Labor Project®

ELEMENTI DI CYBERSECURITY E SICUREZZA DELLE INFORMAZIONI

CORSO SPECIFICO PER NON I.T.

PERCHÈ SCEGLIERE QUESTO CORSO

Apprendi le migliori strategie e mettile al servizio delle tue aziende e organizzazioni potenziando le tue competenze. **Non** devi essere un hacker o un informatico per garantire la sicurezza delle informazioni. **Diventa un esperto di Cyber Security** senza essere un I.T.

Un corso cybersecurity è imprescindibile per:

- **formazione sulla sicurezza dei dati**, con focus sull'importanza di proteggere le informazioni sensibili e su quali minacce dannose prestare attenzione;
- **consapevolezza** della sicurezza informatica e riduzione dei rischi;
- **comportamenti** da seguire.

PERCHÈ NOI

Labor Project srl ha conseguito la certificazione ISO 9001:2015 ed è Ente di formazione accreditato dalla Regione Lombardia per i servizi di Istruzione e Formazione Professionale (accreditamento n. 543).

È stata riconosciuta da CEPAS società di Bureau Veritas Italia Spa UNI 11697 quale soggetto qualificato per l'erogazione del "Corso di Alta Formazione Data Protection Officer".

Labor Project srl è membro dell'Associazione Data Protection Officer (ASSO DPO), che ha nominato quale Presidente il Dott. Matteo Colombo - A.D. di Labor Project srl.

Labor Project srl è Bronze Sponsor di IAPP | International Association of Privacy Professionals, di cui il Team Leader è anche membro.

DESTINATARI

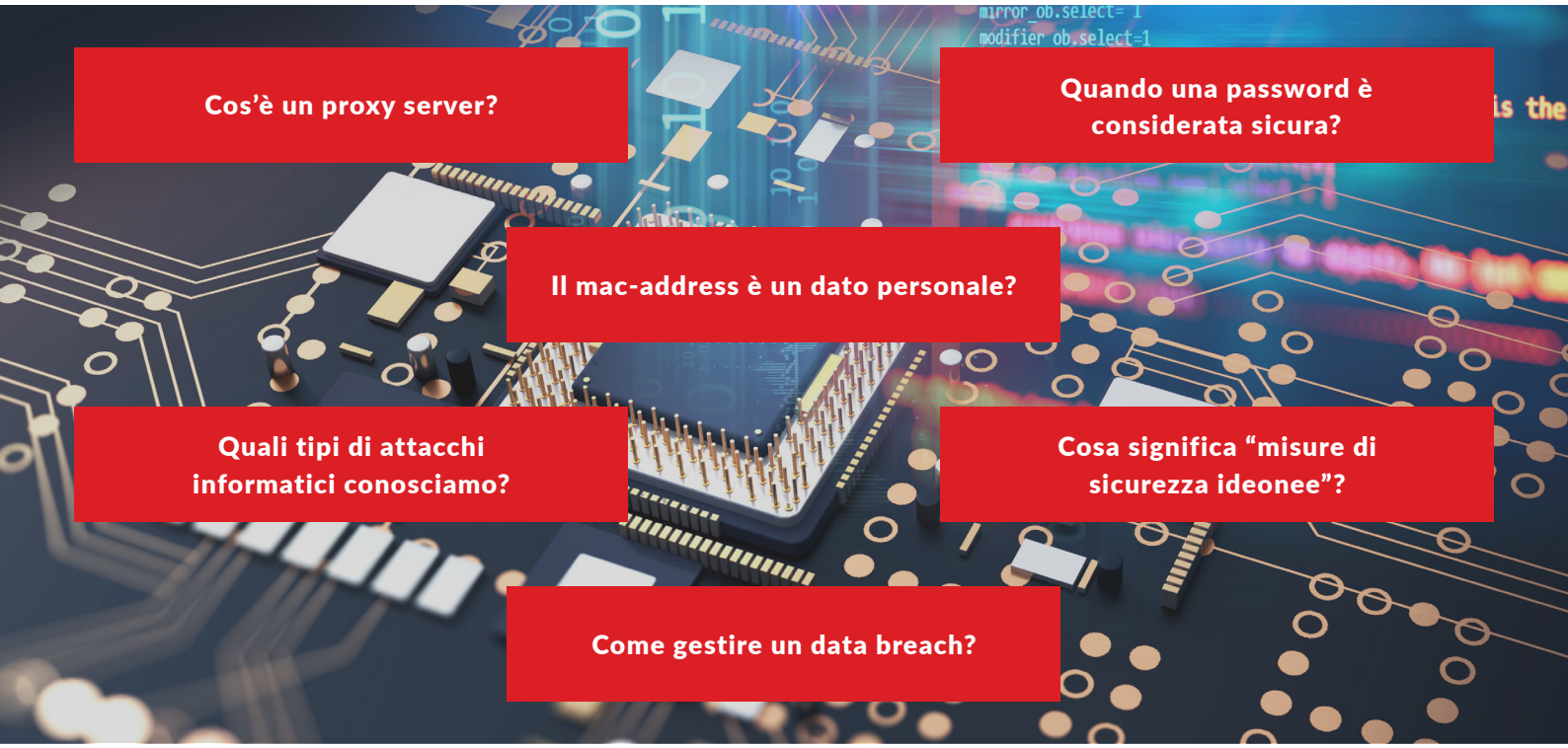
Il corso è un'offerta di formazione continua destinata a Legal Compliance Officer, Data Protection Officer (DPO), Privacy Manager, consulenti privacy, legali d'impresa e designati al trattamento che **non hanno una profonda cultura informatica** e che vogliono aumentare la propria conoscenza e consapevolezza in tema di Cybersecurity e Sicurezza delle informazioni.

