COMPLETO a 360°!

Sintetico ed esaustivo!

"Corso molto interessante con relatori eccellenti"
Amministratore di Rete - EUROVITA ASSICURAZIONI

"Molto interessante per un neofita, quale sono, sull'argomento"
Addetto Ufficio Sicurezza Logica - BANCO di DESIO e della BRIANZA

"Ho trovato questa iniziativa un'opportunità per conoscere in modo abbastanza approfondito i rischi da valutare"
Resp. Gestione Software Centralizz. e Portale - COMUNE di TORRE ANNUNZIATA

Principi, Metodi e Fondamenti di Sicurezza Informatica

Aspetti ORGANIZZATIVI | **Aspetti TECNICI** | **Aspetti LEGALI** | **Aspetti TECNOLOGICI**

*Un **Corso Semplice** e **Pratico** per apprendere i Principi Base, le Regole e la Terminologia della Sicurezza Informatica nella propria Organizzazione*

- POLICY SICUREZZA
- VIRUS
- FIREWALL
- RETI
- BACK UP
- DISASTER RECOVERY
- CODICE PRIVACY
- CRITTOGRAFIA
- ILLECITI PENALI
- PUBLIC KEY INFRASTRUCTURE
- ANTISPAM
- ACCESSO e AUTENTICAZIONE

- Apprendere i **concetti base** della sicurezza informatica
- Conoscere le principali **vulnerabilità** di reti, software e hardware
- Individuare gli elementi chiave per definire una **policy** sulla sicurezza

*Inoltre uno **speciale Approfondimento** post corso:*

Conoscere TUTTO su

FIRMA DIGITALE e POSTA ELETTRONICA CERTIFICATA

Un approccio pratico e comparativo per chiarire tutti i dubbi e comprendere come agire in sicurezza

1ª edizione: **21 novembre 2008** *2ª edizione:* **20 febbraio 2009**

SCONTI per iscrizioni **entro 1 mese dall'evento**

Luogo e data

Milano
Holiday Inn Milan Garibaldi
19-20 novembre 2008
18-19 febbraio 2009

Trasmettere a

- Staff Direzione Sistemi Informativi
- Responsabile Organizzazione
- Funzionari Auditing e Ispettorato
- Responsabile Ufficio Acquisti

Informazioni e iscrizioni
tel. 02.83847.627 ■ fax 02.83847.262
conferenze@iir-italy.it ■ www.iir-italy.it

Istituto Internazionale di Ricerca
Know how to achieve

Sicurezza Informatica

OBIETTIVO DEL CORSO

L'obiettivo del corso è fornire ai partecipanti i **concetti base** in tema di Sicurezza Informatica per essere in grado di riconoscere le *vulnerabilità*, valutare le *cause* e analizzare i *danni* ai Sistemi informativi della propria organizzazione, comprendendo quali sono le azioni necessarie per proteggere i sistemi.

Il corso illustra tutti gli aspetti legati alla Sicurezza, partendo dalle definizioni di Rischio e Vulnerabilità del sistema, approfondendo la conoscenza dei diversi tipi di Attacchi Informatici, individuando le Azioni Preliminari per salvaguardare il sistema per poi essere in grado di sviluppare un Piano di Disaster Recovery. Il programma del corso è arricchito da una parte dedicata agli *aspetti legali*, dal *Codice della Privacy* alle conseguenze penali previste dalla legge per mancato rispetto degli *standard* di Sicurezza.

A CHI SI RIVOLGE IL CORSO

Il corso si rivolge a tutti coloro che intendono avere un *quadro semplice*, *sintetico* ed *esaustivo* in tema di Sicurezza Informatica.

E' rivolto in particolare a:

- **Staff della Direzione dei Sistemi Informativi** per approfondire la conoscenza e avere un quadro completo sui temi di Sicurezza;
- **Responsabili dell'Ufficio Acquisti** per poter valutare le offerte dei fornitori ed effettuare con i Responsabili dei Sistemi Informativi le scelte più appropriate;
- **Responsabili dell'Organizzazione** per comprendere quali politiche e procedure adottare per il proprio Ente a e nei confronti del Personale;
- Chi svolge **Funzioni di Ispettorato e Auditing** per essere in grado di effettuare verifiche più appropriate ed eseguire i controlli sulla Sicurezza.

Indispensabile

Il corso è dedicato comunque a tutti coloro che, ricoprendo una posizione di rilievo all'interno dell'Ente, vogliano approfondire la conoscenza dei principi della Sicurezza Informatica.

