



**PROGRAMACIÓN DO CURSO
DE AUDITORÍA INFORMÁTICA**

**Colexio Profesional de
Enxeñaría en Informática
de Galicia**

CONTIDO

1	Obxectivos.....	3
2	Audiencia.....	3
3	Prerrequisitos.....	3
4	Cronometría.....	3
5	Metodoloxía.....	3
6	Material didáctico.....	4
7	Unidades didácticas.....	4
	7.1 Módulo de igualdade.....	4
	7.2 Módulo I. Auditoría informática. Protección e seguridade na empresa do século XXI.....	4
	7.2.1 Programación.....	4
	7.2.2 Relator.....	6
	7.3 Módulo II. Auditoría software.....	6
	7.3.1 Programación.....	6
	7.3.2 Relator.....	7
	7.4 Módulo III. Auditoría informática.....	9
	7.4.1 Programación.....	9
	7.4.2 Relator.....	10

1 OBXECTIVOS

Formar e adestrar a Enxeñeiros/as en Informática na disciplina da Auditoría en Informática.

2 AUDIENCIA

20 alumnos/as Enxeñeiros/as ou Licenciados/as en Informática con perfil de auditores e consultores de informática.

3 PRERREQUISITOS

- Coñecementos de seguridade informática.
- Licenciatura ou Enxeñaría en Informática.

4 CRONOMETRÍA

Programado para 6 sesións de 5 horas cada unha delas, sumando un total de 30 horas lectivas, máis unha sesión adicional de 5 horas con contidos de igualdade. As sesións repártense en 3 módulos, un teórico e dous prácticos, cada un deles impartidos por diferentes poñentes.

5 METODOLOXÍA

Logo da introdución dos contidos teóricos, o curso estará fortemente orientado á exposición práctica por parte dos poñentes de casos, experiencias e exercicios reais que serán comentados e realizados polo alumnado.

6 MATERIAL DIDÁCTICO

- Apuntamentos de cada módulo para facer un seguimento da exposición.
- Entregarase o libro: PIATTINI, Mario y otros; Auditoría de Tecnologías y Sistemas de Información. RA-MA. 2008.

7 UNIDADES DIDÁCTICAS

7.1 Módulo de igualdade

Sesión única (sábado 27 de setembro de 9:00 a 14:00)

7.2 Módulo I. Auditoría informática. Protección e seguridade na empresa do século XXI

7.2.1 Programación

1ª sesión e 2ª sesión (venres 24 de outubro 16:30 a 21:30 e sábado 25 de outubro de 9:00 a 14:00)

- 1 Introducción
 - 1.1 Visión Xeral da Auditoría Informática
 - 1.2 Organización e Xestión da Función de Auditoría Informática
 - 1.3 Necesidade dunha Función de Auditoría Informática Independente
- 2 Controles de Xestión e Controles de Aplicación
 - 2.1 Xestión Xeral e Xestión de Auditoría Informática
 - 2.2 Desenvolvemento de Sistemas
 - 2.3 Xestión da Programación: Controles do Ciclo de Vida
 - 2.4 Administración de Bases de Datos
 - 2.5 Xestión de Operacións
 - 2.6 Resumo
 - 2.7 Casos de Estudo
- 3 Quality Assurance: Auditoría e Control de Calidade de Proxectos Informáticos
 - 3.1 Introducción

- 3.2 Concepto de Control de Calidade
- 3.3 Necesidade e Requisitos de QA
- 3.4 Ámbito e Severidade de QA
- 3.5 Niveis e Tarefas de QA
- 3.6 QA de Migración
- 3.7 Control de Versións do Software
- 3.8 Outros aspectos de Control de Calidade
- 3.9 Consideracións finais

4 Recuperación de Sistemas Informáticos en Situacións de Desastre

- 4.1 Introducción
- 4.2 A contorna do Plan de Recuperación
- 4.3 Metodoloxía de Recuperación de Sistemas
- 4.4 Resumo
- 4.5 Anexos

5 Aspectos Legais: Lei Orgánica de Protección de Datos de Carácter Persoal

- 5.1 Dereito de Información
- 5.2 Consentimento do afectado
- 5.3 Real Decreto 994/1999
- 5.4 Niveis de seguridade
- 5.5 Datos especialmente protexidos
- 5.6 Medidas de seguridade: Nivel Básico
- 5.7 Medidas de seguridade: Nivel Medio
- 5.8 Medidas de seguridade: Nivel Alto
- 5.9 Datos de carácter persoal: Consecuencias prácticas
- 5.10 Ficheiros temporais
- 5.11 Infraccións e sancións

