

# Consapevolezza, formazione e scambio di informazioni: strumenti indispensabili per la sicurezza informatica

**Convegno Assintel**

**Tecniche e Strumenti per la sicurezza e la privacy dei dati**

**Milano, 18 novembre 2004**



**Associazione Italiana per la  
Sicurezza Informatica**

Associazione "no profit" con sede presso l'Università degli studi di Milano, Dipartimento di Informatica e Comunicazione

Oltre 400 soci: in rappresentanza dell'intero "Sistema Paese"



Gli obiettivi principali che l'Associazione persegue sono **la creazione e la diffusione di una cultura della sicurezza informatica** presso le aziende private, gli enti della pubblica amministrazione e le organizzazioni economiche del nostro paese.

# CLUSIT- Associazione Italiana per la Sicurezza Informatica

## CLUSIT fa parte di un Network europeo



**CLUSIT** Italia



**CLUSIS** Svizzera



**CLUSIF** Francia



**CLUSIB** Belgio



**CLUSSIL** Lussemburg

## CLUSIT partecipa alle principali iniziative in materia di Sicurezza Informatica

è Partner scientifico di



è Education Affiliate (ISC)<sup>2</sup> per i seminari ed esami CISSP e SSCP



sostiene la Certificazione EUCIP IT Administrator modulo Security



patrocina i Master in Sicurezza Informatica di



La consapevolezza, la formazione, il continuo aggiornamento professionale e lo scambio di informazioni sono gli strumenti più efficaci per far fronte ai problemi della sicurezza



**L'impegno CLUSIT nella formazione**

# Il D.Lgs. 196/03 prevede interventi formativi

Il Testo Unico sulla Privacy (D.Lgs. 196/03 - allegato B) prevede *interventi formativi degli incaricati del trattamento per renderli edotti di:*

- rischi che incombono sui dati
- misure disponibili per prevenire eventi dannosi
- profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività
- responsabilità che ne derivano
- modalità per aggiornarsi sulle misure minime adottate dal titolare.



**Approfittiamo di un obbligo imposto dalla legge per trarne una serie di vantaggi**

# La formazione in Sicurezza Informatica come investimento a protezione degli asset Aziendali

- **La formazione mitiga il costo dell'ignoranza:**  
E' necessaria una formazione di base in Sicurezza Informatica **-Awareness-** per evitare danni sostanziali che spesso partono da errori banali.
- **La formazione aiuta ad effettuare scelte corrette:**  
E' indispensabile avere le conoscenze per definire le strategie e le policies di sicurezza più idonee al proprio tipo di business.
- **La formazione per una competizione ad *armi pari*:**  
E' necessario avere le conoscenze per affrontare le emergenze: ogni ritardo può essere un vantaggio a favore dei concorrenti.

# Security Awareness

## La consapevolezza

Molti dipendenti non sanno di ricoprire un ruolo di grande rilevanza nella sicurezza delle loro aziende. La trascuratezza nella gestione delle password, la leggerezza nel fornire informazioni a terze persone, scaricare programmi da Internet, scambiare programmi sono tutti fattori che contribuiscono a mettere a repentaglio la sicurezza delle reti aziendali.

Il personale che non è consapevole dei rischi presenti e non conosce le precauzioni necessarie per evitarli rappresenta un serio rischio per qualunque azienda

La formazione non deve essere rivolta al solo il personale coinvolto direttamente nel ICT, ma deve essere allargata alle principali funzioni aziendali: come chi si occupa di affari legali, responsabili outsourcing, direzione acquisti, risorse umane, ecc.

## La sicurezza inizia con il Management

Il raggiungimento degli obiettivi aziendali dipende in modo decisivo dalle piattaforme tecnologiche impiegate e dai processi organizzativi nelle varie organizzazioni.

Un Management consapevole dei possibili rischi e delle relative ripercussioni, può implementare un Information Security Management di tipo proattivo.

Il Management deve conoscere i possibili scenari di rischio per individuare i processi necessari per controllare e supervisionare eventuali rischi ICT.

