Univa Servizi

Formazione Cybersecurity

Attività formativa finanziata sull'Avviso 1/2022 di Fondimpresa

Le caratteristiche dell'Avviso

L’**Avviso 01/2022** finanzia la formazione collegata a piani di innovazione di prodotto e di processo all’interno delle aziende.

01 Azione minimo **8 ore** max **100 ore**

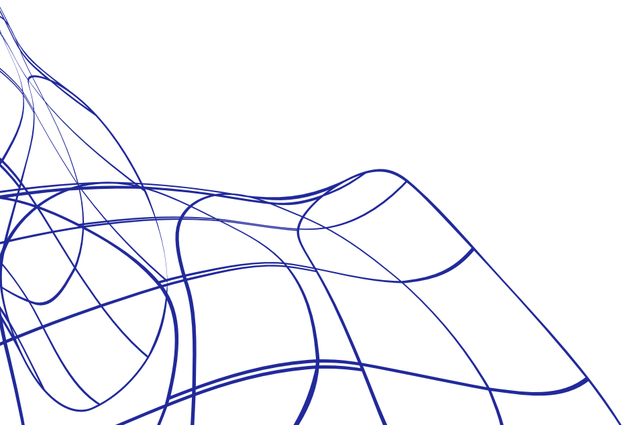
02 Ogni lavoratore max **100 ore**

03 Minimo **15** dipendenti coinvolti

04 **Verifica dell'apprendimento** obbligatoria

05 In ogni aula max **20** persone

06 Coinvolgimento di un’**Università** come partner del soggetto proponente



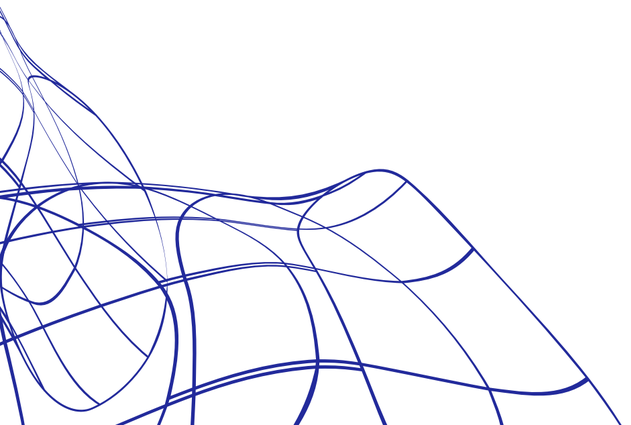
L'impegno delle aziende

- Per partecipare al piano l’azienda deve avere un **reale progetto di innovazione** per la quale la formazione – finanziata da Fondimpresa – è necessaria alla realizzazione.
- In fase di presentazione, dev’essere indicato il **team imprenditoriale** che ha il compito di sovraintendere al progetto.
- È chiamata a **compartecipare alla progettazione** e compilazione del formulario, illustrando gli aspetti principali del progetto di innovazione e le caratteristiche dell’azienda.

L’impegno di Univa Servizi

- **Univa Servizi** ha sviluppato una progettualità formativa sul tema della **cybersecurity**, con una proposta di corsi che risponde a tutte le esigenze dell’azienda ed è **completamente finanziabile** da Fondimpresa.
- **Univa Servizi** è **soggetto presentatore** e **gestore del piano** e si occupa dei rapporti con il Fondo, con l’**Università**, con i **sindacati** e del **rispetto dei requisiti** previsti dall’Avviso.

L’iter per la partecipazione al bando



Step 1 La scelta dell'impianto didattico

L’azienda sceglie all’interno della proposta formativa di Univa Servizi i corsi a cui interessata indicando anche il numero di edizioni che vuole realizzare. È possibile comunque chiedere l’introduzione di nuovi corsi specifici, ma sempre riguardanti il tema cybersecurity.

Step 2 La compilazione del questionario

L’impresa dovrà rispondere al questionario inviato da Univa Servizi e che riguarderà:

- soluzione di cybersecurity che l’azienda vorrà attivare (contenuto, tecnologie, valore degli investimenti, proprietà intellettuale)
- mercato di riferimento rispetto alla soluzione (analisi del valore, inquadramento del mercato, analisi competitiva)
- Team imprenditoriale (CV, ruolo in azienda, ruolo sul piano)

Step 3 Gli aspetti amministrativi

L’impresa dovrà infine firmare la dichiarazione di adesione al piano.

