TITOLO CORSO

Cybersecurity

REQUISITI SOGGETTIVI RICHIESTI AI PARTECIPANTI AI FINI DELL'ACCESSO

Non sono richiesti prerequisiti specifici per la partecipazione al corso. Tuttavia, è consigliata una conoscenza di base dei concetti di informatica e internet.

FUNZIONE CORSO

- **Corso libero ai fini di upskilling**
  - Lingue straniere, italiano per stranieri
  - Vendita, marketing
  - **Contabilità, finanza**
  - **Gestione aziendale (risorse umane, qualità, ecc) e amministrazione**
  - Lavoro d'ufficio e di segreteria
  - Sviluppo delle abilità personali
  - Informatica
  - Tecniche e tecnologie di produzione manifatturiera e delle costruzioni
  - Tecniche e tecnologie di produzione dell'agricoltura, della zootecnia e della pesca
  - Tecniche, tecnologie e metodologie per l'erogazione di servizi sanitari e sociali
  - Salvaguardia ambientale
  - Salute e sicurezza sul lavoro
  - **Tecniche, tecnologie e metodologie per l'erogazione di servizi economici**
  - **Conoscenza del contesto lavorativo**

- Corso rivolto all'acquisizione di qualificazioni, certificazioni ed abilitazioni professionali

  - Corsi di upskilling/reskilling con rilascio di certificati di qualificazione, anche relativi a singole competenze, ai sensi del D. Lgs. 13/13 o di altra norma pubblica
  - Corsi abilitanti all'esercizio di attività e professioni oggetto di norma pubblica nazionale, ivi inclusi i corsi di cui al D. Lgs. 81/08
  - Corsi conclusi dal rilascio di certificazioni di parte terza privata
  - Corsi ECM accreditati dalla Commissione nazionale con attestazione dei crediti da parte del provider
  - Corsi per assolvimento di obblighi di aggiornamento professionale definiti dai relativi Ordini e Collegi
  - Corsi con attestazioni/certificazioni almeno di parte seconda privata, relativi a prodotti e servizi digitali, erogati da soggetti abilitati dai relativi vendor

OBIETTIVI FORMATIVI

Al termine del corso, i partecipanti saranno in grado di:

- Comprendere i principi base della sicurezza informatica
- Riconoscere le minacce informatiche più diffuse
- Proteggere i propri dati personali e aziendali

- Difendersi da attacchi informatici come phishing, malware e ransomware
- Navigare in internet in modo sicuro
- Utilizzare i social media in modo consapevole
- Mantenere aggiornati i software e i sistemi informatici
- Adottare un comportamento sicuro online

MODALITA' DI VALUTAZIONE DEGLI APPRENDIMENTI

La valutazione degli apprendimenti individuali costituisce uno degli aspetti definiti nel sistema di qualità aziendale certificato di Ottima Formazione Srl nell'ambito del Project Cycle Management adottato, con lo scopo di verificare:

- quali conoscenze sono state trasmesse ai partecipanti

- quali abilità sono state sviluppate

- quali atteggiamenti sono stati modificati

Vengono così ottenute informazioni a integrazione di quelle raccolte con il sistema di monitoraggio e valutazione, utili al completamento dell'analisi dei risultati sotto il profilo concettuale, in particolar modo per quanto riguarda l'efficacia delle metodologie utilizzate e la spendibilità della formazione nel contesto di lavoro.

TIPOLOGIA ATTESTAZIONE RILASCIATA

- ☐ Attestazione trasparente delle competenze acquisite
- ☐ Dispositivi di certificazione regionali
- ☐ Acquisizione di titoli abilitanti a professioni regolamentate
- ☐ Certificazioni privatistiche
- ☐ Acquisizione di certificazioni standard in materia di informatica e lingue straniere
- ☐ Acquisizione di crediti ECM o altri crediti previsti da Ordini Professionali
- ☐ Crediti formativi universitari
- ☐ **Attestato di frequenza**

MODALITA' DI CONTATTO DEL SOGGETTO FORMATIVO

I professionisti di Ottima Formazione sono reperibili telefonicamente dal lunedì al venerdì, dalle 8.30 alle 13.00 e dalle 14.00 alle 18.00 al numero 0544465108, oppure tramite mail all'indirizzo segreteria@ottimaformazione.it

FREQUENZA MINIMA OBBLIGATORIA

70 %

COSTO PER PARTECIPANTE

450,00

DURATA

20 h

NOTE:

PAGINA WEB DI RIFERIMENTO INFORMATIVO:
https://www.ottimaformazione.it/servizi-2/fon-coop/

