



# Màster en Tecnologies de Seguretat Informàtica

Màster 04-05



# Formació a l'ICT

La formació a l'ICT es basa en un model pedagògic propi que té com a principal referent l'empresa i els seus professionals, de manera que la metodologia dels cursos està orientada a la pràctica i a la posterior aplicació a l'entorn professional dels participants.



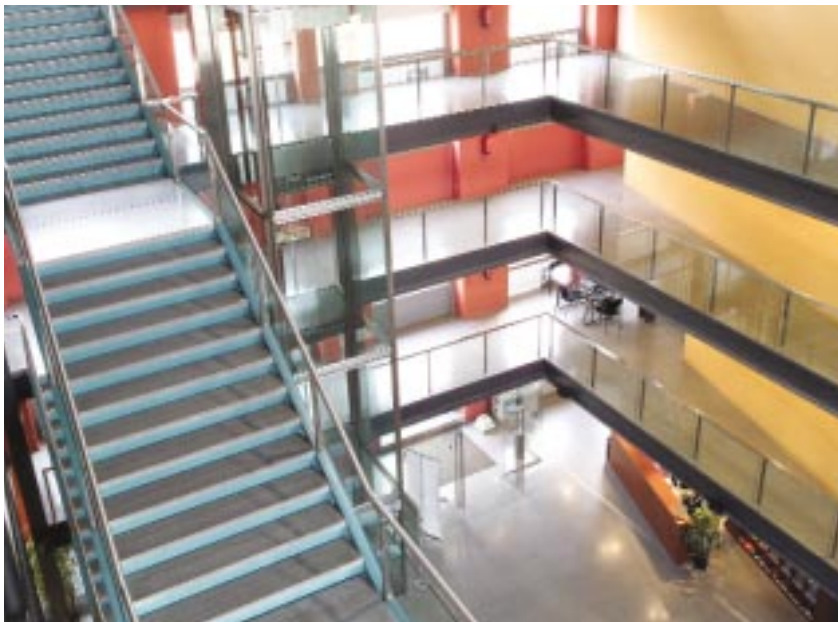
L'ICT és una institució privada sense finalitat lucrativa creada el 1986 pel Col·legi d'Enginyers Industrials de Catalunya.

És una fundació centrada en la qualitat, que complementa els serveis de formació amb serveis d'assessorament i d'informació empresarial. Aquesta oferta de serveis permet conèixer la realitat empresarial i transferir, en forma de casos pràctics, aquesta realitat als diferents programes de formació.

La formació de l'ICT es basa en un model pedagògic propi que combina, en la seva metodologia, elements presencials i d'e-learning.

**INTEGRAR LES TECNOLOGIES DE LA INFORMACIÓ I LA COMUNICACIÓ (TIC) PER OBTENIR UN AVANTATGE COMPETITIU QUE MILLORI ELS PROCESSOS DE L'EMPRESA.**

L'augment de la productivitat que generen les TIC en les empreses depèn, en gran mesura, del grau d'aprofitament que es faci d'aquestes. Des de l'ICT, entenem les tecnologies de la informació com una eina que les organitzacions han d'incorporar per millorar els seus processos. És per això que l'orientació dels nostres màsters és integrar les tecnologies de la informació i la comunicació a la gestió de l'empresa.



*Els continguts dels cursos recullen la llarga experiència professional de l'ICT assolida en l'assessorament de més de 1.000 empreses en diversos sectors productius i de serveis.*

## **Màster relacionats**

## **inici**

*Màster en Gestió de la Informació i de Continguts Digitals*

*octubre 2004*

*Postgrau en Anàlisi i Disseny Estructurat i Orientat a Objectes*

*octubre 2004*

*Postgrau en Administració de Xarxes i Comunicacions*

*octubre 2004*

*Postgrau en Direcció del Sistemes d'Informació*

*novembre 2004*

*Així mateix, durant tot l'any acadèmic es desenvolupa el Programa de Formació Contínua que cobreix altres aspectes relacionats amb les Tecnologies de la Informació a través d'una formació de menys durada i enfocada a resoldre els problemes concrets i a satisfer les necessitats del treball diari.*

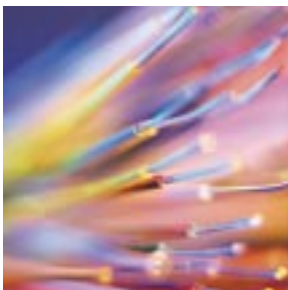
# Master en Tecnologies de Seguretat Informàtica. 3a edició

La globalització dels mercats i l'avenç en les noves tecnologies de la informació i la comunicació (TIC) fa que cada vegada més les empreses vegin aquests recursos tecnològics com un avantatge competitiu que permet millorar els resultats de l'empresa, i com una aposta de futur.



