comunicaciones. Igualmente forma parte del Equipo de Organización de Securmática, Congreso anual de Seguridad en Tecnologías de Información y Comunicaciones, y de Espacio TiSEC.
De la Peña ha participado como ponente en numerosos cursos, congresos y seminarios nacionales e internacionales sobre seguridad de la información, control y auditoría de seguridad de sistemas. Actualmente es miembro de Isaca y de su Capítulo de Madrid, Asia (Asociación de Auditores y Auditoría y Control de los Sistemas y Tecnologías de la Información y Comunicaciones), y de CriptoRed.

Límites a la externalización de la operación de los sistemas tecnológicos de protección

Asociada a la tendencia empresarial de externalizar las funciones de las tecnologías de la información, el ámbito de las actividades de seguridad de la información no se sustrae a dicha tendencia, pese a la sensibilidad del tema. Ha surgido un mercado en el que los proveedores ofrecen este tipo de servicios y por supuesto clientes que los contratan.

Algunos de los temas sobre los que reflexionar son: ¿cuáles son las causas, tanto tecnológicas como operativas, que impulsan este nuevo mercado?, ¿qué criterios generales podemos aplicar?, ¿qué estrategia podemos seguir y reservarnos ciertas prerrogativas si optamos por contratar servicios de este tipo?, ¿son suficientes los tradicionales SLA's?, ¿todas las actividades son susceptibles de externalizarse?, ¿es la gestión de la seguridad una *'commodity'*?

Manuel Palau Rolduá es responsable de Seguridad Informática y de Proyectos Especiales en la Dirección de Sistemas de Iberdrola. Desde 1994 ha ocupado distintas posiciones relacionadas con la seguridad en el equipo de dirección de la función informática de Iberdrola o en Iberdrola Sistemas, compaginándolas con otras relativas a la calidad, a la innovación tecnológica, al control de gestión y al desarrollo de sistemas. Es miembro del grupo ICCP Task Group on Security de BIAC (Business and Industry Advisory Committe), organismo asesor de la O.C.D.E.

¿Qué información requiere el director de sistemas para gestionar los riesgos de seguridad del sistema tecnológico que gobierna?

El ajuste fino y la mejora permanente de la gestión de la seguridad de la información y de los sistemas tecnológicos que la tratan es una de las diversas responsabilidades que tienen hoy los directores de sistemas en tanto que gestores y responsables globales del sistema de información de su organización. En la ponencia se tratará de contextualizar el concepto de seguridad TIC en este nivel de abstracción directiva con una perspectiva histórica y evolutiva, y proyectarlo hacia lo previsible tras repasar la situación actual, su dimensión, su impacto, y los requisitos técnicos y humanos que son necesarios para proporcionar a un CIO y a la entidad que representa unos niveles de seguridad suficientes y soportables.

Jesús Marquina Cogolludo. Director de Sistemas de Información de Bankinter. Licenciado en Informática por la Universidad Politécnica, inició su carrera profesional en el Banco Exterior, institución que abandonó en 1987 siendo Director de Producción para asumir las responsabilidades de Fundador, Director de Producción y miembro del Comité de Dirección de la entonces denominada Rural Informática, la actual Rural Servicios Informáticos (RSI). En 1989 ingresó en Bankinter para dirigir un proyecto de migración de sistemas, y en 1991 fue nombrado Director de Sistemas de la entidad financiera.

El riesgo como métrica de las decisiones de gasto en seguridad TIC

Siempre se dice; pero no siempre se hace. Un análisis de riesgos que indique a qué estamos expuestos, en qué medida y qué hemos hecho para que esa exposición sea asumible. El gasto que la organización ha realizado en salvaguardas (técnicas y no técnicas), el coste en productividad que supone seguir unas reglas de operación segura, ¿está justificado? ¿Tenemos que gastar más? Exactamente, ¿qué es eso llamado riesgo residual? Conocer las insuficiencias en la defensa de nuestro sistema de información es el fundamento de una confianza razonada y de un gasto responsable.

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 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).

Seguridad TIC: de la gestión por impulsos a la planificada, o cómo conseguir que lo urgente no desplace a lo importante

En la ponencia se explicarán las iniciativas de Rural Servicios Informáticos (RSI), tanto en la organización de la seguridad TIC como en los proyectos y orden de los mismos a acometer, con el fin de caminar y avanzar, de forma sistemática, planificada y controlada en la gestión proactiva de la protección. También, se abordarán asuntos específicos, tales como la necesidad real de la seguridad (para el negocio, para las personas y en sus relaciones con el medio); la seguridad tradicional *versus* la seguridad gestionada (evolución de la seguridad), y cómo llegar a la seguridad gestionada en el reto del día a día (evaluación, diseño, planificación, implantación y despliegue). Igualmente se dará cuenta de los principales proyectos de RSI (pasados, presentes y futuros) y se aportará una visión a futuro de la seguridad TIC (externalización de funciones y servicios, experiencia y visión).