# Security Awareness

## Un programma di Security Awareness

- Aumenta la consapevolezza dell'importanza della sicurezza informatica nella politica aziendale
- Riduce il carico di lavoro degli amministratori di rete diminuendo le richieste di intervento e di supporto agli utenti
- Minimizza i rischi di attacchi di social engineering
- Favorisce l'introduzione di strumenti di protezione dei dati coinvolgendo tutto il personale aziendale
- Aiuta a comprendere le implicazioni legali relative alle responsabilità connesse alla sicurezza informatica

## Gli aspetti principali di un programma di Security Awareness

- Il perchè della sicurezza
- Le implicazioni legali
- La sicurezza organizzativa: ruoli, responsabilità, policies aziendali
- Le minacce e le tipologie di attacco
- Le principali contromisure

# Lo scambio di informazioni e di conoscenze

Il crimine informatico è organizzato: le comunità criminali si tengono costantemente aggiornate sulle nuove vulnerabilità e si scambiano gli strumenti di attacco.

Il FIRST (Forum of Incident Response and Security Teams) è l'organismo internazionale che dal 1989 riunisce i CERT (Computer Emergency Response Team) nazionali per cooperare nell'affrontare gli incidenti di sicurezza e promuovere programmi di prevenzione. Nel proprio sito il FIRST riporta come headline:

**"Improving Security Together"**

Lo scambio di informazioni e di conoscenze è uno strumento essenziale per contrastare le minacce di sicurezza.

E' necessario diffondere la conoscenza delle Best Practices.

E' necessario diffondere rapidamente le informazioni sulle nuove vulnerabilità.

Sui siti web del FIRST e dei CERT sono disponibili moltissime informazioni, come pure sui siti web dei Vendors di prodotti antivirus. E' necessario tenersi aggiornati frequentando i forum specifici ed iscrivendoli alle mailinglist di sicurezza.

Nel sito [www.clusit.it](http://www.clusit.it) si trovano i link delle principali organizzazioni che diffondono informazioni.

# Scelta dei collaboratori qualificati e Certificazioni Professionali

Le certificazioni professionali sono tra gli strumenti utili a riconoscere il personale qualificato per gestire la sicurezza informatica.

Nella sicurezza informatica le certificazioni sono necessarie per **riconoscere** chi possiede:

- **le competenze**
- **l'etica**
- **l'esperienza**

Molte aziende leader richiedono una certificazione in sicurezza per le posizioni di maggiore responsabilità.

Una certificazione in sicurezza informatica oltre a favorire la carriera individuale, aumenta la credibilità dei professionisti della sicurezza.

# Breve panoramica delle principali certificazioni vendor-neutral

- ❖ **(ISC)<sup>2</sup>** International Information Systems Security Certifications Consortium
  - **CISSP\*** ⇒ Certified Information Systems Security Professional
  - **SSCP\*** ⇒ System Security Certified Practitioner
- ❖ **ISACA** Information Systems Audit and Control Association
  - **CISA\*** ⇒ Certified Information Systems Auditor
  - **CISM\*** ⇒ Certified Information Security Manager
- ❖ **SANS Institute**
  - **GSEC** ⇒ GIAC Security Essentials Certification
  - **GCFW** ⇒ GIAC Certified Firewall Analyst
  - **GCIA** ⇒ GIAC Certified Intrusion Analyst
  - **GCIH** ⇒ GIAC Certified Incident Handler
  - **GCWN** ⇒ GIAC Certified Windows Security Administrator
  - **GCUX** ⇒ GIAC Certified UNIX Security Administrator
  - **GSE** ⇒ GIAC Security Expert
- ❖ **ISECOM** - Institute for Security and Open Methodologies
  - **OPST<sup>o</sup>** ⇒ OSSTMM Professional Security Tester
  - **OPSA<sup>o</sup>** ⇒ OSSTMM Professional Security Analyst
  - **OPSE<sup>o</sup>** ⇒ OSSTMM Professional Security Expert
- ❖ **CompTIA** Computing Technology Industry Association
  - **CompTIA Security +**
- ❖ **EUCIP** European Certification of Informatics Professionals
  - **IT Administrator Modulo 5**

\*richiedono l'adesione ad un codice etico e una esperienza lavorativa pregressa.