LIVELLO DI CONOSCENZA RICHIESTA

Per partecipare al corso non sono necessarie competenze specifiche su sistemi e tecnologie. Una conoscenza informatica di base migliorerà la comprensione dei contenuti del corso. Ai partecipanti sarà rilasciato un Attestato di Partecipazione.

CHI CONDUCE IL CORSO

Stefano Zanero
Dottorato di ricerca in Ingegneria dell'informazione presso il Dipartimento di Elettronica ed Informazione del Politecnico di Milano, attualmente assegnista di ricerca. I suoi interessi di ricerca attuali: lo sviluppo di Intrusion Detection System basati su algoritmi di apprendimento, virologia informatica e sicurezza delle web application. Insegna nel corso di Sicurezza degli Impianti Informatici dello stesso ateneo. Oltre all'attività didattica presso varie università italiane ed estere, ha partecipato come relatore a numerosi convegni nazionali ed internazionali, ed è autore di articoli scientifici. È membro del board editoriale del "Journal in Computer Virology", oltre ad essere un reviewer per "ACM Computing Reviews" e "IEEE Security&Privacy". È socio dello IEEE (Institute of Electrical and Electronics Engineers) e della ACM (Association for Computing Machinery). È socio fondatore di AIPSI (Associazione Italiana Professionisti della Sicurezza Informatica). È inoltre socio e responsabile tecnico di Secure Network S.r.l., una società di consulenza, formazione e servizi alle imprese in tema di sicurezza dell'informazione.

Andrea Lisi
Avvocato del Foro di Lecce dal 1999, perfezionato in diritto comunitario. Titolare dello Studio Associato D.&L., consulenza aziendale-legale in ICT & International Trade. Si occupa prevalentemente di diritto delle nuove tecnologie, diritto commerciale-internazionale e diritto civile. Fondatore del Centro Studi & Ricerche SCiNT Curatore di diversi Volumi in tema di e-commerce ed e-privacy. È componente del Comitato Scientifico di varie riviste telematiche. Direttore Editoriale "Rivista di Diritto, Economia e Gestione delle Nuove Tecnologie", Nyberg Editore. Collabora con diverse università in master e corsi post-universitari.

1° GIORNO

Conoscere i concetti base della sicurezza informatica: aspetti introduttivi

- Cosa s'intende e quali sono le differenze tra "Rischio", "Vulnerabilità", "Minaccia", "Attacco"
- Identificare gli asset da proteggere
- Quali sono i principali *standard* di sicurezza
- Individuare i requisiti di sicurezza

Valutare l'efficacia della propria Policy di sicurezza e definire procedure sicure e semplici

- Definire una Policy sulla sicurezza
- Strategie integrate per la sicurezza
- Considerare la sicurezza fisica
- In che misura e in che modo provvedere alla formazione degli utenti

Vulnerabilità dei sistemi, Analisi di vulnerabilità

- Come funzionano le principali categorie di vulnerabilità di sistema
- Cosa significa effettuare un *vulnerability assessment* di un sistema
- Come riconoscere un "buon" assessment da un "pessimo" assessment

Controllo accessi

- Creare una politica di controllo degli accessi
- Sistemi di autenticazione forte
- I rischi del Social Engineering

Definire i tipi di attacchi informatici

- Quali sono le categorie di attacchi informatici
- Le minacce: identificare i possibili aggressori
- Attacchi di rete
- Cosa sono le vulnerabilità del software e dei sistemi
- Cosa sono i virus informatici

2° GIORNO

Sicurezza di rete

- Sistemi di protezione basati su firewall
- Architettura a due livelli delle reti
- Protocolli sicuri: SSL, IPSEC e VPN

Elementi di Crittografia

- Cos'è la Crittografia e come funziona
- Cosa sono le PKI - Public Key Infrastructure
- I fondamenti dei vari tipi di Firma Digitale

Gestire gli incidenti informatici

- Strategia di risposta agli incidenti informatici
- Attacchi e disastri: pianificare le risposte
- Cosa s'intende per Disaster Recovery; principi per creare un piano
- Valutazione dei rischi, *Business Impact Analysis*
- Analisi forense e valutazione post-incidente

Aspetti legali sulla sicurezza

- Conoscere gli aspetti normativi, le responsabilità dei Direttori dei Sistemi Informativi in base alla Legge sulla Privacy e la Direttiva n. 217 del 16/02/2002 del Presidente del Consiglio sulla "Sicurezza delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali"
- Approfondire gli aspetti sulla sicurezza del Codice della Privacy
- Conoscere gli illeciti penali previsti dal Codice
- Individuare le responsabilità e le conseguenze penali
- Quali sono le sanzioni amministrative
- Ispezioni del Garante