Pedro Pablo López Bernal es Gerente de Infraestructura de Seguridad y Auditoría de Rural Servicios Informáticos, empresa que presta los servicios de *outsourcing* global a las Cajas Rurales y Empresas Participadas que forman el Grupo Caja Rural (más de 73 Entidades Financieras y Seguros). Técnico Informático desde 1986, posee un Master en Auditoría Informática desde 1991 y es auditor Cisa por la Isaca. Ha trabajado en los últimos 19 años en los servicios informáticos de empresas tales como: Entel, Citibank, Banco Santander y RSI, desarrollando diversos puestos y funciones. En RSI desde 1988, ha desempeñado funciones de Responsable de Aceptación, Planificación y Automatización de la Explotación y Almacenamiento, Soporte Técnico a Desarrollo y Sistemas, y Gerente de Infraestructura Tecnológica, etc. En la actualidad es el Responsable a nivel Corporativo de Grupo Caja Rural (RSI) de la Infraestructura de Seguridad y Auditoría (Arquitectura, Física, Lógica, Control Interno, y Auditoría), además de miembro del Comité de Seguridad y Salud, Comité de Informática y varios Grupos de Trabajo de CCI, IBM y Swift. Como Responsable de Seguridad Corporativa, ha diseñado y está llevando a cabo la implantación del Plan Director de Seguridad Corporativa tanto para RSI como para las Entidades en la que ésta presta sus servicios, conforme a los requerimientos y objetivos marcados y en base a una política y una metodología de implantación propias.

La auditoría como pieza indispensable en el ajuste continuo de la eficacia y la eficiencia de los controles

Se realizará una exposición de los nuevos riesgos que afectan a las empresas con motivo de los cambios en las tecnologías utilizadas y que dan lugar a nuevas necesidades de control, ya no siendo suficiente con revisiones y auditorías tradicionales de los sistemas de información. La experiencia de Ernst & Young indica que deben incluirse técnicas avanzadas como auditorías remotas, internas y externas, auditorías de *hacking wireless* (una tecnología cada vez mas extendida en distintos sectores), *honey pots* y analisis forense (es necesario conocer qué hace un potencial atacante para mejorar la defensa), etc.

Durante la conferencia se incidirá también en la necesidad de realizar este tipo de revisiones e incluso en incluirlas en el plan anual de auditoría, para complementar las más tradicionales, al objeto de asegurar todo el perimetro de riesgo y al mismo tiempo asegurar que no se están olvidando del examen rutinario puertas de acceso importantes. Igualmente, se evidenciará la necesidad de poder medir todo esto mediante la implantación de métricas desarrolladas *ad-hoc*.

Marc Martínez Marce es Director del departamento de Technology and Security Risk Services de Ernst & Young. Martínez, licenciado en Ciencias Económicas y Empresariales, Actuario de Seguros y Auditor Informático Certificado Cisa y asociado a la Isaca, cuenta con más de doce años de experiencia en el campo de la auditoría y la seguridad informática. Durante estos años ha desarrollado su trabajo en las oficinas de Ernst & Young en Barcelona, Madrid y Los Angeles.

DEBATE

¿Debe el departamento de seguridad TIC operar los sistemas de protección de la empresa?

La forma en la que se están conformando los departamentos de seguridad TIC en lo referente a sus competencias, no es uniforme. Algunos cumplen una labor consultiva y prescriptora, en tanto que otros, además, operan todos o parte de los sistemas tecnológicos de protección TIC existentes, o bien mantienen un control directo de la operación por terceros. ¿Cuál es el mejor modelo posible para conseguir la eficacia y unos niveles de eficiencia óptimos en el cumplimiento del objetivo final que se persigue, es decir, gestionar el riesgo de seguridad del sistema de información tecnológico de la organización? ¿Qué tendencias se vislumbran en la materia? ¿Qué ventajas y qué inconvenientes plantean los distintos enfoques?

