

FONDAMENTI DI CYBERSECURITY E PROTEZIONE DEI DATI PER AZIENDE E PROFESSIONISTI

1. Informazioni generali

Titolo del corso: Fondamenti di Cybersecurity e Protezione dei Dati per Aziende e Professionisti

Docente: Per. Ind. Riccardo Ettore Tittaferante

Durata complessiva: 40 ore

Modalità di erogazione: Formazione online tramite piattaforma Teams o GoToMeeting

Frequenza proposta: 3 giornate settimanali (MARTEDI', MERCOLEDI' E GIOVEDI')

Fascia oraria proposta: 13.30 – 17.30

Durata prevista del percorso: circa 4 settimane

Nota organizzativa: la frequenza e la fascia oraria indicate costituiscono una proposta organizzativa e potranno essere concordate e rimodulate in funzione delle esigenze didattiche, organizzative e del gruppo classe.

2. Descrizione del corso

La crescente diffusione delle tecnologie digitali, del cloud computing e dei servizi online rende sempre più importante la conoscenza delle principali problematiche legate alla sicurezza informatica e alla protezione dei dati.

Il corso fornisce una preparazione introduttiva ma concreta sui temi della Cybersecurity e della Data Protection, affrontando i principali rischi informatici che interessano aziende, professionisti e privati cittadini.

Attraverso esempi pratici, casi reali e discussioni guidate, i partecipanti acquisiranno una maggiore consapevolezza nell'utilizzo degli strumenti digitali e comprenderanno le principali misure di prevenzione e protezione da adottare nella quotidianità lavorativa e personale.

3. Obiettivi formativi

Al termine del percorso i partecipanti saranno in grado di:

© Comprendere i principi fondamentali dell'informatica e della trasformazione digitale.

- ⊗ Distinguere gli ambiti della Data Protection e della Cybersecurity.
- ⊗ Comprendere i principali obblighi normativi relativi alla protezione dei dati personali.
- ⊗ Identificare le principali minacce informatiche moderne.
- ⊗ Riconoscere comportamenti a rischio e adottare corrette misure di prevenzione.
- ⊗ Comprendere i concetti di continuità operativa e gestione degli incidenti informatici.
- ⊗ Acquisire maggiore consapevolezza nell'utilizzo di strumenti e servizi digitali.

4. Destinatari

Il corso è rivolto a:

- ⊗ Disoccupati e persone in cerca di occupazione.
 - ⊗ Lavoratori dipendenti.
 - ⊗ Impiegati amministrativi.
 - ⊗ Professionisti e consulenti.
 - ⊗ Piccoli imprenditori.
 - ⊗ Diplomati e neodiplomati.
 - ⊗ Utenti che desiderano acquisire competenze introduttive nel settore della sicurezza informatica.
- Non sono richieste competenze tecniche avanzate.

5. Programma didattico

Modulo 1 – Fondamenti di ICT e Trasformazione Digitale

- ⊗ Introduzione all'informatica moderna.
- ⊗ Hardware, software e sistemi operativi.
- ⊗ Reti informatiche e Internet.
- ⊗ Cloud Computing e servizi digitali.
- ⊗ Evoluzione delle tecnologie digitali.
- ⊗ Digitalizzazione delle imprese.
- ⊗ Principali rischi connessi all'utilizzo delle tecnologie informatiche.

Obiettivo del modulo Fornire le basi necessarie per comprendere il funzionamento dei sistemi informatici e il loro ruolo nei moderni processi aziendali.

Modulo 2 – Data Protection e Protezione dei Dati Personali

- ⊗ Introduzione alla Data Protection.
- ⊗ Dati personali e dati particolari.
- ⊗ Principi fondamentali del GDPR.
- ⊗ Ruoli e responsabilità nella gestione dei dati.
- ⊗ Trattamento e conservazione delle informazioni.
- ⊗ Violazioni dei dati personali (Data Breach).
- ⊗ Analisi di casi pratici.

Obiettivo del modulo Comprendere i principi della protezione dei dati personali e le principali responsabilità organizzative e operative.

Modulo 3 – Fondamenti di Cybersecurity

- ⊗ Differenze tra Data Protection e Cybersecurity.
- ⊗ Information Security e Cybersecurity.
- ⊗ Minacce informatiche moderne.
- ⊗ Malware, ransomware e spyware.
- ⊗ Phishing e social engineering.
- ⊗ Sicurezza della posta elettronica.
- ⊗ Gestione delle password.
- ⊗ Autenticazione multifattore.
- ⊗ Sicurezza della navigazione web.
- ⊗ Introduzione alla sicurezza delle reti.

Obiettivo del modulo Comprendere il panorama delle minacce informatiche e le principali tecniche di prevenzione e difesa.

Modulo 4 – Sicurezza Operativa e Continuità dei Servizi

- ⊗ Sicurezza dei dispositivi informatici.
- ⊗ Aggiornamenti e gestione delle vulnerabilità.

ATTAL GROUP S.P.A.

Agenzia per il Lavoro
Aut. Min. Prot. N°0013582
del 03/10/2012
C.F. e P.I. 06961760722
R.E.A. Milano n° 1968033

Sede Legale

Via Marco D'Aviano, 2
20131 - Milano (MI)
Tel 02 454320 - info@attalgroup.it
www.attalgroup.it



- ⊗ Backup e protezione delle informazioni.
- ⊗ Business Continuity.
- ⊗ Disaster Recovery.
- ⊗ Sicurezza nel lavoro da remoto.
- ⊗ Introduzione alle misure di protezione delle infrastrutture informatiche.

Obiettivo del modulo Acquisire le conoscenze fondamentali per garantire la continuità operativa e la protezione dei dati in ambito lavorativo.

Modulo 5 – Casi Studio e Verifica Finale

- ⊗ Analisi di incidenti informatici realmente accaduti.
- ⊗ Discussione guidata.
- ⊗ Analisi delle contromisure adottate.
- ⊗ Ripasso generale dei contenuti.
- ⊗ Verifica finale dell'apprendimento.

Obiettivo del modulo Consolidare le competenze acquisite attraverso l'analisi di casi concreti e la verifica delle conoscenze maturate.

6. Metodologia didattica

Il percorso formativo sarà erogato attraverso:

- ⊗ Lezioni frontali online.
- ⊗ Presentazioni multimediali.
- ⊗ Analisi di casi reali.
- ⊗ Discussioni guidate.
- ⊗ Esempi pratici tratti dall'esperienza professionale del docente.
- ⊗ Sessioni di confronto con i partecipanti.
- ⊗ Verifica finale dell'apprendimento.

8. Note finali

Il percorso è stato progettato sulla base dell'esperienza professionale e didattica maturata dal docente nell'ambito della consulenza informatica, della sicurezza delle informazioni e della formazione professionale.

L'impostazione del corso privilegia un approccio pratico e orientato alla realtà operativa di aziende e professionisti, con particolare attenzione ai temi della protezione dei dati, della consapevolezza digitale e della prevenzione dei rischi informatici.