

## Corso: **Cybersecurity Fundamentals (CSX)**

L'IT è la struttura nella quale si concentrano le informazioni necessarie per la gestione del business aziendale. Cybersecurity Nexus (CSX) è il programma professionale di ISACA Intl con il quale verranno sviluppate le conoscenze per una corretta gestione della sicurezza informatica. Il programma CSX è il risultato dell'esperienza ultra decennale maturata da ISACA International nelle attività di auditing, gestione dei rischi, security management e IT Governance. CSX sta aiutando a plasmare il futuro della sicurezza informatica.

Con CSX imprenditori e professionisti informatici possono ottenere le conoscenze e gli strumenti per essere all'avanguardia di un settore vitale ed in rapida evoluzione.

### Durata

Il corso ha la durata di **due giornate** (ogni giornata prevede **8** ore di formazione, con un'ora di pausa per il pranzo).

### Obiettivi

Questo corso, organizzato da NPC in collaborazione con ISACA Rome Chapter, fornisce tutte le competenze teoriche e pratiche, nonché i suggerimenti utili per sostenere l'esame CSX Fundamentals di ISACA.

- Ulteriore obiettivo del corso è quello di fornire le competenze pratiche per:
- Spiegare i principi chiave della sicurezza delle informazioni
- Identificare i componenti chiave dell'architettura di una Cyber Security Network
- Applicare i principi dell'architettura di Cyber Security
- Descrivere i processi e le pratiche di Risk Management
- Identificare i security tools e le tecniche di hardening
- Distinguere minacce e vulnerabilità della sicurezza dei sistemi e delle applicazioni
- Descrivere le diverse classi di cyber-attacchi
- Definire i tipi di incidents, tra cui categorie, responses e responses' timeline
- Descrivere le nuove ed emergenti tecnologie IT e IS
- Analizzare minacce e rischi nel contesto dell'architettura di cyber-security
- Valutare i cybersecurity incidents per applicare la contromisura più adeguata
- Valutare i risultati connessi agli scenari di Cybersecurity derivanti dai processi decisionali



## Destinatari del corso

Il Corso è rivolto a:

- ▼ CIO, Manager IT, Specialisti IT
- ▼ Responsabili della Sicurezza
- ▼ Internal Audit
- ▼ IT Auditor
- ▼ Esperti di sicurezza IT
- ▼ Privacy officer
- ▼ Consulente della Privacy

## Programma del corso

- ▼ Cybersecurity: introduzione e panoramica
  - Definizione di Cybersecurity
  - Obiettivi della cybersecurity
  - Fattori chiave tecnologici e di business
  - Ruolo e governance della Cybersecurity
  - Domini della cybersecurity
- ▼ Nozioni sulla Cybersecurity
  - Nozioni, terminologia e quadri di riferimento del risk management
  - Tipologie e vettori degli attacchi più comuni
  - Processi generali e attributi degli attacchi cyber
  - Malware
  - Riferimenti e linee guida per politiche e procedure
  - Processi di controllo della cybersecurity
- ▼ Architettura di sicurezza
  - Nozioni sul perimetro di sicurezza
  - Architetture di sicurezza e quadri di riferimento
  - Il modello OSI e il protocollo di comunicazione TCP/IP
  - Defense in depth
  - Nozioni sui firewall e sulle loro implementazioni
  - Isolamento e segmentazione
  - Sistemi di intrusion detection e prevention
  - Antivirus e anti-malware
  - Fondamenti di crittografia, tecniche e applicazioni



▼ Sicurezza delle reti, sistemi, applicazioni e dati

- Strategie di risk analysis, risk assessment e di mitigazione
- Scanning, assessment e gestione delle vulnerabilità
- Penetration testing
- Network management e configurazione
- Port number e protocolli
- Rischi e controlli per l'accesso remoto e wireless
- Hardening sei sistemi e virtualizzazione
- Sistemi specializzati
- Conoscenza dei command line e degli strumenti
- System development life cycle (SDLC)
- OWASP top ten application security risk
- Processo di classificazione dei dati e requisiti