CONDIZIONI DI ATTIVAZIONE: Il corso sarà attivato al raggiungimento di almeno 4 iscritti

EVENTUALE SCONTISTICA: Sconto del 20% sul 2° iscritto

DESCRIZIONE DEL CORSO: Il corso fornisce una panoramica completa delle minacce informatiche più diffuse e delle strategie per difendersi. Il corso approfondisce i concetti di sicurezza informatica, i rischi per le persone e le organizzazioni, e le metodologie per la protezione dei dati e dei sistemi informatici.
Vengono inoltre illustrate le best practice per la sicurezza informatica, come la creazione di password sicure, l'utilizzo di un software antivirus aggiornato e la navigazione sicura in internet.

MODALITA' EROGAZIONE CORSO

- Aula
- **Webinar, videoconferenza**
- Affiancamento, training on the job, coaching, mentoring
- Project work assistito
- Stage esterno all'impresa beneficiaria
- Corsi di Fad on line

TEMATICA FORMATIVA

- Lingue straniere, italiano per stranieri
- Vendita, marketing
- Contabilità, finanza
- Gestione aziendale (risorse umane, qualità, ecc) e amministrazione
- Lavoro d'ufficio e di segreteria
- Sviluppo delle abilità personali
- **Informatica**
- Tecniche e tecnologie di produzione manifatturiera e delle costruzioni
- Tecniche e tecnologie di produzione dell'agricoltura, della zootecnia e della pesca
- Tecniche, tecnologie e metodologie per l'erogazione di servizi sanitari e sociali
- Salvaguardia ambientale
- Salute e sicurezza sul lavoro
- Tecniche, tecnologie e metodologie per l'erogazione di servizi economici
- Conoscenza del contesto lavorativo

DESCRIZIONE CONTENUTO MODULO FORMATIVO

MODULO 1 – 3 ore

Introduzione alla Cybersecurity

- Concetti fondamentali di sicurezza informatica

- Importanza della cybersecurity nell'era digitale
- Panoramica delle minacce e degli attacchi informatici più comuni

Principi di Sicurezza Informatica
- Confidenzialità, integrità e disponibilità (CIA triad) dei dati
- Principi di difesa in profondità (defense in depth) e mitigazione dei rischi
- Approccio proattivo vs. reattivo alla cybersecurity

MODULO 2 – 3 ore

Minacce e Attacchi Informatici
- Malware (virus, worm, trojan, ransomware, ecc.)
- Phishing e social engineering
- Attacchi di tipo Denial-of-Service (DoS) e Distributed Denial-of-Service (DDoS)

Sistemi Operativi Sicuri
- Sicurezza nei sistemi operativi desktop e server
- Patch management e aggiornamenti di sicurezza
- Configurazioni di sicurezza e hardening dei sistemi operativi

MODULO 3 – 4 ore

Reti Sicure
- Concetti di base delle reti informatiche
- Architetture di rete sicure
- Firewall, VPN e altre tecnologie per la protezione delle reti

Crittografia e Sicurezza dei Dati
- Principi di crittografia e algoritmi crittografici
- Utilizzo della crittografia per proteggere i dati in transito e a riposo
- Gestione delle chiavi crittografiche e certificati digitali

MODULO 4 – 4 ore

Gestione delle Identità e degli Accessi
- Autenticazione e autorizzazione degli utenti
- Single Sign-On (SSO) e federazione delle identità
- Best practice per la gestione degli accessi privilegiati

Sicurezza delle Applicazioni
- Principi di sviluppo sicuro delle applicazioni
- Testing della sicurezza delle applicazioni (penetration testing, code review, ecc.)
- Best practice per la sicurezza dei siti web e delle applicazioni web

MODULO 5 – 4 ore

Monitoraggio e Risposta agli Incidenti

- Ruolo del monitoraggio dei log e degli eventi di sicurezza
- Pianificazione e gestione degli incidenti di sicurezza
- Investigazione forense digitale

Compliance e Normative sulla Sicurezza

- Principali normative e standard di sicurezza informatica (GDPR, PCI DSS, HIPAA, ecc.)
- Processi di conformità e audit
- Ruolo della privacy e della protezione dei dati personali

MODULO 6 – 2 ore

Tendenze e Sfide Emergenti

- Evoluzione delle minacce informatiche
- Sicurezza nell'era del cloud computing, dell'Internet of Things (IoT) e dell'intelligenza artificiale
- Implicazioni della cybersecurity nel contesto geopolitico