Els sistemes informàtics són ja una part molt important per a un gran nombre d'empreses, i aquesta importància creix cada dia. És per això que cal protegir aquests sistemes davant les amenaces a què estan exposats, amenaces també canviants en el temps.

Cal gent capaç d'avaluar la seguretat d'aquests sistemes, de gestionar-la, d'actualitzar-la. Cal que la seguretat en aquests sistemes sigui tinguda en compte per tots els qui hi actuen, i cal conèixer les eines de seguretat necessàries.



El Màster en Tecnologies de Seguretat Informàtica dona una visió global de com millorar la seguretat en els sistemes informàtics, de les aplicacions existents amb aquest objectiu, i de com fer que aquests coneixements siguin directament aplicables en l'entorn de treball dels assistents.

**EL CURS VA ADREÇAT A EMPRESES QUE VULGUIN CREAR EL SEU PROPI EQUIP DE RESPOSTA A INCIDENTS, A ADMINISTRADORS DE SISTEMES, A TITULATS EN INFORMÀTICA QUE VULGUIN ESPECIALITZAR-SE EN SEGURETAT, A ADMINISTRADORS DE SEGURETAT DE SISTEMES INFORMÀTICS, A AVALUADORS DE SEGURETAT DE SISTEMES INFORMÀTICS, ETC.**

*La seguretat de la informació afecta a tota l'organització.*

*L'objectiu final es tradueix en el fet que el participant, en finalitzar el curs, sigui capaç de:*

- *Avaluar i millorar la seguretat de l'entorn de sistemes informàtics.*
- *Obtenir una visió completa i actual dels mecanismes de seguretat informàtica.*
- *Identificar i dimensionar amenaces en els sistemes informàtics.*
- *Fer pràctiques de configuració i administració de mecanismes de seguretat.*



# Estructura i Contingut

La seguretat informàtica és clau tant pel que fa al bon funcionament de les empreses com pel que fa a la confiança en els sistemes informàtics dels qui hi operen.

## Visió general de la seguretat

- Panorama actual de les telecomunicacions.
- Introducció a la seguretat global.
- La seguretat i la seva justificació des del punt de vista del negoci.

## Xarxes de comunicacions

- Model OSI, xarxes LAN, nivell 3-IP, nivell de transport.
- Segregació de xarxes: nivell 1, 2, 3, 4.

## Criptografia i sistemes de certificació digital

- Fonaments.
  - Criptografia simètrica o asimètrica, funcions de Hash.
  - Estàndards: X509, PKCS, FIPS, RFCs.
- Aplicacions.
  - PKI, entitats de certificació.
  - Terceres parts confiabls: Time Stamping, OCSP.
  - Autenticació, single sing-on i gestió de claus.
  - Seguretat a Internet basada en criptografia: signatura de codi, ssh, ssl, ipsec, signatura i xifrat de dades, pgp.
- Criptografia actual.
  - XML Signature i XML Encryption.
  - Mitjans de pagament: m-commerce, identrus, set.
  - Protecció de propietat intel·lectual: Watermarking, fingerpriting.
  - Criptografia avançada: blind signature, privacitat, e-voting, e-gambling, e-cash.
- Smart Card.
  - Estàndards i productes: ISO 7816, PKCS11, Cryptographic and Memory Card, JavaCard, OpenCard, PS/SC.
  - Aplicacions: DNI digital, autenticació, SSO.

## Seguretat en xarxes

- VPN: IPsec.
- Routers i protocols.
- Cisco IOS.
- QoS.
- VLAN i routing.
- Protocols en l'àmbit de l'aplicació.
- Eines per a l'anàlisi de tràfic.

