

Estándares de auditoría, seguridad, control y buen gobierno de las TIC

Fecha: 14 y 15 de Septiembre 2011

OBJETIVO:

El curso está dirigido a profesionales de la seguridad y auditoría informática principalmente, así como a la Dirección de Sistemas de información, para conocer, comparar e iniciar en el uso de algunos de los estándares más relevantes en la gestión y seguridad de las Tecnologías de la Información y Comunicaciones.

TEMARIO:

1.- Introducción a los estándares relacionados con la auditoría, seguridad, control y buen gobierno de las TIC:

La necesidad

Objetivos de los estándares

Visión general de estándares, certificaciones, alcance y organismos internacionales (ISACA, ISO, BSI, etc.)

Selección de estándares: requerimientos de negocio y legales

Tendencias

Caso práctico

2.- Seguridad

La serie ISO 27000

Introducción e historia de los estándares

ISO 27000: Términos y definiciones

ISO 27001: Requisitos del Sistema de Gestión de Sistemas de Información.

ISO 27002: Guía de Buenas Prácticas de Objetivos de Control y Controles de Seguridad de la Información

ISO 27003: Guía de implementación del Sistema de Gestión de SI y uso del modelo PDCA

ISO 27004: Métricas y técnicas de medida de la eficacia del SGSI

ISO 27005: Directrices de Gestión del Riesgo

ISO 27006: Requisitos para la acreditación de entidades de auditoría y certificación de SGSI

ISO 27007: Guía de auditoría de un SGSI

Particularizaciones y otros estándares de la serie ISO 27000: 27011, 27031, 27032, 27033, 27034, 27799

Caso práctico.

3.- Auditoría, Control y Buen Gobierno de las TIC

3.1 CobIT

Introducción e historia del estándar

CobIT 4.1

Seguridad en CobIT

Mapeo de CobIT, ITIL v3 e ISO/IEC 27002

CobIT y las regulaciones Sabanes-Oxley y Basilea II

Otras publicaciones relacionadas del Framework de CobIT

3.2 ValIT: Inversiones en IT

Introducción e historia del estándar

Relación con CobIT

ValIT 2.0

3.3 ISO/IEC 38500

Introducción e historia del estándar

Mapeo y complementariedad con los anteriores

Caso práctico

4.- Mejores prácticas de gestión de servicios de las TIC: ITIL

Introducción e historia del estándar

ITIL v3: la gestión de servicios de TI: prestación de servicios y soporte.

ITIL v3: Otras guías operativas: infraestructura, seguridad, negocio, aplicaciones y activos Sw

Guías de implementación de la gestión de servicios

5.- Modelo de Madurez CMMI:

Introducción a CMM y CMMI e historia del estándar

CMMI como modelo para la evaluar el nivel de madurez respecto a estándares de seguridad y control.

Caso práctico

6.- Otros estándares técnicos de Seguridad Informática:

Common Criteria: ISO 15408

NIST SP 800

BSI Alemán

PCI – DSS

Otros

Caso práctico

PONENTES

María Jesús Casado Robledo, Licenciada en Ciencias Empresariales (UAM). Pertenece al Cuerpo Superior de Sistemas y Tecnologías de la Información, certificada como CISA y CGEIT, es miembro de ASTIC (Asociación del Cuerpo Superior de Sistemas y Tecnologías de la Información) e ISACA. Con más de veinte años de experiencia en el ámbito de las TIC, dispone de una amplia experiencia en Dirección y Gestión de la Seguridad de la Información, en Auditorías de Sistemas de Información, en aplicación de las nuevas tecnologías en el desarrollo e implantación de Sistemas de Información y en impartir formación en temas relacionados con Dirección y Gestión de la Seguridad de la Información, Auditorías de Sistemas de Información y nuevas tecnologías.

Luis Saiz Gimeno, Ingeniero de Telecomunicación por la UPM, certificado CISA y CISSP. Con más de 12 años de experiencia en diferentes áreas de seguridad de la información, trabaja en este campo desde el 2000 en el Grupo BBVA. Actualmente es el Responsable de Prevención de Delitos Tecnológicos del Grupo BBVA dentro del Departamento de Seguridad Lógica, siendo el ámbito de actuación la prevención, detección e investigación de los delitos cometidos por medios telemáticos.

Nelson Sanchez Vera, Ingeniero Informático. CISA y Lead Auditor 27001. Actualmente es Gerente del Área de Riesgos Tecnológicos de PricewaterhouseCoopers. Con más de 10 años de experiencia en seguridad de la información, especializado en análisis y gestión del riesgo y sistemas para la gestión de la seguridad de la información basados en las normas ISO 27001 y 27002. En los últimos años ha diseñado más de doce planes directores de seguridad en organizaciones de gran magnitud además de soportar la implantación y certificación de los SGSI para algunas de ellas. Entre sus responsabilidades como gerente de Riesgos Tecnológicos de PricewaterhouseCoopers esta el diseño, desarrollo y evolución de las herramientas y metodologías de análisis y gestión del riesgo.

