# SMAW-22 - DIGITAL TRANSFORMATION IN AZIENDA

Categoria: **Smart Working**

## INFORMAZIONI SUL CORSO

| Durata: | Categoria: | Qualifica Istruttore: | Dedicato a: | Produttore: |
|---|---|---|---|---|
| 5 Giorni | Smart Working | Docente Senior (min. 5 anni) | Utente Esperto | PCSNET |

## OBIETTIVI

Smart Working e Remote Working sono le nuove frontiere della collaborazione tra le risorse aziendali. Affinché questi strumenti possano essere integrati con efficacia nelle organizzazioni, è necessario sviluppare competenze che consentano di poter essere produttivi anche al di fuori dell'ufficio, attraverso il corretto uso degli strumenti di supporto alla collaborazione aziendale quali: chat, conference call, piattaforme cloud per la creazione e la condivisione dei documenti di lavoro, …
Obiettivo del corso è fornire ai partecipanti una visione complessiva sull'importanza dell'adozione delle piattaforme di social collaboration e sulle principali soluzioni presenti sul mercato, le competenze necessarie per la corretta gestione delle attività di smart working e remote working e le competenze tecniche di base per l'utilizzo delle piattaforme di collaborazione aziendale, in particolare l'uso delle piatteforme OneDrive e Google Drive.

## PREREQUISITI

Nessun prerequisito.

## CONTENUTI

**Modulo 1 - Social Collaboration, Smart Working e Remote Working**

- -Smart Working e Remote Working: i vantaggi per le aziende e per i dipendenti.
- -Casi aziendali di successo nell'applicazione della social collaboration.
- -Come creare un modello di collaborazione digitale.
- -Le piattaforme di social software a supporto del lavoratore remoto.
- -Microsoft OneDrive e Google Drive come strumenti di social collaboration.

**Modulo 2 - Introduzione all'utilizzo di uno spazio "cloud": Microsoft OneDrive e Google Docs**

- -Caricamento, organizzazione, visualizzazione file.
- -Ricerca di file e documenti.
- -Funzionalità di condivisione.
- -Gestione documenti e versioning.
- -Recupero di un file dal cestino.
- -Versione mobile / App.

**Modulo 3 - Analizzare i dati con Excel**

-Usare gli elementi di analisi statistica in Excel.
-Gestire le fonti dati e le tabelle relazionate.
-Collegare tra di loro tabelle diverse e ricavarne le informazioni funzionali al tuo lavoro.
-Gestite Tabelle Pivot per generare un rapporto di analisi dinamico e PowerPivot per l'analisi cubica su multiple fonti di dati.
-Logica Database: concetti di modellazione delle tabelle in stile DB per finalizzare i dati all'analisi.
-Relazioni: possibilità di creare direttamente all'interno della cartella di lavoro correlazioni fra due tabelle.
-Tabella Pivot avanzata: analisi approfondita dell'uso e delle meccaniche della Tabella Pivot.
-Tabelle PowerPivot con Excel 2016 e Office 365: Tabella Pivot applicata all'analisi cubica su multiple fonti di dati.
-Connessioni ODBC: creazione di relazioni dirette tra tabelle usando il linguaggio SQL di Microsoft.
-Importazioni dati: gestione dell'importazione dati da CSV, Access e server SQL.
-Dashboard: creazione ed ideazione di un pannello di controllo finalizzato all'analisi dei dati.

**Modulo 4 - Alla scoperta di Prezi, il sistema di presentazione rivoluzionario progettato sui principi delle neuroscienze che sta reinventando l'arte della presentazione**

-Cosa dice la scienza riguardo all'essere persuasivi, coinvolgenti e all'arte di farsi ricordare.
-L'impostazione del racconto.
-L'area di lavoro di Prezi, i menu, la barra laterale e gli strumenti.
-I template di Prezi … per facilitare i primi passi o per chi ha fretta.
-Come sfruttare il concetto di zooming: dalla Big Picture ai minimi dettagli senza soluzione di continuità.
-Metafore e immagini.
-Le inquadrature dinamiche.
-Inserimento di testi, immagini e filmati.
-Trasformazioni e rotazioni.
-Percorsi non-lineari, bottoni zoom e home.
-Come esportare il mio lavoro in un Prezi portatile e in .pdf.

**Modulo 5 - Cyber Security Awareness**

-I dati del crimine informatico nell'Italia e nel mondo: il rapporto CLUSIT.
-Cyberwarfare, la guerra cibernetica: casi famosi.
-Deep Web, Dark Web e Bitcoin: cosa sono e perché ci riguardano.
-I problemi ed i rischi nelle aziende e negli studi professionali.
-I danni economici generati alle aziende.
-Cos'è il Social Engineering.
-La crescita esponenziale del phishing e lo Spear phishing: le tecniche d'attacco.
-I Ransomware: come attaccano e come proteggersi.
-Sono stato colpito da un Ransomware: cosa fare ora?
-Ransomware: aspetti giuridici (è reato pagare il riscatto?) e disciplinari (a carico del dipendente).
-La tecnica BEC (Business Email Compromise): le truffe "The Man in the Mail" e "CEO fraud".
-Lo spoofing.
-Come usare l'email in modo sicuro.
-La PEC e la posta crittografata.
-I Social Network come mezzo di attacco sempre più usato.
-Gli Spyware negli smartphone.
-La prevenzione del mobile malware: una corretta policy aziendale.
-Messaggistica istantanea: WhatsApp, Telegram, iMessage. Ci possiamo fidare?
-Gli strumenti (sempre più potenti) degli hackers: alcuni famosi casi di attacchi e "data breach".
-Le regole per una Password sicura e gli errori comuni da evitare.

-Le “domande di (in)sicurezza”.
-I Password Manager.
-L’autenticazione a due fattori: una protezione ulteriore.
-Una corretta policy di Backup.
-I rischi dell’utente interno.

## INFO

**Materiale didattico:** Materiale didattico e relativo prezzo da concordare
**Costo materiale didattico:** NON incluso nel prezzo del corso
**Natura del corso:** Operativo (previsti lab su PC)