

# Transizione digitale e la sicurezza informatica

Proposta formativa per laboratorio sul campo

Durata: 8 ore due incontri da 4 ore

Destinatari: Personale tutto

## Primo Incontro

### Introduzione alla Transizione Digitale e Sicurezza Informatica

Concetti chiave della transizione digitale: definizioni, obiettivi e impatti sulle organizzazioni.

Panoramica sulla sicurezza informatica: principi fondamentali e importanza nella trasformazione digitale.

Normative e regolamenti: overview delle leggi e linee guida pertinenti, come il GDPR.

### Infrastrutture Digitali e Sicurezza delle Reti

Modernizzazione delle infrastrutture IT: cloud computing, virtualizzazione e loro implicazioni sulla sicurezza.

Sicurezza delle reti: protezione delle reti aziendali, firewall, VPN e segmentazione della rete.

Gestione delle vulnerabilità: identificazione, valutazione e mitigazione dei rischi.

### Protezione dei Dati e Privacy

Data governance: strategie per la gestione e protezione dei dati durante la transizione digitale.

Crittografia e controllo degli accessi: tecniche per garantire la riservatezza e l'integrità dei dati.

Privacy by design: integrazione della protezione dei dati nei processi e nei sistemi.

## Secondo Incontro

### Applicazioni e Servizi Digitali Sicuri

Sviluppo sicuro del software: pratiche di coding sicuro e gestione delle vulnerabilità applicative.

Sicurezza dei servizi cloud: valutazione e gestione dei rischi associati ai servizi cloud.

DevSecOps: integrazione della sicurezza nel ciclo di vita dello sviluppo software.

### Gestione degli Incidenti e Continuità Operativa

Piani di risposta agli incidenti: preparazione, rilevamento e risposta agli incidenti di sicurezza.

Disaster recovery e business continuity: strategie per garantire la continuità operativa.

Simulazioni pratiche: esercitazioni su scenari di incidenti informatici.

### Cultura della Sicurezza e Formazione Continua

Consapevolezza e formazione del personale: programmi di sensibilizzazione alla sicurezza informatica.

Ruolo del Responsabile per la Transizione Digitale (RTD): compiti e responsabilità nella sicurezza informatica.

Aggiornamento continuo: importanza della formazione continua e dell'adeguamento alle nuove minacce.