PROFESORES

APARICIO, Fernando
Auditor Certificado de Sistemas de Información (CISA). Executive Master in Business Administration, Instituto de Empresa. Licenciado en Derecho, Universidad Nacional de Educación a Distancia. Licenciado en Ciencias Políticas, Universidad Complutense de Madrid. Socio y Director Comercial Security Xperts. Profesor del Área de Sistemas de Información del Instituto de Empresa.

ARROYO SALIDO, Tomás
Responsable de Normativa y Control Interno en el área de T. I. del BBVA. 28 años de Experiencia en Informática 20 en puestos de Control en BBVA.
CISA – Auditor Certificado en sistemas de Información por la ISACA. Diplomado en Auditoría de la Información y en Dirección de Seguridad de la Información UAM. Diversos estudios de Derecho en la UNED. Evaluador de Calidad, modelo EFQM.
Colaborador/profesor del Master ejecutivo en dirección de Seguridad Global ofrecido por Belt Ibérica y la Universidad Europea de Madrid. Colaborador, articulista y ponente en mesas redondas, grupos de usuarios y presentaciones de diversos foros y revistas de Seguridad. Miembro fundador de ASIA y secretario General del Grupo de usuarios GSE de IBM

BALLESTER, Manuel
Ingeniero Industrial , MBA. Auditor Certificado de Sistemas de Información (CISA). Manager Certificado en Seguridad de la Información (CISM). Es miembro del IEEE (Institute of Electrical and Electronical Engineers). Es miembro del Grupo de Trabajo 08 AEN/CTN 157 de AENOR (Proyectos de Sistemas de Información). Es miembro de la Junta Directiva de la Asociación de Auditores de Sistemas de Información (ASIA). Es miembro del Journal Editorial Board de la ISACA.
Director de la Revista Red Seguridad. Consejero Delegado de TEMANOVA

BOSCH, Antoni
Licenciado en Física Electrónica por la Universidad de Barcelona (UB). Master en Auditoría Informática por CENEI y Ernst&Young. ADE por ESADE. Técnico Superior en Prevención de Riesgos Laborales por la UOC. Seminars in Managing Information Technology en el Center for Information Systems Research del MIT Sloan Management. Certified Information Systems Auditor (CISA). Certified Information Security Manager (CISM). Director de los cursos de preparación al CISA y al CISM en Barcelona. Profesor de la Universidad Autónoma de Barcelona (UAB), Escuela Técnica Superior de Ingeniería, departamento de Ingeniería de la Información y Comunicaciones. Director de los miércoles EPSI-IMQ. Director de los seminarios prácticos EPSI-UAB. Director del Master Interuniversitario en Auditoría y Seguridad de los Sistemas de Información (UAB-UB). Director del IT-Governance Think-Tank Group de Barcelona. Director del Centro de Auditoría y Gestión de Riesgos Tecnológicos EPSI-UAB. Presidente Fundador ISACA-Barcelona (Information Systems Audit & Control Association). Asesor de diferentes empresas y organismos. Experto en IT-Governance.

CASTILLEJO BLANCO, Joaquín
Actualmente es Director General de TB-Security, empresa líder en gestión de la seguridad de la información en España. Anteriormente fue socio fundador y director de Security Xperts, S.L. Ingeniero Informático por la Universidad Politécnica de Madrid, ha desarrollado sus más de 14 años de carrera profesional en el sector de las telecomunicaciones y, específicamente, en la seguridad de la información, habiendo coordinado o dirigido proyectos de seguridad dentro del Grupo Telefónica, como el despliegue de infraestructuras como Ibernet, Infovía e Infovía Plus, o los Centros de Internet (TIC), prestando sus servicios en áreas de Operaciones e Ingeniería.