Responsabile del progetto: Cinzia Ruppi

Agenda dei corsi

09.00 Registrazione Partecipanti (1° giorno)
09.30 Inizio dei lavori del corso
11.00 Coffee Break
13.00 Colazione di lavoro
15.30 Tea Break (solo 1° giorno)
18.00 Chiusura dei lavori

*Inoltre uno **speciale Approfondimento** post corso:*

Conoscere TUTTO su

FIRMA DIGITALE e POSTA ELETTRONICA CERTIFICATA

Un approccio pratico e comparativo per chiarire tutti i dubbi e comprendere come agire in sicurezza

1ª edizione: **21 novembre 2008** *2ª edizione:* **20 febbraio 2009**

9.00 *Registrazione dei partecipanti*
9.15 *Inizio dei lavori*

- Conoscere le caratteristiche e le vulnerabilità della Firma Digitale: come tutelarsi da abusi e frodi della firma
- Quali sono i dispositivi informatici innovativi presenti sul mercato per utilizzare la Firma Digitale
- Quanto è sicura la Posta Elettronica Certificata: come gestire i virus e le vulnerabilità informatiche
- Valutare i pro e contro di allegare al messaggio di testo, immagini, audio, video o altro file
- Quali sono i costi della PEC e quanto si risparmia utilizzandola al posto della Raccomandata
- Quali vantaggi comporta l'immediatezza della consegna del messaggio
- Tener traccia delle ricevute da parte dei gestori: quali sono i vantaggi

Stefano Zanero, *Responsabile Tecnico* **Secure Network**

13.00 *Colazione di lavoro*
14.00 *Ripresa dei lavori*

- Conoscere validità, effetti giuridici, efficacia probatoria, responsabilità civili e penali di Firma Digitale e Posta Elettronica Certificata
- Come funziona il sistema di invio e ricezione della Posta Elettronica Certificata
- Cosa comporta l'attribuzione di valore legale alla PEC e quando conviene utilizzarla
- Quali garanzie fornisce la PEC
- Quali sono i benefici e i disagi che derivano dall'utilizzo della Firma Digitale, della PEC e dell'implementazione di una procedura di Conservazione Sostitutiva
- Conoscere i profili di tutela della privacy nei processi gestionali di innovazione tecnologica

Andrea Lisi, *Avvocato* **Studio Associato D&L**

18.00 *Conclusione dei lavori*

Le segnaliamo alcuni dei prossimi eventi IIR:

ITIL FOUNDATION	22-23 ottobre
COSTI E BUDGET INFORMATICI	7-8 ottobre
CONTRATTI INFORMATICI	9-10 dicembre
CONTRACT MANAGER	13-14 novembre

Sicurezza Informatica

■ Si, desidero partecipare al Corso:

- ☐ **I edizione**: 19-20 novembre 2008 — Cod. A 3449 C
- ☐ **II edizione:** 18-19 febbraio 2009 — Cod. A 4009 C

■ **Quota d'iscrizione: Euro 1.395 + 20% I.V.A.** per partecipante

■ Evento completo: Corso + Approfondimento

- ☐ **I edizione**: 19-20+21 novembre 2008 — Cod. A 3449 CW
- ☐ **II edizione:** 18-19+21 febbraio 2009 — Cod. A 4009 CW

■ **Quota d'iscrizione: Euro 2.190 + 20% I.V.A.** per partecipante

La quota d'iscrizione comprende la documentazione didattica, la colazione e i coffee break. Per circostanze imprevedibili, IIR si riserva il diritto di modificare senza preavviso il programma e le modalità didattiche, e/o cambiare i relatori e i docenti.

SCONTO EURO 150
per chi si iscrive 1 mese prima dalla data dell'evento!

■ Sede del corso

Milano - Holiday Inn Milan Garibaldi
Via Ugo Bassi, 1/A angolo C. Farini
20159 Milano - Tel. +39.02.6076801

Ai partecipanti saranno riservate particolari tariffe per il pernottamento

IIR si riserva la facoltà di operare eventuali cambiamenti di sede dell'evento.

■ Modalità di pagamento

Il pagamento è richiesto a ricevimento fattura e in ogni caso prima della data di inizio dell'evento. La quota deve essere versata secondo le modalità di seguito indicate. Copia della fattura/contratto di adesione al corso verrà spedita a stretto giro di posta.