6 6 Vulnerabilidades en Centros de Proceso de Datos: Amenzas, Ataques e Métodos de Defensa

- 6.1 Introducción
- 6.2 Autoría dun Ataque
- 6.3 Tipos de Ataques: Análise e Catalogación
- 6.4 Sistemas de Prevención e Defensa a Nivel de Empresa
- 6.5 Consellos de Interese para o Usuario Final de Internet
- 6.6 Estudo das Principais Ferramentas de Seguridade Dispoñibles
- 6.7 Resumo de Recomendacións de Seguridade

7 Bibliografía e Referencias Web

7.2.2 Relator

Serafín Caridad:

- Doutor en Informática, Universidade da Coruña, 2002. Enxeñeiro en Informática, Universidad da Coruña, 1992.
- 1993 – Presente: Profesor asociado, Departamento de Computación e Intelixencia Artificial, Facultade de Informática, Universidad da Coruña.
- 1985 – 1987: Co-fundador de Microforma, empresa especializada en Microelectrónica e Informática. Director do Departamento de Desenvolvemento de Software.
- 1976 – 2005: Centro de Proceso de Datos do Banco Pastor. 1976, Programador de Sistemas. Desde 1986, membro do Staff de Xerencia na División de Operacións e Sistemas, con responsabilidades en Xestión de Proxectos e Auditoría do Software, entre outras.
- 1969 - 1972: Técnico de Hardware, IBM de Venezuela, Departamento de Productos de Oficina.
- Presente: Interese principal en investigación sobre Planificación e Xestión de Proxectos, Auditoría do Software, Seguridade do Software, Xestión de Problemas, Xestión de Cambios e Control de Calidade.
- 1988 – 1992: Coordinador xeneral dos relatorios de Informática da Universidade do Atlántico, universidade de verán patrocinada pola Fundación Alfredo Brañas.
- www.scaridad.com
- scaridad@udc.es

7.3 Módulo II. Auditoría software

7.3.1 Programación

3ª sesión e 4ª sesión (venres 31 de outubro 16:30 a 21:30 e sábado 1 de novembro de 9:00 a 14:00)

- 1 Obxectivo. Comprender os procesos sistemáticos de avaliación obxectiva do software, a nivel do seu proceso de desenvolvemento e ao nivel dos produtos resultantes do mesmo.
- 2 **Introdución**
 - 2.1 Por que auditar o software?
 - 2.2 Definición de auditoría software, obxectivos, metodoloxías, etc.
 - 2.3 O papel da auditoría software nas empresas e fábricas de desenvolvemento
 - 2.4 O papel da auditoría nas empresas cliente (externalización)
 - 2.5 Produto vs Proceso
 - 2.6 Segregación de responsabilidades, órganos, etc
 - 2.7 Tipos de controis, riscos, etc
 - 2.8 Asociacións e acreditacións profesionais: CISA - ISACA, CSQE - ASQ, SEI - CMMI, ISO
- 3 **Auditoría do proceso software**
 - 3.1 Obxectivo
 - 3.2 Proceso - Método: fases típicas (o método ideal), métodos de auditoría (scampi, pathfinder), modelos de informe
 - 3.3 Normas de uso: COBIT, CMMI, ISO/IEC 15504, ISO/IEC 29110
 - 3.4 A auditoría da externalización
 - 3.5 Casos prácticos - experiencias
 - 3.6 Exercicios
- 4 **Auditoría do produto software**
 - 4.1 Obxectivo
 - 4.2 Proceso - Método: métricas, estratexias, probas, inspeccións, caixa negra, caixa branca, modelos de informe, etc.
 - 4.3 Impactos por evidencias atopadas
 - 4.4 Normas de uso: ISO/IEC 9126 / 25000
 - 4.5 Outras normas para a avaliación de produtos intermedios do ciclo de vida (arquitectura, deseño, etc.)
 - 4.6 Automatización da avaliación do software
 - 4.7 Casos prácticos - experiencias
 - 4.8 Exercicios

7.3.2 Relator

Javier Garzás:

- Doutor (cum laude por unanimidade) e Enxeñeiro Superior en Informática (premio extraordinario), Master en Enterprise Application Integration (premiado por Pricewaterhousecopers), CISA (Certified

Information Systems Auditor) poa ISACA (Information Systems Audit and Control Association) e CSQE (Software Quality Engineer Certification) poa ASQ (American Society for Quality).