## Seguretat en xarxes sense fils

- Comunicacions sense fil.
- Wireless LAN: regulació (CNAF), OSI,802.11, equipaments.
- Seguretat en sistemes de comunicació cel·lulars: DECT,TETRA, GSM/GPRS i UMTS.
- Seguretat en serveis mòbils: localització, WAP (WTLS, TLS, WIM i SIM) i MEXE (Java).
- Seguretat bàsica i avançada en Wireless LAN.
  - Triangle CIA.
  - Defense-in-depth.
  - Mecanismes 802.11: WEP, filtrat.
  - Futur: WPA, nou esborrament 802.11i: AES.
  - Amenaces: Spoofing, Dos, Suplantació, Man-in-the-middle.
  - Solucions pràctiques segures: filtrat MAC, Activació WEP, Closing Node, EAP/802.1x, VPN.
- Utilitats/Programes Wireless LAN.
  - Coexistència: comunitats lliures, wardriver/walkers.
  - Utilitats i programes: Kismet, Netstumbler, FakeAP, Libpcap, Aircrack-ng, WEPCrack.

## Seguretat dels sistemes operatius: Windows

- Repàs històric: DOS/3.x, W9x/Me, NT/2000, Windows 2003/XP.
  - Arquitectura orientada a la seguretat.
  - Model de xarxa.
  - Autenticació en xarxa.
  - Active Directory.
  - Suport a l'ús en el desenvolupament, CryptoAPI.
  - Autenticació i encriptació de xarxa, transport i aplicació.
  - Protecció de fitxers amb EFS.
  - PKI en Windows.
  - Gestió de VPN.
  - Seguretat en serveis nadius.
  - Seguretat aplicada.
  - Construcció d'un servidor segur.
- Tunning, manteniment de la seguretat: eines d'ajuda.
- Control, auditoria de sistemes.
- Disponibilitat.
- Gestió de pegats i actualitzacions.
- Scripting, WM.

## Seguretat dels sistemes operatius: Unix/Linux

- Seguretat física: BIOS, Lilo, Grub, syslog.
- Autenticació: Kerberos, LDAP, PAM, NIS.
- Discos i sistemes de fitxers: Quota, ACLS, RAID, LVM, ext3, JFS, ReiserFS, XFS.
- Securització de serveis: inetd, xinitd, iptables, tcp wrapper, SetUID, SeGID.
- Gestió i monitoratge: shells, logs.
- Seguretat del kernel.

*La seguretat és un requeriment imprescindible per garantir el correcte funcionament dels sistemes.*

Des de fa temps, s'observa en el mercat laboral una tendència cap a la demanda de personal especialitzat, no tant amb una titulació concreta sinó amb una funció determinada.

#### Intrusions en sistemes informàtics

- Gestió d'un test d'intrusió.
- Integració BS7799 / auditoria tècnica.
- Limitacions de l'osstm.
- Metodologia.
  - Obtenció d'informació.
  - Obtenció d'accés.
  - Escalada de privilegis.
  - Avaluació d'objectius.
  - Metàstasi d'una intrusió.
- Eines.
  - Anàlisi: anonimitzadors, escàners.
  - Explotació: exploits, web, contrasenyes.
  - Gestió: rootkits, troians.
- Buffer overflows, exploits i shellcodes.
- Anàlisi d'aplicacions web.
- Eliminació i anàlisi de rastres.

#### Mecanismes de protecció

- NAT, DMZ.
- Firewall: de paquet, d'aplicació, proxys.
- Productes comercials.
- Linux/Iptables.
- VPN.
- Alta disponibilitat.

#### Mecanismes de detecció

- Intrusion Detection Systems.
- HIDS: trywire.
- NIDS: Snort.
- Honeypots.
- Gestió de logotips.
- Antivirus.
- Computer forensics.
  - La delinqüència en la societat de la informació.
  - El sistema judicial.
  - Els perits: forenses digitals.
  - La prova pericial i la cadena de custòdia.
  - Les maneres d'actuar.
  - L'examen pericial: el detectiu forense.

#### Planificació de la seguretat informàtica

- Anàlisi de riscos.
- Política de seguretat.
- UNE/ISO 17799.
- Plans de contingència.
- Auditoria.

#### Legislació

- Noves tecnologies: àmbit legal.
- Legislació nacional i europea.
  - LOPD.
  - Comerç electrònic.
  - Propietat intel·lectual.
  - Signatura electrònica.
  - LSSIce.
  - Dret laboral.
  - Civil/Mercantil: identitats, noms de domini.
  - Penal: ciberdelictes.
- Implicacions legals per a l'empresa.
- Riscos de no-adaptació a la legislació.
- Accions legals.