Raúl Bretón Pérez es experto en seguridad en la Gerencia de Seguridad de Redes y Servicios de Teléfonica Móviles España. Ingeniero Técnico de Telecomunicaciones por la Universidad de Alcalá de Henares e Ingeniero de Telecomunicaciones por la UPC, en su haber profesional acarrea una extensa formación y experiencia en gestión y despliegue en los ámbitos de la seguridad TI, las redes IP y MPLS, los sistemas y aplicaciones más tradicionales, en los entornos web, y muy especialmente en los nuevos entornos de comunicaciones. Comenzó su andadura profesional en 1993 en Telefónica de España en los departamentos de RedesX25, y en 1996 pasó a Telefónica Móviles España para colaborar en el despliegue de las herramientas de planificación y gestión de la red GSM. En 1998 pasó a trabajar como experto en sistemas y comunicaciones en las áreas de Nuevos Servicios de Valor Añadido de la compañía. Finalmente, en 2001 inició las actividades de seguridad de red y servicios, donde ha estado definiendo e implantando las políticas y herramientas de seguridad de TME en los departamentos de Red y Servicios. Entre las actividades desarrolladas en este ámbito destacan el diseño y despliegue de plataformas de monitorización de seguridad, el desarrollo de políticas de gestión de usuarios, el desarrollo de políticas de segmentación y arquitecturas de red y, últimamente, la definición de los procedimientos y herramientas para valoraciones dinámicas de riesgo.

Javier del Riego Fernández es Jefe de Seguridad Lógica de Vodafone España. Licenciado en Informática por la Universidad Politécnica de Madrid, inició su carrera profesional en Media Planning, fuera del ámbito de la seguridad tecnológica. A principios de 1994 se incorporó a Caja Madrid como auditor informático dentro de la unidad de Auditoría, en la que se responsabilizó de la ejecución y seguimiento de auditorías técnicas, tanto de la matriz como de las empresas de la corporación. A finales de 1997 da el salto a Seguridad Lógica de Vodafone España –por aquel entonces Airtel Móvil–, donde desde finales de 1998 asume la responsabilidad de la gestión del equipo, que abarca actualmente la seguridad de todos los procesos tecnológicos de la compañía.

Diego Sacristán Sifredi es Responsable de Seguridad y Calidad de la Información de Pfizer. Su trayectoria profesional se inició en el desarrollo de sistemas de información, especializándose posteriormente en la seguridad de la información y sistemas asociados, ámbito en el que desarrolló su actividad en PricewaterhouseCoopers; posteriormente se incorporó a la multinacional biomédica Pfizer como Responsable de Seguridad y Calidad de la información. Sacristán es Licenciado en Ciencias Económicas y Empresariales por la UCM y CISSP.

Seguridad TIC: ¿qué hay que medir?

El modelo de gestión de las TIC y la Seguridad está cambiando muy rápidamente en los últimos años. Hemos pasado de un esquema basado en la innovación tecnológica y la carrera de armas, a un modelo cimentado en la evaluación y control de las inversiones. En el pasado el miedo, la incertidumbre y la duda (FUD) han sido suficientes para justificar las inversiones en seguridad, pero actualmente, bajo la creciente demanda de análisis coste/beneficio en el mundo empresarial, las métricas juegan un papel fundamental en la gestión de la seguridad.

La presentación abordará, desde un punto de vista basado en la experiencia propia, los siguientes aspectos: el papel de las métricas en la gestión de la seguridad, los factores de los que depende la elección de las métricas a utilizar, los tipos de indicadores que resultan más eficaces para distintos propósitos, y el uso de las métricas en el proceso de mejora continua de la organización.

Daniel Barriuso Rojo es actualmente Responsable de Seguridad de la Información de Credit Suisse España. Con una experiencia de más de 10 años en Seguridad y TIC, la prioridad de Barriuso se centra en los aspectos organizativos de la seguridad, tales como el gobierno, la estrategia y la gestión del riesgo. Además de las responsabilidades locales en España, forma parte del "Regional Information Security Strategy Team" de Credit Suisse y participa en diversos foros e iniciativas en el ámbito internacional. Desde 2002, imparte clases como profesor en el Master de Seguridad y Auditoría de la Universidad Politécnica de Madrid (UPM-ALI) sobre áreas tales como el gobierno y la gestión de la inversión en seguridad. Barriuso es Ingeniero Superior en Informática por la Universidad Carlos III de Madrid y está certificado como Lead Auditor BS7799.

Conjuntos de indicadores organizativos

"Gestión" es un vocablo que se está utilizando en demasiados contextos, desde el de la gestión de usuarios, hasta el de la seguridad gestionada. El Diccionario de la Lengua Española define gestionar "*Como acción o diligencias conducentes al logro de un negocio o un deseo cualquiera*"; por tanto, indicadores de gestión serían todo tipo de indicadores (técnicos, operativos, organizativos) que permitan cumplir los objetivos de seguridad marcados por la compañía. En este caso, se dedicará la ponencia a los indicadores organizativos.