ESTEVES, José
Profesor de Sistemas de Información en el Instituto de Empresa desde el año 2004. Es Doctor (Ph.D.) en Software, especialidad en Sistemas de Información por la Universidad Politécnica de Catalunya (UPC), Barcelona, Master en sistemas de información por la Universidad do Minho (UM) en Portugal, DBA por Instituto Superior de Tecnología Empresarial, Porto, Portugal, y ingeniero en sistemas y infomatica. Es autor de varios estudios sobre sistemas ERP publicados en revistas y congresos internacionales. Sus intereses se centran en el campo de implantación y uso de sistemas ERP, impacto de los sistemas de información en las empresas y satisfacción de los usuarios, beneficios de los sistemas de información para las empresas, gestión de conocimiento y su uso a nivel organizacional.

FERNÁNDEZ SÁNCHEZ, Carlos Manuel
Ing. en Informática (UPM). Diplomado en Administración de Empresas CEPADE-UPM. Diplomado en Estudios Avanzados en Informática. (Doctorando).UPSAM. Está certificado como CISA Certified Information System Auditor (1989) y Certified Information Security Manager (2004) por la ISACA. Auditor jefe y Product Manager en AENOR. Responsable Certificación SGSI. Desde Diciembre 2003.
Profesor universitario de Auditoría Informática y Control de los SI en la Universidad Pontificia de Salamanca en Madrid. UPSAM. (desde 1985). Directivo y fundador de la Asociación de Auditores de SI. Capítulo de Madrid de la ISACA. Consejero de la revista SER EMPRESARIO. Con más de 25 años de experiencia en el sector de las TICs, en la Administración Pública y en empresas internacionales de informática y financieras. (Banco Bilbao-GISA, Ministerio de Marina, T&G Ibérica-Cullinet, Citigroup-Citibank (España y Europa), Microsoft Ibérica, Business Software Alliance y AENOR). Desde 1985 dedicado a la Auditoría de los Sistemas de información. Ponente de Auditoría Informática en Masters en España (ALI-UPM, ICADE, U. Complutense, Garrigues, La Salle, etc..) y en el extranjero. (Profesor de la UNESCO).

GABARRÓ, Ricardo
Ingeniero Naval por la Universidad Politécnica de Madrid - ETSIN, Auditor de Calidad por el LRQA, Doctorando por la Universidad Politécnica de Madrid - ETSIN. Es Jefe de Seguridad de la Información del Grupo Eulen y Profesor del Área de Tecnologías y Sistemas de Información en el Instituto de Empresa.

MAESTRE, Javier
Abogado, responsable de la oficina en Madrid de Bufet Almeida (www.bufetalmeida.com), despacho especializado en el asesoramiento y defensa de empresas, profesionales y particulares relacionados con Internet, los Servicios de la Sociedad de la Información, Informática y Telecomunicaciones. Autor de numerosos trabajos de investigación y de los libros "El derecho al nombre de dominio" y "La Ley de Internet: Régimen jurídico de los servicios de la sociedad de la información y comercio electrónico".

MEDINA LLINÀS, Manel
Catedrático Arquitectura Computadores (Seguridad Informática) en la Universidad Politécnica de Catalunya. Director del esCERT-UPC, equipo de seguridad de la UPC. Director del Centro de Aplicaciones de Internet, de la UPC (cANet-UPC).
Presidente de TB-Security/InetSecur, empresa de servicios de prevención y auditoría de seguridad. Dirección técnica y organizativa de SeMarket. Presidente de AEFTIC: Asociación de Expertos Forenses en TIC. Tesorero y fundador de Consorcio Digital, asociación para la promoción de la digitalización de documentos y factura-e. Fundador de Safelayer Secure Communications. Miembro de ESRAB (European Security Research Advisoriy Board), para asesorar a la Comisión Europea en la definición de los planes de I+D en Seguridad.

Instituto de Empresa
Business School

EXECUTIVE EDUCATION
Castellón de la Plana, 8 - 28006 Madrid
Tel: 902-30.21.30 // 91 745 47 60
Fax: 91- 561.77.68
e-mail: Soledad.Castejon@ie.edu
www.execed.ie.edu

INFORMACIÓN GENERAL

FECHAS Y LUGAR DE REALIZACIÓN
El Programa de Desarrollo se celebrará los días 25, 26 y 27 de Octubre de 2005, en el Instituto de Empresa situada en la calle Castellón de la Plana 8, Madrid, según el horario que figura en el programa.