- Comezou a súa carreira profesional en ALTRAN, como consultor senior en TIC e responsable do centro de competencias en enxeñaría do software, onde participa en varios proxectos estratéxicos, destacando ser responsable de enxeñaría software de TELEFÓNICA MÓVILES corporación, participar no redeseño do sistema SACTA de INDRA para o control de tráfico aéreo e liderar a automatización da simulación da rotativa de EL MUNDO. Máis tarde foi responsable da mellora da calidade software e responsable de proxectos de desenvolvemento software de mCENTRIC, participando nas implantacións para as operadoras de NIXERIA, MÉJICO e ESPAÑA. Posteriormente foi DIRECTOR EXECUTIVO E DE INFORMÁTICA de empresa de desenvolvemento de ERPs para a xestión como maior número de clientes en España.
- Desde 2006 é SOCIO-DIRECTOR de KYBELE CONSULTING, e consultor estratéxico, liderando varios proxectos en administracións e empresas como INFORMÁTICA DE LA COMUNIDAD DE MADRID (ICM), RENFE, DIRECCIÓN GENERAL DE TRÁFICO (DGT), ALHAMBRA - EIDOS, IEICSA, MINISTERIO DE ADMINISTRACIONES PÚBLICAS (MAP), AVANZIT, SISTEMAS TÉCNICOS DE LOTERÍAS (STL), CENTIC, etc.
- Experto en xestión e dirección de departamentos e fábricas software (realizando implantacións de fábricas e melloras en España, Colombia, Chile e Venezuela), cunha ampla experiencia en enxeñaría do software, calidade e mellora de procesos (líder da mellora e avaliación de procesos CMMI en varias empresas multinacionais).
- Foi profesor na UNIVERSIDAD DE CASTELA - A MANCHA e actualmente comparte a súa actividade profesional coa de docente como profesor na UNIVERSIDADE REI JUAN CARLOS.
- Participou en varios proxectos de I+D nacionais e internacionais, relatorios, editou varios libros e publicou máis de 50 traballos de investigación.
- Membro de varias asociacións informáticas destacando a AEC (Asociación Española da Calidade) (vogal), Colexio de Enxeñeiros de Castela e León (membro da xunta de goberno), ISACA (Information Systems Audit and Control Association), ASQ (American Society for Quality) e do SC7/GT24 de AENOR.
- jgarzas@gmail.com

7.4 Módulo III. Auditoría informática

7.4.1 Programación

5ª sesión e 6ª sesión (venres 7 de novembro de 16:30 a 21:30 e sábado 8 de novembro de 9:00 a 14:00)

- 1 Obxectivo. Achegar aos asistentes coñecementos e información para que poidan saber desde a experiencia práctica en que consiste a auditoría informática, a súa posible utilidade, cómo abordala e realizala, e como “sufri-la” por parte dos auditados.
- 2 Contido
 - 2.1 Xorde a necesidade ao cliente (entidade pública ou privada). Pasos que dá. Chéganos a nova de posible auditoría vía un intermediario? Razóns do cliente para pensar en auditoría externa vs interna
 - 2.2 Chaman a entidades auditoras. Que criterios seguen? Queren auditores certificados, pero non hai regulación? Determinar tipo de auditoría (informática, S. de I, avaliación do control interno...), obxectivos, alcance, profundidade, marco temporal e económico. Refírese a un período de tempo?
 - 2.3 Pescudar información. Recibir Prego / Posible documentación, compromiso de confidencialidade?
 - 2.4 Piden auditoría e queren consultoría? Prohiben que se chame auditoría?
 - 2.5 Visión dos posibles auditados: de responsables, de técnicos... impacto no seu traballo, nivel de sinceridade. Prefiren facer eles auditoría / autodiagnóstico?
 - 2.6 Viabilidade: podemos / queremos? Posible falta de: independencia, perfís, outros recursos, presuposto baixo, prazo curto, sobrecarga... subcontratamos?
 - 2.7 Elaboración da proposta. Quen contrata? Nivel? Estimación do esforzo e tempo. Posible planificación incluída. Especialistas externos? Perfil dos auditores. Equipo/s de traballo. Instrumentación dos colaboradores externos
 - 2.8 Casos en que afecta a un terceiro auditado: encargado do tratamento. O caso de revisións para grupos de empresas contratadas pola matriz, ou multinacionais
 - 2.9 Tipos de auditoría: de seguridade, de calidade, de xestión, de datos persoais, só técnica, xurídica, de cumprimento...
 - 2.10 Aprobación verbal? atrasouse? formalizar contrato?
 - 2.11 Recepción de documentación / Planificación de entrevistas e verificacións
 - 2.12 Fases do traballo. Programa de actividades e tarefas. Precedencias. Fitos. Xestión do proxecto. Informes e reunións de seguimento. Posibles incidencias que poden xurdir. Fontes. Papeis de traballo
 - 2.13 Traballo de campo. Realización de entrevistas. Á Dirección? Outras técnicas aplicables: mostraxes, cuestionarios... Quen coordina? Quen controla accesos? Quen audita aos auditores? Relación entre os internos e os externos e con responsables de Informática / SdI / TI, e con Administradores de Seguridade
 - 2.14 Verificacións: contra normativa interna, ISO / UNE, COBIT de ISACA, contratos
 - 2.15 Aplicación do zoom (análise / síntese) Acádanse evidencias? Que facer en caso contrario