Puntos fundamentales antes de decidir qué indicadores quiero recoger, son que la compañía tenga claro los objetivos de seguridad, a dónde quiere llegar y que métricas derivadas de los objetivos debe monitorizar, antes de definir qué tipo de indicadores, en este caso organizativos, debe recoger. Ejemplos de ellos, pueden ser considerados el grado de eficacia del plan de concienciación, el grado de implantación de la normativa de seguridad, la eficacia de la gestión de incidentes, los tiempos de respuesta que se obtienen en las pruebas del plan de contingencia, etc.

Rafael Ortega García es desde noviembre del presente 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.

Conjuntos de indicadores técnicos y de operación

La definición del Conjunto de Indicadores Técnicos y de Operación de Seguridad se ha convertido en un requisito indispensable para aquellas entidades con responsables concienciados y necesidades reales en materia de Seguridad. Dicho conjunto de indicadores debe complementar y verificar el cumplimiento de la Política de Seguridad, ayudando a fortalecer el control de la seguridad y permitiendo focalizar los recursos disponibles con mayor eficiencia en prácticamente cualquier tipo de entidad, independientemente del sector. Su incorrecta definición, selección, tipificación, implantación, monitorización, interpretación y parametrización puede estancar la evolución o el nivel de madurez de la seguridad de una entidad, consumiendo insaciablemente buena parte de sus presupuestos.

Javier Osuna García Malo de Molina es desde noviembre de 2001 Jefe de la División de Auditoría y Planificación de la Seguridad de Soluciones Globales Internet. Licenciado en Gestión de Sistemas Tecnológicos de Información y Master en Administración de Empresas por la Clarkson University (NY-USA), inició su andadura profesional como administrador del servicio web de la citada Universidad. Posteriormente, ya en 1997, ingresó en Arthur Andersen en calidad de Jefe de Equipo en el departamento de Auditoría y Consultoría de CRM de la auditora, hasta enero de 2001, en que pasó a ocupar el puesto de Responsable de la Línea de Servicio de B2B, Supply Chain Management y Marketplaces en la Unidad e-Business de Madrid de Cap Gemini Ersnt & Young hasta su incorporación a Soluciones Globales Internet.

La venta interna de iniciativas de seguridad: métricas, indicadores y otros argumentos

Una de las labores de mayor importancia en el día a día del responsable de seguridad de las organizaciones (CISO, que dicen los anglosajones) es la venta interna de las proyectos corporativos. A lo largo de la conferencia se analizarán los enfoques y aproximaciones más adecuados –y también los menos convenientes– para la defensa del presupuesto de seguridad, prestando una atención especial al uso que en dicha venta interna se hace de las métricas y los indicadores.

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.

La integración de la seguridad TIC en los procesos de negocio

En la actualidad, gran parte de las empresas disponen de sistemas de información como pieza clave para soportar tanto su actividad de negocio diaria como los procesos internos necesarios para la buena administración de la misma. Es en este contexto, cuando surge la necesidad, cada vez más creciente, de integrar ciertos mecanismos de control en los correspondientes sistemas y procesos, con el objeto de asegurar la integridad, disponibilidad y confidencialidad, tanto de los activos, como de los procesos asociados a dicha actividad, teniendo siempre presente el inevitable balance entre seguridad y operatividad. Debido a esto, es preciso que en cada compañía se lancen iniciativas para que el conjunto de procesos, ya sea dentro del ámbito estratégico o de soporte corporativo, sean diseñados integrando perspectivas y procedimientos de seguridad, de tal forma que más adelante puedan implantarse de una manera sencilla y coherente, los controles adecuados sin impactar en el correcto funcionamiento de cada proceso.

Elena Maestre García es Responsable de los Servicios de Seguridad de la Información en PricewaterhouseCoopers. Su trayectoria profesional se inició en el área de auditoría informática de Banesto, completándose posteriormente en el ámbito de la consultoría relacionada con la Seguridad de la Información en PricewaterhouseCoopers, donde lleva trabajando catorce años. Maestre es Licenciada en Ciencias Económicas y Empresariales por la UAM, y posee las certificaciones Cisa y Cism de Isaca.