- ☐ Versamento effettuato sul ns. c/c postale n.16834202
- ☐ Assegno bancario - assegno circolare
- ☐ Bonifico bancario:
  Banca Popolare di Sondrio, Agenzia 10 Milano
  C/C 000002805x07, **ABI** 05696, **CAB** 01609,
  intestato a Istituto Internazionale di Ricerca Srl,
  indicando il codice dell'edizione dell'evento; **CIN** Z;
  IBAN IT29 Z056 9601 6090 0000 2805 X07;
  Swift POSOIT22
- ☐ Carta di credito: ❍ Eurocard/Mastercard ❍ American Express ❍ Diners Club ❍ Visa ❍ CartaSì

N°

Scadenza — Titolare

Firma del titolare

■ Modalità di disdetta

L'eventuale disdetta di partecipazione all'intervento formativo dovrà essere comunicata in forma scritta all'Istituto Internazionale di Ricerca entro e non oltre il 10° giorno lavorativo precedente la data d'inizio dell'evento. Trascorso tale termine, sarà inevitabile l'addebito dell'intera quota d'iscrizione. Saremo comunque lieti di accettare un Suo collega in sostituzione purchè il nominativo venga comunicato via fax almeno un giorno prima della data dell'evento.

5 modi per iscriversi

TEL.	02.83847.627	FAX	02.83847.262
E-MAIL	**conferenze@iir-italy.it**		
WEB	**www.iir-italy.it**		
POSTA	Istituto Internazionale di Ricerca Via Forcella, 3 - 20144 Milano		

FORMAZIONE PERSONALIZZATA

In Company Training Solutions è la divisione di IIR specializzata nell'erogare gli **interventi formativi** presso le aziende clienti. Il nostro costante impegno è quello di identificare le soluzioni più appropriate per le diverse funzioni, allineandole alle peculiarità dei diversi mercati di riferimento. Alcuni tra i numerosi vantaggi:

1. fruire di percorsi mirati alle specifiche esigenze professionali
2. creare un momento di coesione e di confronto interno
3. ridurre l'investimento in formazione fino al 40%

Per approfondimenti o per valutare insieme le necessità formative:
Andrea Arena - Tel. 02.83.847.282
Cell. 348.00.273.57 - Trainingsolutions@iir-italy.it

scheda di iscrizione

PRIORITY CODE:SK SCONTO € 200,00

TUTELA DATI PERSONALI - INFORMATIVA

Si informa il Partecipante ai sensi del D.Lgs. 196/03: **(1)** che i propri dati personali riportati sulla scheda di iscrizione ("Dati") saranno trattati in forma automatizzata dall'Istituto Internazionale di Ricerca (I.I.R.) per l'adempimento di ogni onere relativo alla Sua partecipazione alla conferenza, per finalità statistiche e per l'invio di materiale promozionale di I.I.R. I dati raccolti potranno essere comunicati ai partner di I.I.R. e a società del medesimo Gruppo, nell'ambito delle loro attività di comunicazione promozionale; **(2)** il conferimento dei Dati è facoltativo: in mancanza, tuttavia, non sarà possibile dar corso al servizio. In relazione ai Dati, il Partecipante ha **diritto di opporsi** al trattamento sopra previsto.

TITOLARE E RESPONSABILE DEL TRATTAMENTO è l'**Istituto Internazionale di Ricerca**, via Forcella 3, Milano nei cui confronti il Partecipante potrà esercitare i diritti di cui al D.Lgs. 196/03 (accesso, correzione, cancellazione, opposizione al trattamento, indicazione delle finalità del trattamento).

La comunicazione potrà pervenire via: e-mail **variazioni@iir-italy.it** – fax **02.83.95.118** – tel. **02.83.847.634**

■ Dati del partecipante:

Nome — Cognome

Funzione

Indirizzo

Città — CAP — Prov.

Tel. — Cell.

Si, desidero ricevere informazioni su altri eventi via
(segnalare eventuale preferenza):

❑ Fax

❑ E-mail

Consenso alla partecipazione dato da: Funzione

Nome e Cognome

■ Dati dell'Azienda:

Ragione Sociale

Settore Merceologico

Fatturato in Euro 6 ❑0-10 Mil 5 ❑11-25 Mil 4 ❑26-50 Mil 3 ❑51-250 Mil 2 ❑251-500 Mil 1 ❑+500 Mil

Numero dipendenti G ❑1-10 F ❑11-50 E ❑51-100 D ❑101-200 C ❑201-500 B ❑501-1000 A ❑+1000

Partita I.V.A.

Indirizzo di fatturazione

Città — CAP — Prov.

Tel. — Fax

Timbro e firma

Stampa n. 140