▼ Incident response

- Distinzioni tra eventi e incidenti
- Categorie e tipi di incidenti
- Security event management
- Elementi chiave dei piani di incident response
- Requisiti legali sulle investigazioni e sulla conservazione delle prove
- Requisiti per le investigazioni forensic
- Business continuity planning e disaster recovery

▼ Implicazioni di sicurezza riguardo l'adozione delle tecnologie emergenti

- Tendenze nell'attuale panorama delle minacce
- Caratteristiche e obiettivi delle advanced persistent threat (APT)
- Vulnerabilità dei dispositivi mobili, minacce e rischi
- BYOD e trasformazione dell'IT e dei dispositivi mobili per il mercato consumer
- Rischi e benefici del cloud e della digital collaboration

Il corso è in Italiano e il materiale è in Inglese per specifica disposizione di ISACA

## Materiale didattico

Il materiale didattico comprende:

- ▼ Copia dei lucidi proiettati durante il corso come da programma

## CPE

15 CPE validi ai fini del mantenimento delle certificazioni ISACA

## Esame

L'esame, non incluso, disponibile in modalità online, potrà essere acquistato direttamente dal discente da [www.isaca.org](http://www.isaca.org)



Se di interesse, **i corsi possono anche essere organizzati ad hoc presso il cliente**. In questo caso essendo un corso a voi riservato, sarà nostra cura raccoglie eventuali vostre specifiche esigenze, per affrontarle durante il corso, rendendolo così il più possibile operativo e concreto.

## Docente

### Claudio Cilli

Autorità riconosciuta a livello mondiale nelle aree della Sicurezza nazionale e dell'intelligence, sicurezza dei sistemi informativi e compliance normativa con oltre 25 anni di esperienza, è attualmente advisor di Governi e grandi aziende per la cyber-security e protezione delle infrastrutture critiche.

Docente presso l'Università degli Studi di Roma "La Sapienza", membro di comitati scientifici, e chairman di conferenze internazionali. Certification he currently holds: CIA, CISA, CISM, CGEIT, CRISC, CISSP, CSSLP, HCISPP, M.Inst.ISP, CX, QA. È presidente del Capitolo di Roma dell'ISACA.

Consulente di grandi aziende pubbliche e private, oltre che banche e istituti finanziari, nei settori delle tecnologie dell'informazione, Edp auditing, qualità e certificazione dei sistemi elettronici e del software, ha realizzato interventi di progettazione e adeguamento di grandi sistemi di calcolo, e altri su architetture distribuite. Si occupa di Disaster Recovery e continuità operativa, sicurezza nel trattamento delle informazioni e protezione delle installazioni.

È consulente delle Nazioni Unite a New York per la sicurezza e l'audit dei sistemi informatici e della Difesa degli Stati Uniti.

Nominato dall'European Union Agency for Network and Information Security (ENISA) Esperto per l'assistenza nell'implementazione dei programmi operativi dell'agenzia con un contratto relativo alle attività di Emerging application areas (transportation and automotive, eGovernment, eHealth, etc.) e Information security risk management

È membro di diverse commissioni scientifiche presso l'Unione Europea in tema di sicurezza informatica, cyber-security e rapporti con le strutture accademiche.

Ha progettato sistemi di elaborazione "sicuri" per le Forze Armate. E' autore di libri tecnici e articoli pubblicati su riviste del settore in Italia e all'estero, ed è relatore in conferenze internazionali.



## Prezzo del corso

Corso multiaziendale a calendario (Roma – Milano).