<sup>o</sup> è prevista nella metodologia l'adesione ad un codice etico

# Attività formative CLUSIT

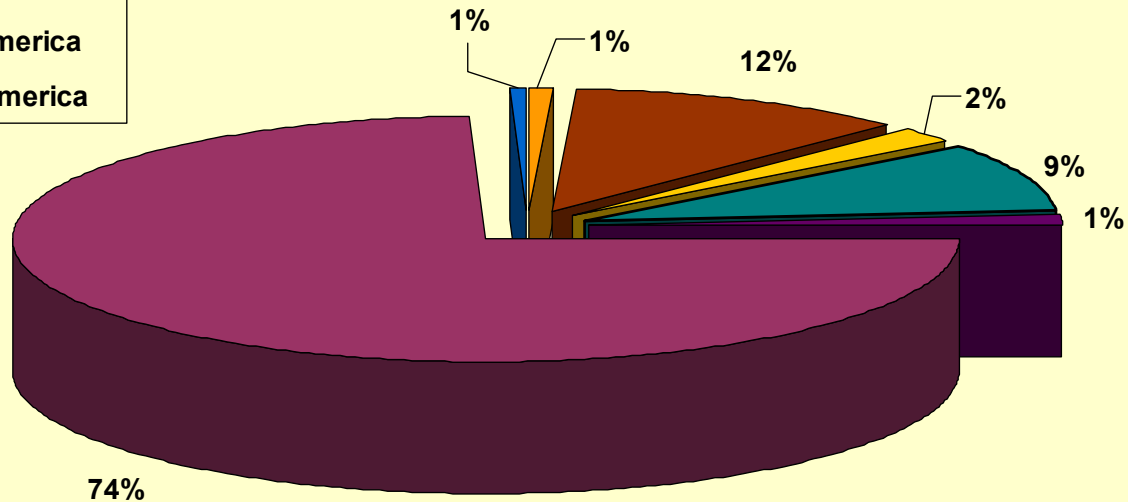
- ✓ **Partnership per l'Italia e il Ticino come Education Affiliate (ISC)<sup>2</sup> per i seminari e gli esami di Certificazione CISSP.**
- ❑ Partnership con AICA nella Certificazione EUCIP - IT Administrator Modulo Security
- ❑ Programma di Seminari CLUSIT Education di approfondimento tecnico scientifico su argomenti di Sicurezza Informatica.

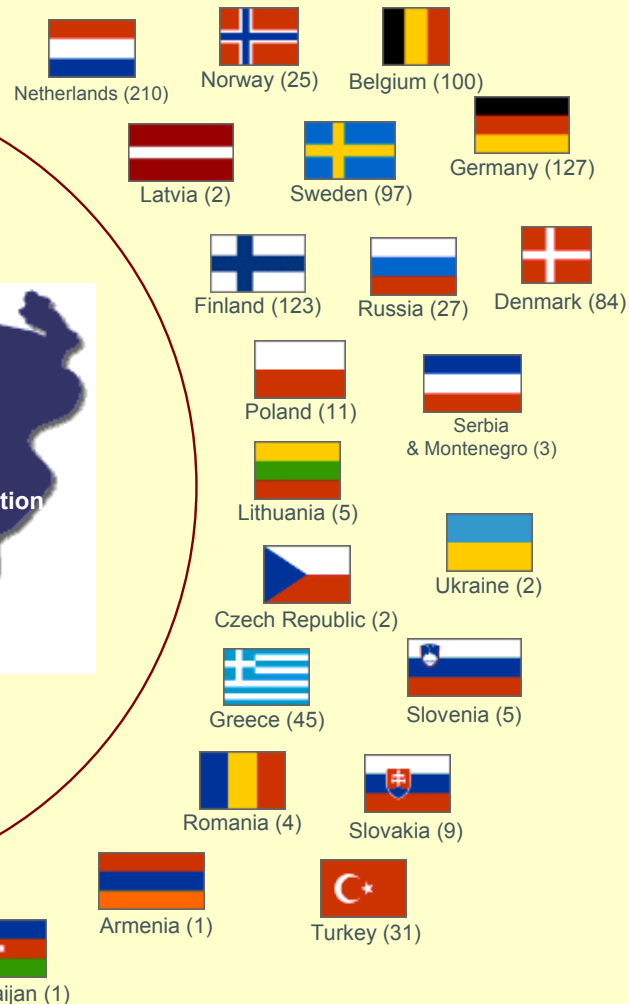
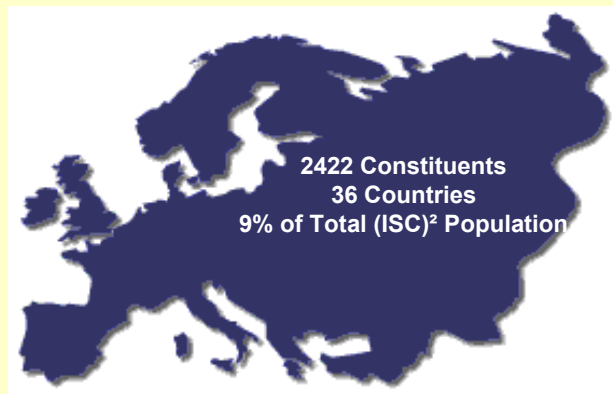
**(ISC)<sup>2</sup> is the non-profit international leader dedicated to training, qualifying and certifying information security professionals worldwide.**