La proposta di Univa Servizi

Formazione sulla cybersecurity per tutti gli utenti aziendali

Cybersecurity Awareness

Formazione per tutta la popolazione aziendale sul tema della Cybersecurity in azienda

Cybersecurity & Privacy

Formazione per i responsabili privacy delle aziende (DPO) sul tema della cybersecurity nella protezione dei dati

Cybersecurity & Quality: approccio alla ISO 27001

Formazione per gli addetti alla qualità per iniziare il percorso verso la ISO 27001.

Cybersecurity & Industry 4.0

Formazione per gli addetti IT per quanto riguarda una strategia informatica di Cybersecurity

Cybersecurity Awareness

Cybersecurity Awareness

Formazione per tutta la popolazione aziendale sul tema della Cybersecurity in azienda

Obiettivo

Informare sui rischi potenziali insiti nell'uso di strumenti informatici, fornendo elementi per l'identificazione e il trattamento delle più rilevanti problematiche in ambito di cybersecurity e social engineering, per identificare rischi e minacce, nonché determinare le più adeguate contromisure da mettere in atto.

Destinatari

Tutta la popolazione aziendale

Argomenti trattati

- Concetti base di sicurezza
- Pirateria informatica
- La figura dell'Hacker
- Contraffazione del Software
- Internet security
- Malware, Ransomware, Downloader, Backdoor
- Social Engineering e Phishing
- Uso dei social network
- Controllo e prevenzione
- Dispositivi Mobili e smart working

Durata

8 ore

Cybersecurity & Privacy

Cybersecurity & Privacy

Formazione per i responsabili privacy delle aziende (DPO) sul tema della cybersecurity nella protezione dei dati

Obiettivo

Indicare il sistema di gestione più idoneo per la protezione dei dati e per gli adempimenti richiesti in materia di privacy tramite policy, regolamenti e modalità di applicazione del Regolamento Europeo UE 2016/679 del codice privacy italiano.

Destinatari

Responsabili della protezione dei dati in azienda (DPO) e IT manager

Argomenti trattati

- I punti rilevanti del testo della normativa per la protezione dei dati personali e sulla privacy
- Adempimenti e regole del trattamento
- Policy, modelli e regolamenti
- Misure minime di sicurezza informatica
- Gestione dei comportamenti a rischio
- Utilizzo idoneo di videosorveglianza, localizzazione e strumenti informatici

Durata

8 ore

Cybersecurity & Quality: approccio alla ISO 27001

Cybersecurity & Quality: approccio alla ISO 27001

Formazione per gli addetti alla qualità per iniziare il percorso verso la ISO 27001

Obiettivo

Comprendere il processo di implementazione di un Sistema di Gestione per la sicurezza delle informazioni, conforme ai requisiti della norma, in ottica di certificazione o come linea di indirizzo per una corretta ed efficiente conduzione della sicurezza delle informazioni aziendali

Destinatari

Responsabili della qualità in azienda e IT manager

Argomenti trattati

- Information security risk management e approccio per processi
- I requisiti della ISO/IEC 27001
- Elementi di valutazione (identificazione, analisi, stima, ponderazione)
- Trattamento dei rischi
- Controlli di sicurezza proposti dall’Annex A (ISO/IEC 27001 e 27002)
- Ambiti applicativi all’interno dell'azienda

Durata

16 ore

Cybersecurity & Industry 4.0

Cybersecurity & Industry 4.0

Formazione per gli addetti IT per quanto riguarda una strategia informatica di Cybersecurity

Obiettivo

Capire se e quando un sistema informatico basato su Industry 4.0 è più o meno sicuro, comprenderne le minacce e le vulnerabilità per proteggere l'azienda da attacchi e perdite di dati che potrebbero compromettere la continuità produttiva e gestionale.

Destinatari

CTO e IT manager

Argomenti trattati

- Identificazione dei rischi informatici in fase di progettazione
- Security level assessment e gap analysis di un impianto o una macchina di produzione
- Security assessment e piani di continuità
- Disaster recovery
- Sviluppare e implementare correttamente i piani di risposta agli incidenti di sicurezza

Durata

16 ore