#### Projectes de seguretat

*Cal assegurar de forma correcta i amb les últimes tecnologies l'actiu més preciós de l'empresa: la informació.*





# Professors

El professorat combina la seva activitat docent amb l'exercici professional a l'empresa. La seva acreditació com a experts en determinats àmbits i la preparació pedagògica que han adquirit els capaciten com a excel·lents formadors.

## DIRECTOR DEL CURS

**Manel Medina Llinas**  
Cap d'esCERT: Spanish Computer  
Emergency Response Team

## PROFESSORAT

**Jordi Aymerich**  
Director Tècnic,  
FESTE

**Jordi Buch**  
Product Marketing Manager,  
Safelayer Secure Communications

**Domingo Cardona**  
Enginyer Superior de Telecomunicacions,  
Consultor de Seguretat Informàtica  
i Comunicacions

**Jordi Castellà Roca**  
Investigador Sctyl Online World Security,  
Consultor UOC

**Josep Comulada**  
Gerent,  
Grubits

**Daniel Cruz Allende**  
Enginyer tècnic en Informàtica de Gestió,  
Consultor de Seguretat Informàtica  
i Comunicacions,  
esCERT-UPC

**Enric Font**  
Project Manager Area Telcos,  
GyD Ibérica

**Carles Frago**  
Comunicacions i Operacions,  
Centre de Supercomputació  
de Catalunya

**Manuel García Cervigón**  
Enginyer tècnic en Informàtica de Gestió,  
Consultor de Seguretat Informàtica  
i Comunicacions,  
esCERT-UPC

**Jess García**  
Instructor SANS,  
Enginyer de Sistemes, Xarxes i Seguretat  
per INTA (Institut Nacional de  
Tècnica Aeroespacial)

**Gema Gómez Solano**  
Enginyera superior en Informàtica,  
Consultor de Seguretat Informàtica  
i Comunicacions,  
esCERT-UPCs

**José Manuel López**  
Project Manager Area Consultoría  
y Proyectos,  
GyD Ibérica

**Manel Medina**  
Catedràtic de la Universitat  
Politécnica de Catalunya i Presidente  
de la Associació d'Experts Forenses  
en Tecnologies de la Informació i  
Comunicacions (AEFTIC)

**Josep Paradells**  
Professor de l'Escola Tècnica  
Superior d'Enginyers de  
Telecomunicacions,  
Universitat Politècnica de Catalunya

**Joan Ramon Patón Martín**  
Enginyer superior en  
Telecomunicaciones,  
Consultor de Seguretat Informàtica  
i Comunicacions,  
esCERT-UPC

**Juan José Perez Mostajo**  
Enginyer tècnic en Informàtica  
de Gestió,  
Consultor de Seguretat Informàtica  
i Comunicacions,  
esCERT-UPC

**Francisco De Quinto**  
Soci del Gabinet Piqué Abogados  
Asociados,  
Departament de Dret  
i Noves Tecnologies

**Ramon Oró**  
Responsable de Noves Tecnologies,  
Departament d'Economia i Finances  
de la Generalitat de Catalunya

**Andreu Riera**  
Fundador i CEO de Sctyl Online  
World Security

**Jaime Robles**  
Coordinador General,  
RedLibre

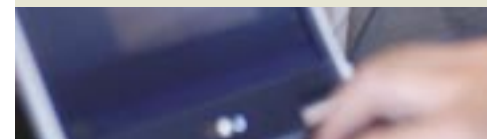
**Zane Ryan**  
Director General,  
ITWay Ibérica

**Juan Salom**  
Comandant en Cap del Grup  
d'Investigació del Departament  
de Delictes Telemàtics,  
Guardia Civil



## Titulació

*Els participants que hagin assistit al 80% de les hores lectives i que superin l'avaluació corresponent, rebran el Diploma en Tecnologies de Seguretat Informàtica del Programa Màster de l'Institut Català de Tecnologia.*



# Més Informació

## Desenvolupament

### ANY ACADÈMIC

data d'inici	data final	durada	horari	preu curs
20 octubre 04	juny 05	270 h lectives + 80 h projecte	dl., dc. i dv. de 18.30 a 21.30 h	4.800 €

### SESSIÓ INFORMATIVA: 29 DE SETEMBRE DE 2004 A LES 19 h

Les sessions informatives serveixen per exposar, d'una manera directa, els continguts i l'aplicació de cada curs.