Corso valido per l'aggiornamento obbligatorio del professionista del trattamento e della protezione dei dati personali certificato UNI 11697:2017.

A COSA SERVE?

OBIETTIVO CORSO

Spesso durante le attività lavorative ci si pone domande tecniche e all'interno di un'organizzazione solo gli informatici o "quello dell'I.T." sanno rispondere.



Il corso, rivolto a chi **NON** è un esperto informatico, ha lo scopo di creare maggiore consapevolezza nelle figure aziendali comunque chiamate a presidio in temi di data protection e permetterà loro di affrontare riunioni e discussioni su questi temi con maggior padronanza.

I PROFESSIONISTI

DOCENTI

Matteo Colombo

A.D. di Labor Project, Direttore di Privacy Desk Suisse e Presidente di ASSO DPO. Socio Fondatore di AIRIA. Data Protection Officer, Certified Information Privacy Professional Europe (CIPP/E), Certified Information Privacy Manager (CIPM) e Fellow of Information Privacy (FIP) di IAPP, consulente d'impresa e formatore.

Alberto Guglielmi

CEO & Co-Founder di Opticon Data Solutions e Opticon Data Swiss, gruppo societario LegalTech specializzato nella consulenza in materia di nuove tecnologie e nello sviluppo di applicativi utili a supportare le aziende nel percorso di Compliance e Data Protection.

Giancarlo Calzetta

Giornalista specializzato in IT da oltre 30 anni, è direttore di Security Info, sito web verticale sulla sicurezza informatica, e B2BLabs, canale business di Tom's Hardware. Per Il Sole 24 Ore online e cartaceo si occupa di tecnologia d'avanguardia e sicurezza informatica.

Giovanni Galimberti

Avvocato con pluriennale esperienza in Diritto del lavoro. Esperto in materia di Privacy e Data Protection. Ha conseguito la certificazione CEPAS UNI 11697 come Responsabile Protezione Dati (DPO). In questi anni ha gestito casi di notifiche all'Autorità Garante per la protezione dei dati personali (GPDP).