- Fondata nel 1989: da 15 anni solo certificazioni in Sicurezza Informatica
- Le certificazioni: **CISSP** Certified Information Systems Security Professional  
**SSCP** System Security Certified Practitioner Certification
- L'aggiornamento del CBK (Common Body of Knowledge):  
I contenuti specialmente nella Sicurezza richiedono un continuo e tempestivo aggiornamento.
- Distribuzione geografica: circa 27.000 certificati in 106 paesi nel mondo.
- Ora anche conforme ISO/IEC 17024: lo standard che stabilisce i riferimenti per la certificazione del personale.



Approximately 27,000 constituents in 106 countries





# La certificazione CISSP

## Il percorso di certificazione

- L'adesione al codice etico (ISC)<sup>2</sup>
- Il superamento dell'esame di certificazione basato sul CBK (Common Body of Knowledge) (ISC)<sup>2</sup>
  - 250 domande a scelta multipla in lingua Inglese.
  - I candidati hanno 6 ore per completare l'esame.
- Una consistente esperienza di lavoro specifica e approfondita di Sicurezza Informatica:
  - 4 anni di esperienza professionale in almeno uno dei domini del CBK
- Il mantenimento della certificazione CISSP è basata sulla formazione continua:
  - 120 crediti CPE (Continuing Professional Education) in 3 anni

# La certificazione CISSP

## Common Body of Knowledge

- Security Management Practices
- Security Architecture and Models
- Access Control Systems & Methodology
- Application Development Security
- Operations Security
- Physical Security
- Cryptography
- Telecommunications, Network, & Internet Security
- Business Continuity Planning
- Law, Investigations, & Ethics

# La certificazione CISSP

## Il valore della certificazione

Essere accreditati **CISSP** rappresenta per i professionisti un riconoscimento internazionale di eccellenza a garanzia della professionalità.

Per le Aziende disporre di conoscenze orientate alle soluzioni e non settoriali, sempre aggiornate.

Aumentare la credibilità con il rigore e l'aggiornamento continuo della certificazione.

Dare al business il corretto orientamento della gestione del rischio.

# Attività formative CLUSIT

- ❑ Partnership per l'Italia e il Ticino come Education Affiliate (ISC)<sup>2</sup> per i seminari e gli esami di Certificazione CISSP.
  
- ✓ **Partnership con AICA nella Certificazione EUCIP - IT Administrator Modulo Security**
  
- ❑ Programma di Seminari CLUSIT Education di approfondimento tecnico scientifico su argomenti di Sicurezza Informatica.

## La partnership CLUSIT con AICA ed EUCIP consiste nel:

- Sostenere la certificazione EUCIP – IT Administrator
- Definire e mantenere aggiornato il Syllabus del Modulo Security
- Collaborare alla preparazione dei testi di riferimento
- Collaborare alla erogazione dei seminari ed esami per gli esaminatori



AICA - Associazione Italiana per l'Informatica ed il Calcolo Automatico è la più importante associazione nazionale di professionisti di informatica. Fondata il 4 febbraio 1961, AICA è una Associazione non a scopo di lucro che ha come finalità principale lo sviluppo delle conoscenze attinenti la disciplina informatica.

