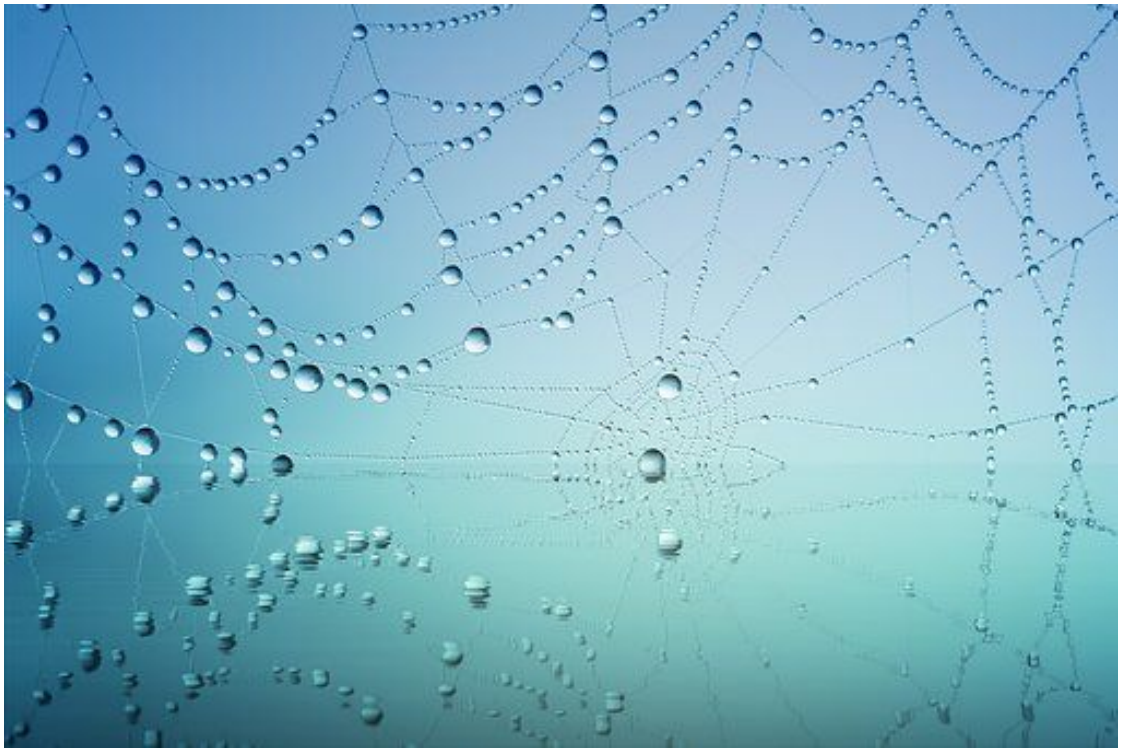
obinlab
obiettivoinnovazione

La sicurezza nelle mani degli utenti



Per dare alle persone il livello di conoscenza necessario per muoversi nella giungla delle applicazioni e delle connessioni diffuse, in modo prudente e consapevole, per proteggere il patrimonio informativo aziendale e personale.

www.obinlab.it/home/i-percorsi-formativi

Corso: La sicurezza nelle mani degli utenti

Perché serve questo corso

La sicurezza informatica in azienda è garantita con soluzioni tecniche, strumenti informatici, protezioni perimetrali ed interne. Ma ha un grande punto debole ormai riconosciuto a livello mondiale: l'utente! L'utente è il principale attore nelle questioni relative alla sicurezza dei dati aziendali e delle infrastrutture tecnologiche.

E' quindi necessario fare in modo che la consapevolezza dei rischi e la conoscenza delle precauzioni facciano parte del bagaglio culturale e pratico di ogni persona che opera in azienda e per l'azienda.

L'utilizzo di dispositivi mobili sempre più diffuso, gli strumenti di collaborazione, lo smart working che prende piede, e molte altre situazioni nuove creano vulnerabilità molto spesso sconosciute o impensabili.

Il corso mira a dare agli 'utenti' il livello di conoscenza necessario per muoversi, nella giungla delle applicazioni e delle connessioni diffuse, in modo prudente e consapevole. Lo scopo finale è incrementare la protezione del patrimonio informativo aziendale e personale.

Argomenti affrontati

- Le infrastrutture e gli strumenti utilizzati
- L'ambiente operativo ed informativo dell'azienda
- Le diverse organizzazioni del lavoro
- La situazione del cybercrime e degli attacchi informatici
- I rischi per l'azienda e per le persone
- Le principali vulnerabilità
- Le contromisure adottabili e le buone prassi
- Normative, obblighi, sanzioni e regolamenti interni
- Conclusioni

Organizzazione del corso

Il corso ha una durata pari a 3,5 - 4 ore.

Può essere svolto in aula, con un massimo di 20 partecipanti, o in videoconferenza con un massimo di 4 sedi remote collegate.

Nella fase di preparazione del corso si organizza un incontro con il personale che in azienda svolge funzioni di direzione e gestione della sicurezza informatica. L'incontro ha lo scopo di raccogliere il quadro dei sistemi usati, delle soluzioni di sicurezza adottate, dei principali rischi percepiti e di eventuali normative interne predisposte.

Sviluppo degli argomenti

Le infrastrutture e gli strumenti utilizzati

- Panoramica sugli strumenti oggi utilizzati e sulle connessioni tra loro
- Come funzionano le applicazioni e gli accessi nelle reti locali
- Come funzionano le applicazioni e gli accessi negli ambienti cloud e misti
- Dispositivi mobili, App e dati trasmessi

L'ambiente operativo ed informativo dell'azienda

- Sistemi in uso presso l'azienda
- Il disegno della rete in azienda
- Tipologie di attività svolta
- Scelte e soluzioni di sicurezza adottate

Le diverse organizzazioni del lavoro

- Classica e Ibrida
- Smart working
- Interazioni privato-professionale

La situazione del cybercrime e degli attacchi informatici

- Attacchi informatici: quadro delle tipologie
- Principali modalità usate
- Il phishing moderno e l'ingegneria sociale

I rischi dell'azienda e delle persone

- Perdite economiche dirette e indirette
- Danni reputazionali
- Danni a dispositivi e disservizi

Le principali vulnerabilità

- Punti critici dei sistemi
- Zone non protette
- Identità digitali e loro utilizzo
- Comportamenti umani

Le contromisure adottabili e le buone prassi

- La competenza dei gestori della sicurezza
- Consapevolezza e conoscenza
- Comportamenti
- Strumenti
- Interazioni tra funzioni

Normative, obblighi, sanzioni e regolamenti interni

- Privacy e protezione dei dati - GDPR
- Normativa interna aziendale

Verifiche e conclusioni

- Questionario di valutazione rapida
- Focalizzazione sugli aspetti critici
- Prossimi passi