Lorenzo Ruspi

Lead Auditor, Consulente e Formatore su diversi schemi di gestione con focus sulle tematiche inerenti alla sicurezza delle informazioni, alla protezione dei dati personali e alla continuità operativa. Ricopre il ruolo di DPO presso strutture sanitarie e socioassistenziali.

DURATA & MODALITÀ

15 ore totali

3 lezioni online da 3 ore in FAD sincrona e/o asincrona

3 lezioni online da 2 ore in FAD sincrona e/o asincrona

PROGRAMMA DELLE LEZIONI

Indice di lezioni e argomenti trattati

Modulo 1 | Dizionario della Cybersecurity e Informatico base

Docente: Giancarlo Calzetta

I **COS'È UNA RETE INFORMATICA E DA COSA È COMPOSTA**

II **COS'È UN REPARTO IT, COM'È COMPOSTO E COSA FA**

Come funziona la squadra che fa funzionare l'IT in un'azienda: dalle piccolissime con "un esperto" alle grandi con reparti strutturati.

II **L'AVVENTO DELL'INTELLIGENZA ARTIFICIALE**

Cos'è e cosa la fa funzionare.

IV **COME DISCUTERE CON UN IT "ALLA PARI"**

Introduzione sul concetto di collaborazione su più livelli e come mettere in chiaro le cose sui ruoli e sulle necessità.

V **COME FUNZIONA L'INFRASTRUTTURA IT NELLE AZIENDE**

- *La vera struttura aziendale dell'IT: la stratificazione, l'automazione etc.*
- *L'infrastruttura moderna è molto più complessa di quella "accademica" del secolo scorso.*

VI **LA SUPERFICIE D'ATTACCO: COS'È E COME SI IDENTIFICA**

Non si può proteggere ciò che non si conosce. Viaggio nel complicato mondo della prima difesa (che è destinata a fallire).

Modulo 2 | Cybersecurity: tipologie di attacchi informatici

Docente: Giancarlo Calzetta

I **ANALISI DELLE PRINCIPALI TECNICHE DI ATTACCO**

Virus - Botnets - DDoS - Spam - Phishing - Spear Phishing - MITM - DNS Poisoning - SS - Data Sniffing - Intrusion systems.

II **TECNICHE, TATTICHE E PROCEDURE UTILIZZATE NEGLI ATTACCHI DI SOCIAL ENGINEERING**

Smishing – Phishing – Scamming – Vishing – Deep Fake.

III **VULNERABILITÀ ZERO DAY**

La vera piaga della sicurezza informatica.

IV **GLI ATTACCHI SUPPLY CHAIN**

Quando l'attacco è invisibile e viene da un fornitore.

V **IL DISASTRO OPEN SOURCE**

Si crede che sia più sicuro, ma non lo è: da Log4J a github.

Modulo 3 | Il fattore umano nella Cybersicurezza

Docente: Giancarlo Calzetta

I **LA VECCHIA SCUSA DE "IL PROBLEMA È TRA LA SEDIA E IL MONITOR"**
L'essere umano non è il punto debole della catena, ma uno degli asset da proteggere senza aspettarsi di trasformarlo in un esperto di sicurezza.

II **COS'È IL SOCIAL ENGINEERING**
Moltissimi attacchi moderni hanno una componente di social engineering. Vediamo di cosa si tratta.

III **CREARE POLICY DI PROTEZIONE DELL'IDENTITÀ DIGITALE CHE SIANO EFFICACI**
Username e password non bastano più, bisogna andare oltre e comunque gestire bene quelle di cui non si può fare a meno.

IV **I SOCIAL NETWORK**
Utilizzo consapevole degli stessi. Focus sulla gestione dei dati.

V **INTERNET OF THINGS E IIOT**
Elementi di debolezza ed insicurezza degli oggetti connessi che oggi sono anche nelle fabbriche.

VI **DISTRUZIONE DEI DOCUMENTI E DEI SUPPORTI**
Cosa deve accadere quando cancelliamo un file o cambiamo i dispositivi elettronici.

VII **CLEAN DESK POLICY**
Il disordine è nemico della sicurezza.

