|  |  |  |  |
| --- | --- | --- | --- |
| **Security in ambiente Power/IBM i (Avanzato)****Dal 20/10/2025 al 23/10/2025****Termine ultimo per l’iscrizione: 05/10/2025** | **Q.tà** | **Quota individuale** | **Importo** |
| **Primo partecipante** | **1** | **€ 900,00** | **€ 900,00** |
| **Ulteriori partecipanti della stessa azienda (quota ridotta)** |  | **€ 450,00** |  |
| **TOTALE** |  |

|  |  |
| --- | --- |
| Ragione Sociale |  |
| Indirizzo |  |
| CAP – Città – Provincia |  |
| P. IVA |  |
| Codice Fiscale |  |
| **Codice Destinatario o PEC** |  |
| Email riferimento risorse umane |  |
| Email riferimento amministrativo |  |
| **Partecipanti**  | **Nome e cognome** | **email** |
|  |  |
|  |  |
|  |  |

Luogo e data: Timbro e firma:

1. **MODALITA’ DI EROGAZIONE**

Il corso si terrà **On-line** **nei giorni dal 20/10/2025 al 23/10/2025 compresi in orario 09:00 – 13:00 (quattro lezioni di quattro ore ciascuna)**

Lo svolgimento del corso sarà confermato solo al raggiungimento di un numero minimo di iscrizioni

Responsabile tecnico e didattico: **Vincenzo Turturro 348 8709470** vincenzo.turturro@faq400.com

Responsabile amministrativa: **Cinzia Bonanomi 348 1568631** cinzia.bonanomi@faq400.com

1. **CORRISPETTIVO E SPESE**

Tutti gli importi si intendono IVA Esclusa

Fatturazione: **al raggiungimento del numero minimo di iscrizioni**

Pagamento: **tassativo entro il quindicesimo giorno solare precedente la data di inizio**

I corrispettivi dovuti dovranno essere versati secondo le modalità comunicate al momento della fatturazione

**Il mancato pagamento del saldo nei tempi indicati comporterà l’annullamento dell’iscrizione**

Faq400 Srl emetterà fattura elettronica, per cui è necessario indicare il codice destinatario o l’indirizzo PEC

1. **TRATTAMENTO DEI DATI PERSONALI**

I dati personali e anagrafici forniti per motivi fiscali e/o contrattuali rimarranno custoditi presso la sede di Faq400 Srl per finalità di archiviazione, elaborazione, documentazione e attività di marketing; in ogni momento è possibile esercitare i propri diritti ai sensi del Regolamento UE 679/2016, scrivendo al Responsabile del trattamento.

Dichiaro di:

* aver preso visione dei punti a), b), c)
* approvare il programma del corso allegato al presente ordine, ritenendolo adeguato alle necessità formative degli iscritti, e **di aver preso visione della voce “Requisiti dei partecipanti”**
* **riconoscere che la firma apposta è vincolante ed impegna alla partecipazione al corso ed al pagamento della relativa fattura che sarà emessa alla conferma del corso da parte di Faq400**

Timbro e firma: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| **Descrizione** | Il corso fornisce informazioni pratiche relative alle attività in ambito cyber security per la protezione dei sistemi Power/IBM i.L’obiettivo del corso è quello di fornire agli Amministratori di Sistema (AdS) le informazioni necessarie per:* evidenziare i rischi
* apportare i corretti interventi per le mitigazioni tecniche
* affrontare correttamente un progetto, basato sugli adempimenti normativi da osservare, per la protezione dei dati e delle infrastrutture

Il corso fornisce agli AdS gli elementi di un Risk Assessment funzionale, a partire dal quale sviluppare il piano di Sicurezza del sistema e della realtà nella quale è integrato, mediante l’interazione con i vari dipartimenti aziendali. |
| **Argomenti** | Quadro normativo* Evidenza delle norme per la sicurezza dei dati
* L’impatto delle norme sulla piattaforma IBM i
* Adempimenti e Incident Response

Cyber security * Attacchi informatici
* Quali sono le cause
* Fattore umano (formazione e ingegneria sociale)
* Strategie di cybersicurezza

L’ambiente IBM i * Risk Assessment & Risk Management
	+ come vengono analizzate le informazioni
* Sicurezza in ambiente IBM i
* Sicurezza di base del sistema
	+ limitare i permessi speciali
	+ limitare l'accesso alla riga comandi
	+ limitare l’accesso all’IFS

Mitigazioni e Remediation* Contesto infrastrutturale
* Dati - Applicativi - Database
* Integrazione con strumenti di Monitoring (SIEM/SOC)
* Il processo
	+ estrazione dei log
	+ elaborazione dei log - SIEM
	+ elaborazione dei log – SOC
	+ analisi ed utilizzo dei risultati
* Audit
* Misure di Sicurezza
* Procedura di Incident Response
 |
| **Durata** | 16 ore |
| **Modalità** | Da remoto |
| **Destinatari** | Amministratori di Sistema, Sviluppatori, Database Administrator, ICT Manager |
| **Numero massimo di partecipanti** | 8 |
| **Requisiti dei partecipanti** | Conoscenza a livello sistemistico del sistema Power/IBM i, conoscenza delle tecnologie di rete, conoscenza degli applicativi e dei database aziendali |
| **Materiale didattico rilasciato** | Slide presentate durante il corsoTool per effettuare Risk AssessmentFile Report Risk AssessmentDocumentazione per RemediationAccesso alla piattaforma e-learning per testAttestato di superamento del test |