- ▼ Soci ISACA Roma **650 € + IVA** per partecipante
- ▼ NON soci: **790 € + IVA** per partecipante

## Scheda di iscrizione

<b>Società</b>				
Ragione Sociale _____				
P.IVA/Cod fiscale _____		Indirizzo _____		
Indirizzo _____		CAP _____	Città _____	Pv. _____
Referente acquisti (nome e cognome) _____, _____,				
Tel. _____		Mail _____		
Partecipanti (nome e cognome) _____, _____,				
Partecipanti (nome e cognome) _____, _____,				
Partecipanti (nome e cognome) _____, _____,				

Segnare nella tabella sottostante il numero dei partecipanti, la data, il luogo e indicare l'importo totale.

N° Partecipanti	Corso	data	Luogo	Importo (IVA esclusa)
	Cybersecurity Fundamentals (CSX)			

## Fatturazione e Condizioni di pagamento

La fatturazione sarà eseguita all'ordine e il pagamento dovrà essere effettuato prima del corso a mezzo:

**Bonifico bancario** al seguente conto corrente:

**Intestatario:** Net Partner Consulting S.r.l.

**Banca:** Banca IntesaSanPaolo

**IBAN:** IT68 K030 6909 2021 0000 0008 106 -

**Oggetto:** "Titolo del corso, numero partecipante, azienda"



Copia dell'avvenuto pagamento dovrà essere inviata a mezzo mail all'indirizzo indicato al punto1 delle condizioni contrattuali.

## Clausole Contrattuali

### 1. Iscrizione

La presente iscrizione, compilata in ogni sua parte e sottoscritta, va inviata a mezzo e mail [corsi@netpartnerconsulting.com](mailto:corsi@netpartnerconsulting.com) che invierà conferma di avvenuta accettazione.

### 2. Tempi e Modalità di Recesso

E' possibile richiedere la restituzione della quota di iscrizione versata se il recesso avviene entro 10 giorni solari precedenti l'inizio del corso. Dopo tale termine non è previsto alcun rimborso e l'importo dovuto verrà fatturato. Se il partecipante non ha attivato il recesso e non si presenta in aula, sarà comunque dovuto l'intero importo. Il recesso dovrà essere attivato a mezzo mail (all'indirizzo di iscrizione) oppure a mezzo fax al num. +39 06 5455 0513

### 3. Variazioni di Programma

NPC si riserva la facoltà di rinviare o annullare il corso programmato dandone comunicazione a mezzo e-mail ai partecipanti entro tre giorni lavorativi prima della data di inizio del corso, in tal caso suo unico obbligo è provvedere al rimborso dell'importo ricevuto senza ulteriori oneri. Altresì si riserva la facoltà di modificare il programma/sede del corso e/o sostituire i docenti indicati con altri docenti di pari livello professionale.

### 4. Foro Competente

Il foro esclusivo competente è quello di Torino.

### 5. Diritti d'autore

I corsi ed i materiali ad essi relativi sono di proprietà esclusiva di NPC. E' vietato pertanto qualsiasi tipo di copia o riproduzione del materiale e la diffusione a terzi del contenuto dei corsi, anche parzialmente, senza previa autorizzazione scritta di NPC. Sono altresì vietate audio /video registrazioni se non preventivamente autorizzate.

### 6. Privacy

Informativa ai sensi dell'art. 13 DLGS 30.06.2003, N. 196 e successive modificazioni. Ai sensi del DLGS N. 196/2003 le informazioni fornite verranno trattate per finalità di gestione amministrativa dei corsi. I dati potranno essere utilizzati per la creazione di un archivio ai fini dell'invio (via e-mail o a mezzo posta) di proposte per corsi ed iniziative future di NPC. Potrete accedere alle informazioni in nostro possesso ed esercitare i diritti di cui all'art. 7 della Legge (aggiornamento, rettifica, integrazione, cancellazione, ecc.) inviando una richiesta a mezzo e mail a [corsi@netpartnerconsulting.com](mailto:corsi@netpartnerconsulting.com).

Firma per accettazione (con timbro aziendale)

---

Firma e timbro per specifica approvazione delle clausole 4, 5 (art. 1341 2° comma Codice Civile)

---