VIII **PRINCIPI DELLA CYBER HYGENE**
Le regole della buona educazione nella sicurezza IT.

IX **ELEMENTI DI PSICOLOGIA DEGLI UTENTI E SULL'APPROCCIO USATO DAGLI ATTACCANTI**
Un buon criminale è anche un bravo psicologo.

X **PERCHÉ TUTTI I PUNTI DI CUI SOPRA NON SERVONO A NULLA**
Sono tutti indispensabili, ma la vera sicurezza è altrove.

Modulo 4 | Intelligenza Artificiale: norme, rischi e opportunità

Docenti: Giancarlo Calzetta
Alberto Guglielmi

I **INTELLIGENZA ARTIFICIALE**
Cos'è l'IA di cui tutti parlano e perché non ha niente a che fare con quello che ci aspettiamo.

II **COS'È L'IA GENERATIVA E A COSA SERVE**
Quali sono i suoi reali utilizzi e quanti tipi ne esistono.

III **DA DOVE ARRIVANO I RISCHI DELL'USO IN AZIENDA?**
L'IA generativa è un alleato potente in azienda, ma può esporre a gravi rischi i documenti e i dati su cui viene addestrata.

IV **DEEPFAKE AUDIO E VIDEO**
Uno degli utilizzi più pericolosi è quello dei deepfake e sono già in uso.

V **ADVERSARIAL**
Come può essere pericoloso fidarsi troppo dell'IA.

VI **GLI ERRORI DELL'IA**
Ci aspettiamo troppo dall'IA e bisogna organizzarsi per gestire bene i suoi errori.

VII **NORMATIVE**
L'IA passerà alla storia come la prima applicazione tecnologica che verrà normata prima di avere una vasta diffusione.

VIII **CYBERCRIMINE TRADIZIONALE ON STEROIDS**
Così come l'IA aumenta la produttività dei singoli, così aiuta i criminali: dal phishing alla scrittura di malware.

IX **MANIPOLAZIONE DI MERCATI FINANZIARI E ALTRI AMBIENTI SENSIBILI**
L'analisi tramite ML dei dati provenienti da ambiti sensibili può portare a scoprire pattern potenzialmente dannosi e sfruttabili da criminali.

X **IMPATTO DELL'IA SU PRIVACY, SORVEGLIANZA E SOCIETÀ**
- *Come l'IA può essere utilizzata per la raccolta e l'analisi di dati personali.*
- *I rischi per la privacy e la sorveglianza derivanti dall'uso dell'IA.*
- *Le normative e i principi etici per l'utilizzo responsabile dell'IA.*

XI **I BLACK ICE DI NEUROMANTE**
Per quanto siamo ancora lontani dalla presa di coscienza, ci sono operazioni che le IA compiono molto bene e una di queste potrebbe essere l'orchestrazione in tempo reale degli attacchi informatici.

Modulo 5 | Tecniche di Audit in tema di Sicurezza del dato e delle informazioni

Docenti: Matteo Colombo
Lorenzo Ruspi

I QUALI POLICIES, PROCEDURE, ISTRUZIONI E LINEE GUIDA OCCORRE IMPLEMANTARE PER "RAFFORZARE" LA PROPRIA GESTIONE DELLE INFORMAZIONI

È importante organizzare le proprie informazioni pensando per sistemi e costruire un impianto documentale solido per creare maggiore consapevolezza nelle organizzazioni sul tema della sicurezza delle informazioni.

II L'IMPORTANZA DI CONDURRE AUDIT SULLA SICUREZZA DELLE INFORMAZIONI CHE INCLUDONO ANCHE I DATI PERSONALI

Fare Audit periodici è considerato un valido strumento di accountability per ogni azienda per verificare l'efficacia delle procedure e delle policies che si è deciso di implementare oltre che per verificare in pratica le bontà delle misure tecniche e organizzative adottate.