DOCUMENTACIÓN
Todos los asistentes a la conferencia recibirán el material didáctico que se utilice en las jornadas. Esta documentación será un manual de obligada consulta para resolver cualquier duda o interrogante sobre el tema.

DERECHOS DE INSCRIPCIÓN
El precio total del programa será de 1.750 euros, incluyendo además de su asistencia a las sesiones, la documentación, el almuerzo y los cafés. Los Antiguos Alumnos de Programas Master del Instituto de Empresa, podrán acceder a una bonificación del 10% y para miembros de la Asociación de Antiguos Alumnos del Instituto de Empresa la bonificación será del 30%.

CANCELACIONES
En caso de no poder asistir al curso una vez formalizada la matrícula, se devolverá el 90% del importe, siempre que se comunique con al menos, tres semanas de antelación a la fecha del inicio. La sustitución de la persona inscrita por otra de la misma empresa podrá efectuarse hasta el día anterior al del inicio del curso.

FORMALIZACIÓN DE LA MATRÍCULA
La formalización de la matrícula se podrá realizar:
- Por teléfono: llamando a los números 902-30.21.30
- Por fax: enviando el boletín de inscripción adjunto al número 91- 561.77.68
- Por correo electrónico: enviando sus datos a: inscripciones@ie.edu
- A través de nuestro boletín de inscripción on-line, disponible en nuestra web: http://www.execed.ie.edu/web/programas

Las inscripciones ser realizarán por riguroso orden de reserva

CERTIFICADO
Los participantes recibirán un certificado acreditativo de su participación en el seminario.

ALOJAMIENTO
Con objeto de facilitar el alojamiento a las personas de fuera de Madrid, el Instituto de Empresa mantiene acuerdos de colaboración con diferentes hoteles próximos a la Escuela, donde se ofrecen interesantes descuentos para los asistentes al curso.

DIVISIÓN DE PROYECTOS IN-COMPANY
Executive Education del Instituto de Empresa a través de su división de Proyectos In-Company, ofrece la posibilidad de desarrollar acciones de formación y consultoría, tanto en el ámbito nacional como internacional, acordes con las necesidades específicas de su empresa.
Pueden ampliar esta información en los teléfonos: 91-745.47.61.

Madrid,
25, 26 y 27 de Octubre de 2005

PROGRAMA DE DESARROLLO

Instituto de Empresa
Business School

IT GOVERNANCE: GESTIÓN DE RIESGOS TECNOLÓGICOS

Buenas prácticas de gobierno de la seguridad de la información

PD PROGRAMA DE DESARROLLO

PROGRAMA

Martes, 25 de Octubre

09,00 a 09,15 h.
Acreditación de los asistentes y entrega de documentación

09,15 a 09,30 h.
Presentación del programa y sistemática.
Moderador de las Jornadas
D. Fernando Aparicio, Profesor Asociado del Área de Sistemas de Información, INSTITUTO DE EMPRESA

09,30 a 10,15 h.
SITUACIÓN ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN
- ¿Qué entendemos por gestión de la seguridad de la información?
- Factores críticos de éxito
- Evolución y panorama actual de la seguridad de la información
- El Gobierno corporativo de los sistemas de información
- Punto de partida de la seguridad de la información

D. Manel Medina, Catedrático de la Universidad Politécnica de Cataluña y Presidente del ESCERT / UPC

10,15 a 10,45 h.
Café

10,45 a 11,45 h.
METODOLOGÍAS Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN
- Buenas prácticas en seguridad de la información
- ISO 17799: Últimas novedades
- Otras normas: COBIT, UNE 71501
- Uso de indicadores y métricas: hacia un cuadro de mando de la seguridad de la información
- Cómo establecer un Sistema de Gestión de la Seguridad de la
- Información (SGSI): La norma UNE 71502