Da qualche anno conosciuta da tutti per la certificazione ECDL

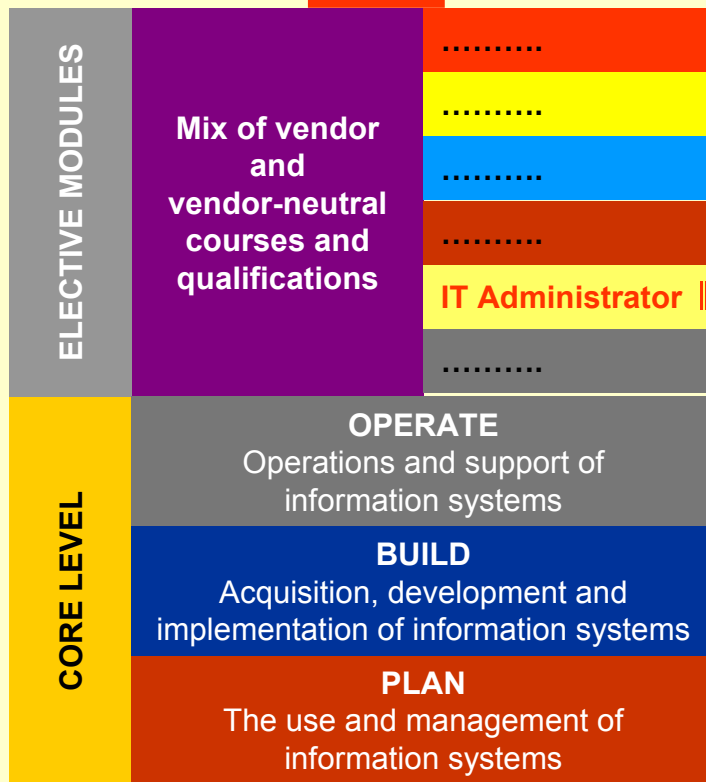


EUCIP - European Certification of Informatics Professionals is a new pan-European qualification scheme for people entering the IT profession and for IT professionals wishing to continue their professional development. EUCIP has been developed as an independent, globally recognised scheme for IT professionals

# La certificazione EUCIP IT Administrator - Modulo Security



- ELECTIVE PROFILES**
- IS Manager
  - IS Quality Auditor
  - Enterprise Sol.Cons.
  - Business Analyst**
  - Logistics & Autom. C.
  - Sales and Applic. C.
  - Client Services Mgr
  - IS Project Manager
  - IT Systems Architect
  - IS Analyst**
  - Web & Multimedia M.
  - Systems Int.& Test.E.
  - Software Developer**
  - Database Manager
  - X-Systems Techn.
  - TLC Engineer
  - Network Architect
  - Security Adviser**
  - Network Manager**
  - Configuration Mgr
  - Help Desk Engineer
  - IT Trainer



## Moduli IT Administrator

- Hardware
- Operating System
- Network Expert Use
- Network Services
- Security**

La certificazione **IT Administrator – Security** è indipendentemente dagli altri moduli.

## ➤ La figura dell'*IT Administrator*

- ✓ L' *IT Administrator* è una figura ampiamente richiesta
- ✓ La certificazione *IT Administrator* corrisponde, per capacità, all'attività di "supervisore del sistema ICT"
- ✓ Tipicamente in aziende medio/piccole o uffici decentrati di grandi organizzazioni pubbliche e private
- ✓ Questa certificazione trova un'importante applicazione presso le scuole secondarie superiori ad orientamento tecnologico

## ➤ Il ruolo dell'*IT Administrator*

Nel suo ruolo un *IT Administrator* deve essere in grado di:

- ✓ amministrare sistemi informativi di contenute dimensioni, tipicamente configurati in modalità client-server;
- ✓ identificare e risolvere problemi di primo livello;
- ✓ diagnosticare problemi di più elevata complessità e richiedere l'intervento del professionista in grado di risolverli;
- ✓ identificare le esigenze (aggiornamenti, modifiche, ampliamenti, ecc.) del sistema informativo e fungere da interfaccia con gli specialisti/fornitori;
- ✓ essere il punto di riferimento per gli utenti del sistema informativo di cui è supervisore.