III L'USO DELLE CHECKLIST COME VALIDO STRUMENTO PER LA CONDUZIONE DEGLI AUDIT

Sia in ambito sicurezza delle informazioni (ISO 27001) che in ambito Data Protection è importante costruire o usare delle "solide" checklist per verificare sul campo se l'impianto documentale impostato è applicato nella sostanza nei vari processi aziendali.

IV COME IMPOSTARE CORRETTAMENTE UN AUDIT

Coinvolgere i giusti interlocutori condividendo scopo e obiettivi di Audit e rendendo noti i criteri con i quali verranno valutate le evidenze raccolte durante l'attività svolta.

V COSA DEVE FARE IL DPO

Come, attraversato il proprio piano di attività, il DPO si confronta con tematiche cyber e focus point dedicate allo svolgimento del suo ruolo.

Modulo 6 | Incidente Informatico e violazione dei dati personali

Docente: Giovanni Galimberti

I CHECKLIST I.C.O

Come capire quando una violazione di dati presenti un rischio per le persone fisiche? Analisi di uno strumento utile per l'analisi della probabilità e della gravità di tale rischio.

II METODOLOGIE DI ANALISI

Panoramica delle metodologie di analisi di un data breach e best practice suggerite da diverse autorità europee.

III ANALISI DELLA GRAVITÀ

Come si valuta la gravità di un data breach? Spunti operativi per un approccio "scientifico" e dimostrabile nella gestione di un data breach a partire dell'applicazione della metodologia ENISA.

IV NOTIFICA ALL'AUTORITÀ GARANTE PRIVACY E COMUNICAZIONE AGLI INTERESSATI: SPUNTI OPERATIVI E CASI PRATICI

- *Come effettuare la notifica all'Autorità Garante Privacy: illustrazione della piattaforma per la notifica dei data breach.*
- *Comunicazione agli interessati: come rispettare gli obblighi del GDPR e i potenziali danni di immagine per il titolare del trattamento.*

V INDAGINE E CASE HISTORY SU UN DATA BREACH

Analisi di un caso concreto di data breach: ripercorriamo insieme i vari step dalla scoperta dell'incidente alla sua chiusura.

NOTE ORGANIZZATIVE

DATE

Modulo 1	17 giugno 2024	09.30 - 12.30
Modulo 2	24 giugno 2024	09.30 - 12.30
Modulo 3	01 luglio 2024	09.30 - 12.30
Modulo 4	08 luglio 2024	09.30 - 12.30
Modulo 5	12 settembre 2024	10.00 - 12.45
Modulo 6	19 settembre 2024	10.30 - 12.30

MODALITÀ

Il corso si svolge, in modalità live webinar, con accesso alla piattaforma **academelearning.ch** ed è fruibile in modalità sincrona e asincrona. Una volta effettuata la registrazione verrà chiesto di creare un account, che permetterà l'accesso alla dashboard di apprendimento e ad una sezione di interazione (Q&A).

MATERIALE DIDATTICO

Il partecipante potrà scaricare le slide del corso direttamente dalla piattaforma online a supporto dell'attività a distanza.

ATTESTATO DI PARTECIPAZIONE

Attestato di partecipazione rilasciato alla fine di ogni modulo.

TEST FINALE DI SUPERAMENTO CORSO

Ottieni un certificato di completamento quando termini il corso. A conclusione del percorso formativo **completo (15 ore)**, è previsto un test finale facoltativo di autoapprendimento erogato su piattaforma **academelearning.ch**, a seguito del quale si potrà scaricare il relativo attestato di superamento corso.

Per la frequenza e il conseguimento dell'attestato di superamento test non è richiesto un background specifico.

COSTI

Costo del corso : **790 €** + IVA

Costo del singolo modulo: **150 €** + IVA

Il corso è finanziabile con Fondi Interprofessionali.

PER ISCRIZIONI E INFORMAZIONI:

E-MAIL

formazione@laborproject.it

TELEFONO

+39 031 704381 (interno 1)

SITO

www.laborformazione.it

Labor Project®