- 2.16 Elaboración do informe (borrador) Cantos niveis de informes? cadros? métricas? cores? Revisión cruzada multinivel. Posible comparación con anteriores. Informes feitos por outros?
- 2.17 Entrega / envío ao cliente? Formato, protección? A quen dar / amosar?
- 2.18 Discusión do informe. Esixen que se cambien ou anulen cousas. Cobraremos? Ética
- 2.19 Escenarios posibles: auditados exauditados, auditores exauditados, o proxecto alargase, non verifican o borrador, piden máis cousas, sobrepasamos as estimacións internas, hai cambios organizativos no cliente, queren que implantemos os auditores, pídenos un certificado...
- 2.20 Fin da asistencia. Seguemento das implantacións? Haberá continuidade?
- 2.21 Situacións en xeral: demasiada carga de proxectos, pouca carga, pagos atrásanse... solapamento de varias auditorías diferentes
- 2.22 Posible caso/s a desenvolver polos asistentes, e comentar / discutir
- 2.23 Posibles preguntas CISA de mostra, con finalidade pedagóxica, que os asistentes contestan, e se comentan. De especial utilidade para quen pensen presentarse ao exame no futuro, ou o estea formulado.

7.4.2 Relator

Miguel Ángel Ramos:

- Doutor en Informática (Tese: Sistemas Expertos aplicados á Auditoría Informática). Cum laude. Universidade Politécnica de Madrid (24-9-1990)
- Dirixiu numerosos proxectos de auditoría informática en España e noutros países, en case todos os sectores de actividade durante 18 años
- É Profesor (Asociado) de Auditoría Informática, de Auditoría de Sistemas de Información e de Calidade do software na Universidade Carlos III de Madrid e foi á vez durante anos de Auditoría Informática na Universidad Nacional de Educación a Distancia (en Ensinanza Aberta e en Doutoramento).
- Foi durante doce anos (desde a fundación) profesor de MBAs na Escola de Negocios IEDE (Sistemas de Información)
- Impartiu moitos cursos de Auditoría Informática en IBM, IIR, INAP, Cuba, Panamá, Chile, Portugal, e de Control en varios Países do Leste (proxecto europeo PHARE)...
- Socio Director de IEE - INFORMÁTICOS EUROPEOS EXPERTOS, entidade que fundou en 1990 e Presidente desde 1994

- Corenta e un anos de experiencia en Informática como informático: programador, analista, directivo, auditor informático (18 anos de experiencia)
- Foi o primeiro Presidente da Organización de Auditoría Informática e do Capítulo Español da EDP Auditors Association (agora ISACA, Information Systems Audit and Control Association)
- CISA ("Certified Information Systems Auditor") pola EDPAF, agora ISACF
- Coautor de varios libros sobre auditoría, seguridade e protección de datos (podense ver en www.ie-e.es). Relator en congresos, autor de artigos...
- Sobre Auditoría Informática dirixiu unha tese doutoral na Universidade Carlos III e numerosos proxectos Fin de Carrera e Fin de Master (en total uns 50)