11,45 a 12,30 h.
CASO PRÁCTICO: EJEMPLO DEL ESTABLECIMIENTO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN UNA EMPRESA ESPAÑOLA

D. Carlos Manuel Fernández. CISA, CISM.
Product Manager-Auditor Jefe de SGSI de AENOR.

12,30 a 13,30 h.
ANÁLISIS Y GESTIÓN DE LOS RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN
- Concepto de análisis de riesgo: qué es y para qué sirve
- Activos, amenazas, vulnerabilidades y controles (salvaguardas)
- Estrategia de gestión del riesgo
- Asunción, mitigación o transferencia del riesgo
- Tipología de análisis de riesgo
- Metodologías de análisis de riesgo: MAGERIT

13,30 a 14,30 h.
CASO PRÁCTICO: EJEMPLO DE ANÁLISIS DE RIESGO EFECTUADO EN UNA EMPRESA ESPAÑOLA

D. Antoni Bosch, Director del Centro de Auditoría y de Gestión de Riesgos Tecnológicos y Profesor de la UNIVERSIDAD AUTÓNOMA DE BARCELONA

14,30 a 16,30 h.
Almuerzo

16,30 a 18,30 h.
GESTIÓN DE RIESGOS DE SEGURIDAD DERIVADOS DE LAS COMUNICACIONES Y OPERACIONES
- Seguridad en las comunicaciones y operaciones
- Selección de controles en materia de seguridad de las comunicaciones
- Controles de acceso: autenticación y autorización
- Riesgos y amenazas de la seguridad en comunicaciones
- Tecnologías y soluciones tecnológicas

18,30 a 19,30 h.
CASO PRÁCTICO: EJEMPLO DE ANÁLISIS DE VULNERABILIDADES REALIZADO EN LA RED CORPORATIVA DE UNA EMPRESA ESPAÑOLA

D. Joaquín Castillejo, Director General de TB-Security

Miércoles, 26 de Octubre

09,30 a 10,30 h.
ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN
- Concepto de Plan Director de Seguridad
- Políticas, estándares, guías y procedimientos
- Definición de roles y responsabilidades
- Estructura organizativa de la seguridad
- Clasificación y control de los activos

10,30 a 11,00 h.
Café

11,00 a 12,00 h.
CASO PRÁCTICO: EJEMPLO DE ESQUEMA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN UNA EMPRESA ESPAÑOLA

D. Tomás Arroyo, Responsable de Calidad de Servicio y Control Interno en Sistemas Europa de BBVA

12,00 a 13,30 h.
GESTIÓN DE RIESGOS DE LA SEGURIDAD DERIVADA DE ACCIONES HUMANAS
- Trascendencia del factor humano
- Divulgación y sensibilización de la seguridad de la información
- Responsabilidad del empleado en materia de seguridad
- Límites al control de la actividad del empleado
- Seguridad física y del entorno: controles ambientales

13,30 a 14,30 h.
CASO PRÁCTICO: DESCRIPCIÓN DE LA REALIZACIÓN DE UN PLAN DE DIVULGACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN UNA EMPRESA ESPAÑOLA

D. Fernando Aparicio, Profesor Asociado del Área de Sistemas de Información, INSTITUTO DE EMPRESA

14,30 a 16,30 h.
Almuerzo

16,30 a 18,30 h.
GESTIÓN DE RIESGOS DE SEGURIDAD DERIVADOS DEL DESARROLLO, ADQUISICIÓN, IMPLEMENTACIÓN Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN:
- La opción desarrollo Vs. adquisición: selección de controles
- Estrategias alternativas de desarrollo de software
- Especificación de los requisitos de seguridad

18,30 a 19,30 h.
CASO PRÁCTICO: EJEMPLO DE ESTABLECIMIENTO DE CONTROLES EN ENTORNOS DE DESARROLLO, ADQUISICIÓN, IMPLANTACIÓN Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN EN UNA EMPRESA ESPAÑOLA