Per accedir al curs cal presentar la sol·licitud d'admissió i, si s'escau, mantenir una entrevista personal amb el/la director/a del Màster/Postgrau o amb el/la responsable del programa



## Serveis complementaris

### BORSA DE TREBALL

Amb el servei de Borsa de Treball les empreses i els participants tenen a la seva disposició una eina eficaç per entrar en contacte amb un ampli ventall de perfils professionals, d'ofertes laborals i de pràctiques que tenen com a denominador comú la formació de l'ICT.

El servei està adreçat a tots els participants en les accions formatives de l'ICT sempre que no hagin estat matriculats per la seva empresa:

- Accés a les ofertes laborals de les empreses que s'adrecen a l'ICT per cercar professionals formats a l'Institut.
- Pràctiques en empreses: a través dels convenis subscrits entre l'ICT i les empreses, els participants en els cursos del Programa Màster i Postgrau tenen la possibilitat de complementar la seva formació amb pràctiques a l'empresa.

### CAMPUS VIRTUAL

El Campus Virtual és un entorn a Inter-net a través del qual el participant pot accedir a espais de relació i comunicació entre alumnes, formadors, coor-dinadors i personal de gestió; a la documentació del curs; i a espais de seguiment del seu procés formatiu.

### COMUNITATS VIRTUALS

Les comunitats són espais virtuals destinats a facilitar la interrelació entre professionals d'un sector i posar al seu abast els millors recursos existents a Internet. ICTnet disposa actualment de 30 comunitats distribuïdes per àrees: Gestió Empresarial i Qualitat, Tecnologies de la Informació, Enginyeria i Informàtica Industrial, Medi Ambient i Legal.

### BIBLIOTECA DE L'ENGINYERIA

La biblioteca de l'Associació d'Enginyers Industrials de Catalunya posa a disposició dels participants en els cursos un ampli fons documental i bibliogràfic amb bases de dades, monografies, revistes especialitzades i informació legislativa i tècnica.

### INSTAL·LACIONS

La seu de l'ICT, ubicada dins de l'àrea 22@ com a zona de fort impuls tecnològic, gaudeix de molts accessos tant a través de transport públic com privat. Les instal·lacions compten amb tots els mitjans pedagògics i tècnics per al desenvolupament de les accions formatives. L'ICT disposa d'un total de 28 aules amb suport informàtic, així com d'una sala de treball i un servei de cafeteria-restaurant.

Amb la col·laboració de:



Nota: L'ICT es reserva el dret de fer modificacions puntualment sobre la informació que apareix en aquest catàleg. En qualsevol cas, l'ICT garantirà la qualitat del servei.



Informació i inscripció:

**Institut Català de Tecnologia**

Servei d'Orientació Formativa:

Ciutat de Granada, 131, 08018 Barcelona

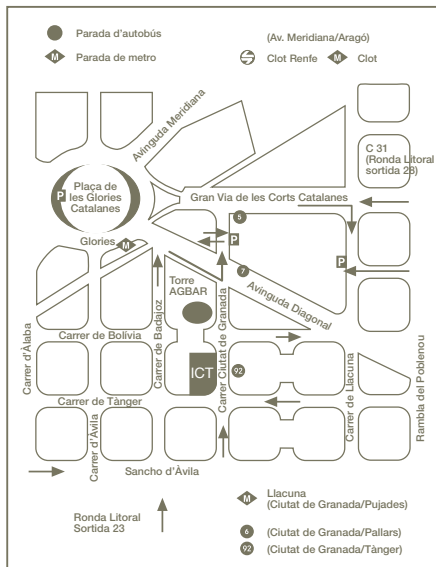
Tel. 93 485 85 93 o 93 485 85 85

A/e: [formacio@ictonline.es](mailto:formacio@ictonline.es)

Fax 93 309 45 59 o 93 485 85 88

<http://formacio.ictonline.es>

De dilluns a divendres,  
de 9 a 21 hores



<http://formacio.ictonline.es>