# Attività formative CLUSIT

- ❑ Partnership per l'Italia e il Ticino come Education Affiliate (ISC)<sup>2</sup> per i seminari e gli esami di Certificazione CISSP.
- ❑ Partnership con AICA nella Certificazione EUCIP - IT Administrator Modulo Security
- ✓ **Programma di Seminari CLUSIT Education di approfondimento tecnico scientifico su argomenti di Sicurezza Informatica.**

# Seminari CLUSIT Education



- E' una iniziativa nata per i propri Soci
- Estesa a chiunque voglia partecipare
- CLUSIT ha convenzioni con organizzazioni partner (AIEA, AUSED, Federcomin)

Argomenti di interesse particolare, specifico e trattato in profondità.

I seminari sono mirati all'approfondimento tecnico e scientifico.

I contenuti dei Seminari sono indipendenti da ogni logica di sponsorizzazione.

Ogni seminario permette di farsi riconoscere 4 crediti/ore CPE (Continuing Professional Education) validi per il mantenimento delle certificazioni CISSP, CSSP, CISA, CISM

Il programma in corso fino a maggio 2005 prevede un seminario di 4 ore (intensive) ogni mese sia a Milano che a Roma.



## Programma seminari 2004 - 2005

- ✓ **Principi di Crittografia**
- ✓ **Voice-over-IP**
- ✓ **Il documento elettronico**
- **Crittografia Quantistica**
- **Reti Wi-Fi**
- **Tecniche biometriche**
- **Sicurezza VLAN e LAN**
- **RFID**
- **DRM**

- La consapevolezza
- La formazione
- Il continuo aggiornamento professionale
- Lo scambio di informazioni

Sono gli strumenti più efficaci per far fronte ai problemi della sicurezza

# Riferimenti:

Seminari ed esami **CISSP**: [www.clusit.it/isc2](http://www.clusit.it/isc2) - [isc2@clusit.it](mailto:isc2@clusit.it)  
Iscrizione mailinglist: [www.clusit.it/edu/form\\_news\\_edu.htm](http://www.clusit.it/edu/form_news_edu.htm)

Certificazione **EUCIP - IT Administrator - Modulo Security**:  
[www.aicanet.it](http://www.aicanet.it)

Seminari **CLUSIT EDUCATION**: [www.clusit.it/edu](http://www.clusit.it/edu) - [edu@clusit.it](mailto:edu@clusit.it)  
Iscrizione mailinglist: [www.clusit.it/edu/form\\_news\\_edu.htm](http://www.clusit.it/edu/form_news_edu.htm)

(ISC) <sup>2</sup>	<a href="http://www.isc2.org">www.isc2.org</a>
ISACA	<a href="http://www.isaca.org">www.isaca.org</a>
SANS Institute	<a href="http://www.sans.org">www.sans.org</a>
ISECOM	<a href="http://www.isecom.org">www.isecom.org</a>
CompTIA	<a href="http://www.comptia.org">www.comptia.org</a>
EUCIP	<a href="http://www.eucip.org">www.eucip.org</a>

# Riferimenti:

Sarà rilasciato a breve un **Quaderno CLUSIT** sulle principali Certificazioni in Sicurezza Informatica dove viene riportato un quadro generale delle certificazioni sia vendor che vendor-neutral.

Per ciascuna certificazione si illustra il percorso formativo, si identificano i prerequisiti necessari sia in termini di conoscenze, che di esperienza maturata e si precisano le modalità di svolgimento degli esami.

Per informazioni: **[www.clusit.it](http://www.clusit.it)** - **[info@clusit.it](mailto:info@clusit.it)**

*Giorgio Giudice, CISM  
Socio fondatore e membro del  
Comitato Tecnico Scientifico CLUSIT  
[ggiudice@clusit.it](mailto:ggiudice@clusit.it)*