D. Manuel Ballester, Director de la Revista RED SEGURIDAD

Jueves, 27 de Octubre

09,30 a 11,00 h.
GESTIÓN DE LA CONTINUIDAD DE NEGOCIO DE LA ORGANIZACIÓN:
- Planes de contingencia Vs. Planes de continuidad de negocio
- Fases de un Plan de Continuidad de negocio:
  - Planificación
  - Desarrollo
  - Prueba
  - Mantenimiento
- Reevaluación

11,00 a 11,30 h.
Café

11,30 a 12,15 h.
CASO PRÁCTICO: EXPOSICIÓN DE UN EJEMPLO DE IMPLANTACIÓN DE UN PLAN DE CONTINUIDAD DE NEGOCIO EN UNA EMPRESA ESPAÑOLA

D. Ricardo Gabarró, Jefe de Seguridad de la Información del GRUPO EULEN
Profesor del Área de Tecnologías y Sistemas de Información del INSTITUTO DE EMPRESA

12,15 a 13,45 h.
GESTIÓN DE LOS RIESGOS LEGALES DE LA SEGURIDAD DE LA INFORMACIÓN
- Conformidad legal: cumplimiento de la normativa vigente
- Protección de datos e intimidad de la información
- Propiedad intelectual Vs. Propiedad industrial
- Registro de dominios en Internet
- Prestación de servicios de información por Internet: LSSI
  - Delitos informáticos y la problemática de la prueba digital

13,45 a 14,30 h.
CASO PRÁCTICO: EJEMPLO DE UN PROYECTO DE ADECUACIÓN INTEGRAL A LA NORMATIVA DE PROTECCIÓN DE DATOS PERSONALES EN UNA EMPRESA ESPAÑOLA

D. Javier Maestre, Socio del Bufete Almeida y Asociados

14,30 a 16,30 h.
Almuerzo

16,30 a 17,30 h.
LA OPCIÓN DE LA TRANSFERENCIA DEL RIESGO
- Transferencia del riesgo al proveedor de servicios
- Seguros de riesgo electrónico
  - Panorama del sector asegurador
  - Modalidades
  - Condiciones de cobertura
  - Reclamaciones de terceros y empleados
  - Cobertura de daños propios
  - Gestión de siniestros

17,30 a 18,00 h.
CASO PRÁCTICO: EJEMPLO DE CICLO DE VIDA DE LA CONTRATACIÓN DE UNA PÓLIZA DE RIESGO ELECTRÓNICO EN UNA EMPRESA ESPAÑOLA

D. Fernando Aparicio, Profesor Asociado del Área de Sistemas de Información, INSTITUTO DE EMPRESA

18,00 a 19,00 h.
LA OPCIÓN DE LA EXTERNALIZACIÓN DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
- Concepto de seguridad gestionada
- Servicios profesionales de seguridad vs. Seguridad gestionada
- Factores que llevan a la consideración de la seguridad gestionada
- Ventajas y desventajas de la externalización de la gestión de la seguridad
- Aspectos críticos para seleccionar un proveedor de seguridad gestionada (MSSP)
- Los acuerdos de nivel de servicio (SLA)

19,00 a 19,30 h.
CASO PRÁCTICO: EJEMPLO DE GESTIÓN EXTERNA DE SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN EN UNA EMPRESA ESPAÑOLA