Datos personales: riesgos asociados en sistemas y aplicaciones

Durante el tiempo reservado a esta ponencia se pretende comunicar, de forma objetiva, cuáles son algunos de los factores más importantes que hay que tener en cuenta en las distintas fases del proyecto de adaptación a la legislación vigente sobre protección de datos personales, tanto con vista a la posible inspección de la Agencia Española de Protección de Datos, como con el objetivo de fijar el marco de control exigible, todo ello de forma práctica y directa: actividades formativas y de divulgación, integración de los controles dentro de los procedimientos de la empresa, soporte a la auditoría, personas y perfiles que dan soporte a la Inspección, estructura organizativa, documentación disponible, y tipificación y gestión de incidencias.

Tomás Arroyo Salido es Responsable de Calidad de Servicio y Control Interno de BBVA, entidad financiera en la que ha ocupado durante veinte años cargos relacionados con actividades profesionales vinculadas al Control. Arroyo tiene más de veintiocho años de experiencia en informática, es Auditor Certificado en sistemas de Información por la Isaca (CISA), Diplomado en Auditoría de la Información y en Dirección de Seguridad de la Información por la UAM, Evaluador de Calidad (modelo EFQM) y cuenta con diversos estudios de Derecho (UNED). Es, además, colaborador/profesor del Master ejecutivo en dirección de Seguridad Global ofrecido por Belt Ibérica y la Universidad Europea de Madrid, Miembro fundador de ASIA (Capítulo de Madrid de Isaca), Secretario General del Grupo de usuarios GSE de IBM, y colaborador en diversos cursos de verano y programas de formación de diversas instituciones (UNED, IIR, IFE...).

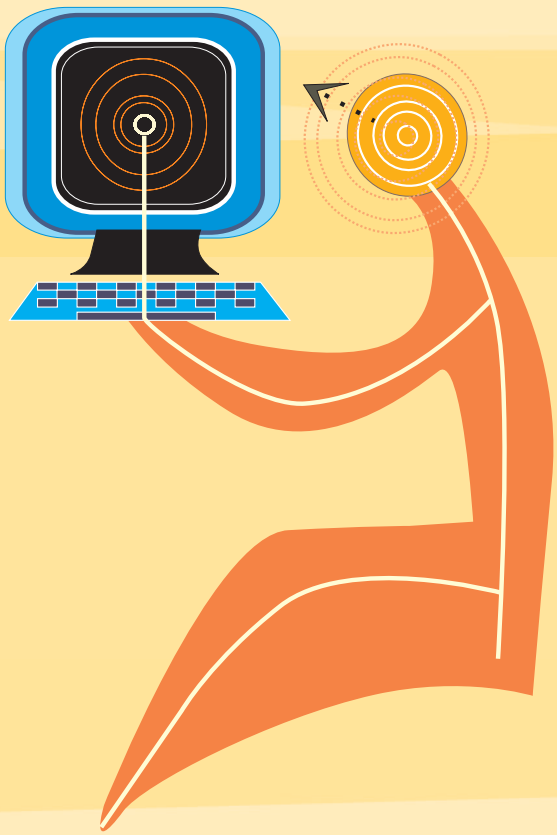
SGSI: modelo de certificación vs modelo de auditoría externa

Muchas empresas deciden acogerse a la certificación de su Sistema de Gestión de la Seguridad de la Información (SGSI) bajo un estándar, como por ejemplo BS7799-2:2002, lo cual es apropiado cuando hay una necesidad de reconocimiento en el ámbito público o ante agencias externas. Esto proporciona un sello de garantía, pero también algo que puede ser reconocido o entendido por el sector.

Por otra parte, en una certificación el alcance puede ser ampliado por el auditor externo, partiendo de una premisa: que está cualificado para ello, que complemente al estándar, ya sea mediante otro tipo de normas o de buenas prácticas (Cobit, ITIL, etc.) En contraposición a estos aspectos, otras empresas optan por someter su SGSI a modelos de auditoría externos, siguiendo los planes implantados dentro de su entidad u otros planes en los que no rijan las normas de certificación de un SGSI, ya que sólo necesitan un reconocimiento interno para conformar con los requisitos reguladores.

En esta ponencia se tratarán los pros y contras de someter un SGSI a una certificación como por ejemplo BS7799-2:2002 o a unos controles bajo un modelo de auditoría externo.

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 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. Actualmente en 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, asi como del Instituto de Auditores Internos. Finalmente es profesor de Auditoría Informática de la Universidad de Barcelona, así como en otros foros.



ESPACIO TiSEC 2004

AFORO LIMITADO

Fecha y lugar

Espacio TiSEC 2004 tendrá lugar los días 24 y 25 de noviembre de 2004 en el Hotel NOVOTEL*. Campo de las Naciones de Madrid.

Derechos de inscripción

- Los asistentes inscritos en Espacio TISEC 2004 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 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 91 401 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 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 2004

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 2004
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 2004, 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