José Ramon Coz Fernández, Doctor en Ingeniería Informática con la Calificación de Sobresaliente Cum Laude (ETSI Informática de la UNED). Licenciado en Ciencias Físicas (Universidad de Cantabria). Diversos Postgrados en Telecomunicaciones y Redes para la Seguridad y la Defensa (Escuela Superior de Ingenieros de Telecomunicación, Universidad Politécnica de Madrid.). Máster de Dirección de Tecnologías de la Información (IDE-CESEM). Graduado Especialista en Gestión de las Administraciones Públicas (CEPADE-UPM). Experto Universitario en Sistemas de la Información para la Empresa (CEPADE-UPM). Certificaciones Oficiales del APM GROUP, EXIN, Open Group y la OGC (Oficina del Gobierno Británico): TOGAF, PRINCE2 Registered Practitioner y Foundations, MSP Practitioner y Foundations, ITIL V3 Foundations e ISO 20000 Foundations. Certificaciones Oficiales de la ISACA (Information Systems Audit and Control Association): COBIT Foundations, CISA, CISM, CGEIT y CRISC (Titulaciones acreditadas por ANSI ISO/IEC 17024). Curso Oficial CMMI Foundations del SEI (Software Engineering Institute). Máster en Redes (TISA-CESINE). Certificación de Privacidad (ACP Consultant). Experto en Implantación de SGSI (Sistema de Gestión de la Seguridad de la Información), por APPLUS.

Miguel García-Menéndez, Ingeniero de Informática (Universidad de Oviedo). CGEIT, CISM, CISA. Managing Consultant de la práctica IT Governance & Processes de Atos Consulting. 15 años de experiencia en el mundo TIC. Ha sido CIO de ENSILECTRIC, S.A. (Grupo Acerlor-Mittal), Jefe de la Unidad de Seguridad de Atos Research & Innovation y miembro del equipo de Information Security & Compliance de Atos Consulting. Actualmente es responsable del Programa de iniciativas de Buen Gobierno Corporativo de las TIC dentro de la firma. Ponente habitual en conferencias y cursos, es miembro del claustro de profesores del Máster en Buen Gobierno de las TIC de la Universidad de Deusto (MaGTIC) e instructor acreditado de CobiT (ACT) por la ISACA.

LUGAR Y CELEBRACIÓN DE CURSO

El curso se realizará en la sede del Instituto de Auditores Internos situada en la Calle Santa Cruz de Marcenado 33, Planta 1, 2B, durante los **días 14 y 15 de Septiembre 2011**.

El horario del curso será de 09:00 a 14:00 h y de 15:00 a 18:00 h.

CERTIFICADO DE ASISTENCIA

La asistencia a este curso proporciona 16 horas de formación continua.

INSCRIPCIONES

Para inscribirse en este curso es necesario cumplimentar el boletín de Inscripción y remitirlo por fax al número 91 634 77 23.

Las cancelaciones de inscripción al curso, sólo serán aceptadas hasta 7 días antes de la celebración del mismo.

Importe (IVA no incl.): 900 €. Asociados (ISACA/IAI): 400 € - Miembros entidades colaboradoras: 15% descuen.

CURSO “ _____ ”

Para realizar la inscripción al curso, arriba indicado, por favor cumplimentar y enviar este boletín de Inscripción por fax al número 91 634 77 23

Marque el importe a pagar, según corresponda, en el siguiente cuadro

	Precio c/IVA
Precio del curso	€
Miembros de las entidades con acuerdos de colaboración (ATI, AI2, AENOR-SC27) 15% de descuento	€
Precio especial para Asociados ASIA – ISACA / IAI	€
Total a pagar (IVA incluido)	€

Las cancelaciones de inscripción al curso, sólo serán aceptadas hasta 7 días antes de la celebración del mismo.

() Sólo se considerarán definitivas las inscripciones cuyos importes hayan sido previamente abonados, mediante transferencia bancaria. La transferencia deberá realizarse a nombre de la Asociación de Auditores de Sistemas de Información; CIF: G83254755; Cuenta Corriente: 0128.0051.23.0500004696.**

Para cualquier consulta dirigirse a formacion@isacamadrid.es.

Nombre y Apellidos Asistente: NIF:

Asociado ISACA Nº Asociado ATI Otros (indicar)

Empresa: Dpto. y Cargo:

Dirección Personal:.....

Localidad: Código Postal: Tfno. Personal:

E-mail:

Para hacer efectivos los descuentos tendrán que aportar en este formulario el número de asociado a ISACA, o a la entidad con la que se tiene el acuerdo. Los descuentos no son acumulables.

DATOS DE FACTURACIÓN: Por favor, marque y cumplimente la opción deseada

La factura debe ser emitida a la empresa: CIF

Domicilio empresa: C.P. y Localidad

Envío de la factura Att. D./D^a:

Dpto:..... Cargo:.....

Teléfono empresa: Fax empresa:

E_mail:.....

Inscripción autorizada por: D./D^a

Departamento: Cargo:.....

Dirección:

Teléfono: E-mail:.....

Fecha..... Firma y Sello:

La factura debe ser emitida a título personal: D/D^a.....

NIF: Domicilio:

Cód. Postal: Localidad:

Los datos se solicitan para el único efecto de la gestión del curso, procediéndose a la cancelación de los mismos una vez finalizado el mismo, conservándose los estrictamente necesarios por requerimientos contables y tributarios, y de aspectos administrativos del curso. Estos datos no se cederán a ningún tercero.