D. José Esteves, Director del Área de Sistemas de Información, INSTITUTO DE EMPRESA

19,00 a 19,30 h.
CLAUSURA Y ENTREGA DE DIPLOMAS

PROGRAMA DE DESARROLLO

IT GOVERNANCE: GESTIÓN DE RIESGOS TECNOLÓGICOS

Buenas prácticas de gobierno de la seguridad de la información

OBJETIVOS

Los riesgos crecientes sobre los activos de la información están obligando a las organizaciones a desarrollar estrategias que permitan evaluar y gestionar adecuadamente los riesgos asociados. La gestión de la seguridad de la información ya no sólo es un problema interno, sino que la cada vez mayor interconexión y dependencia de las redes y los sistemas informáticos obliga a las organizaciones a una adecuada gestión de sus riesgos si no quiere que estos terminen afectando a sus clientes, proveedores y socios en general. La seguridad de la información es una de las mayores preocupaciones de los directivos de TI, además es el segmento del sector donde mayores inversiones se han realizado y estas siguen creciendo.
Crece por tanto la necesidad de establecer sistemas de gestión de la seguridad de la información basados en estándares de amplio reconocimiento, que permitan a las organizaciones establecer una estrategia de actuación siguiendo controles y códigos de buenas prácticas ampliamente aceptadas por el mercado, y que sirvan de requisito para seleccionar a las organizaciones con las cuales se desean desarrollar actividades.
Esta realidad evidencia la necesidad de una mayor sensibilización y formación de los niveles ejecutivos de la empresa, que a través de un conocimiento objetivo de la problemática y las soluciones y prácticas que existen, permita al asistente establecer las bases para el desarrollo de una estrategia de seguridad en su organización. Como ejemplo de esta falta de sensibilización, podemos señalar que alrededor de un 80% de las empresas e instituciones españolas no tienen establecido un plan de acción para la salvaguarda de sus intereses si se produce un intento de acceder a sus sistemas de información o si se producen incidentes graves o desastres que resultan en una pérdida de información sensible.
El Seminario, basado en la presentación de casos reales de organizaciones en cada uno de los diferentes aspectos tratados, permite al alumno conocer de forma práctica cómo otras organizaciones han resuelto su problemática, al igual que obtener referencias e ideas útiles para su caso particular.
La gestión de los Sistemas de Información, comprende un amplio espectro de diferentes temáticas. El programa comprende una visión global y completa del tema, abarcándose entre otros los siguientes temas:
- Se expondrán los conocimientos necesarios para poder analizar paso a paso el estado actual de la seguridad de los sistemas de Información y detectar las áreas de mejora
- Se profundizará en el concepto de análisis y alternativas de gestión del riesgo derivado del uso de los sistemas de información, así como las implicaciones estratégicas que tiene este concepto para su organización.
- Se incidirá en la importancia de desarrollar una estrategia de seguridad de la información, incluyendo roles y responsabilidades, que sea adecuada para la cultura corporativa de la organización y que se extienda desde la Dirección General hasta el usuario final.
- Conoceremos las metodologías, mecanismos y prácticas empresariales existentes para la protección de la información.
- Se evaluará en profundidad el entorno normativo que condiciona la actividad de los sistemas de información de toda
- Se analizará la posibilidad de externalizar las funciones de seguridad, debatiendo la conveniencia de los servicios de seguridad gestionada.

METODOLOGÍA

Este es un programa intensivo con carácter marcadamente práctico en el que se combina el estudio de casos, con sesiones lectivas, conferencias y trabajo de los participantes en grupos.
Esta metodología facilita la puesta en marcha de los conceptos aprendidos a lo largo de las sesiones, tanto en el desarrollo del programa como en la propia empresa.
La propia dinámica del programa brinda la oportunidad de generar contactos profesionales y compartir experiencias con profesores y asistentes al mismo.

A QUIEN VA DIRIGIDO

El programa va dirigido a todas aquellas personas que cuenten, entre sus funciones, con aquellas relacionadas con la gestión de los Sistemas de Información, y tengan competencias en la definición de la estrategia de dichos sistemas.
Entre otros, va dirigido a: Directores Generales, Directores de Tecnología, Directores de Sistemas de Información, Auditores de Sistemas de Información, Consultores IT, Project Managers IT, Directores Financieros, Directores de Calidad, Consultores y Asesores de Empresa, Asesores Jurídicos y, en general, cualquier persona interesada en la gestión práctica de la seguridad de la información de las organizaciones.