SISTEMA DI MONITORAGGIO VALUTATIVO

AT : BASILICATA

Azienda : PUBLISYS S.P.A.

Ambito tematico strategico: Innovazione tecnologica di processo e di prodotto

Titolo : CARONTE

Codice identificativo del piano: 220392

A cura di : Marcello Faggella

Rapporto realizzato nel mese di Novembre 2021

INDICE

1.Introduzione

Publisys spa è una società con sede a Potenza fondata nel 1982 specializzata nella produzione di software applicativo, nell'erogazione di servizi di assistenza e consulenza per la PA e nella realizzazione di progetti complessi di System Integration.

Da sempre attenta alla formazione aziendale e ad ogni progresso tecnologico, negli anni è stata in grado di misurarsi con importanti sfide che le hanno permesso, oggi, di rappresentare una delle eccellenze del territorio della Basilicata in grado di affrontare i cambiamenti tecnologici e normativi del Paese.

2. Strategie aziendali e ruolo della formazione continua

2.1 Breve profilo dell'azienda e del settore

Nel 1982, i Fratelli Rossi a seguito di esperienze acquisite nel campo dell'informatica fondano la System House Rossi Computer.

Gli anni tra 1985 e il 1991 sono decisivi per l'azienda particolarmente impegnata nella realizzazione e progettazione di sistemi informatici per la Pubblica Amministrazione.

Nel 1992 il nuovo corso intrapreso e le competenze acquisite portano all'evoluzione della Rossi Computer nell'attuale Publisys spa che nel 1994 sviluppa la prima versione della suite integrata dedicata agli enti locale URBE.

Nel 1998 le attività si diversificano ampliando i servizi offerti anche all'ambito della sanità pubblica.

Il 2004 è un anno importante per l'azienda in quanto viene sviluppata la nuova release del software URBE che implementa tecnologie web di ultima generazione.

Nel 2005 Publisys inizia ad operare nell'ambito degli enti regionali sviluppando servizi digitali e soluzioni di e-government.

Nel 2006 l'azienda entra far parte del consorzio CreaTec : inizia così la partecipazione a importanti progetti di ricerca nazionali.

Dal 2010 al 2018 l'azienda rafforza notevolmente la sua presenza nel centro sud Italia aprendo una sede a Salerno e un'altra in provincia di Benevento guadagnando una posizione leader nel mercato della PA locale che mantiene ancora oggi.

Per quanto riguarda il settore, come riportato nel recente rapporto Anitec-Assinform, negli ultimi anni, si è assistito a una progressiva crescita del mercato digitale nel paese, che di anno in anno ha contribuito a trasformare l'industria manifatturiera e quella dei servizi, il commercio, la pubblica amministrazione e – più in generale – la società. Nel 2020 il mercato valeva oltre 71,5 miliardi di euro, con una performance migliore rispetto all'economia nel suo complesso, confermando il trend già osservato negli anni precedenti, che mostra come l'incidenza del mercato digitale sul PIL nel triennio 2017-2020 sia passata dal 4,0% al 4,3%.

Sono numeri incoraggianti, se pensiamo che il 2020 è stato un anno del tutto eccezionale. Un anno che per le trasformazioni e gli impatti sulle persone e sulle imprese ha condensato in 12 mesi cambiamenti che avvengono normalmente in almeno 5 anni.

Per quanto riguarda i comparti tecnologici si è registrata una diminuzione delle componenti più tradizionali del mercato, come i servizi di rete (-6,4%, 19.391 milioni di euro), che hanno registrato una continua riduzione dell'ARPU (Average Revenue Per User), e la componente software (-2,3%, 7.517 milioni di euro), che subisce l'impatto negativo della sospensione delle attività di molte aziende, in particolare PMI. In controtendenza la spesa in dispositivi e sistemi (+1,3%, 19.368 milioni di euro), che ha beneficiato della crescita della domanda di PC e dispositivi mobili associata alla diffusione del lavoro da remoto, e il mercato dei servizi ICT (+3,3%, 12.702 milioni di euro), trainato dalla necessità di garantire il funzionamento di sistemi e applicazioni. Con segno più anche il segmento dei contenuti digitali (+3,6%, 12.526 milioni di euro), che ha beneficiato della crescita del video on demand.

Trasversali tra i vari comparti, i Digital Enabler sono le tecnologie più innovative e quelle caratterizzate da un dinamismo più marcato. Tra quelle con volumi d'affari maggiore si segnalano: Mobile Business (+4,4%, 4.326 milioni di euro) e Cloud (+20,4%, 3.408 milioni di euro). Nell'insieme i Digital Enabler sono cresciuti del 7,1%.

Il mercato digitale nel 2020 ha avuto dinamiche differenziate e talora opposte nei diversi settori. Quelli più colpiti dalla crisi economica, Travel & Transportation (-5,7%, 2.360,6 milioni di euro) e Distribuzione e Servizi (-5,6%, 4.301 milioni di euro) hanno registrato i cali più consistenti. Nel settore industriale le dinamiche sono state eterogenee, ma i dati complessivi di spesa hanno evidenziato un calo (-4,8%, 7.909,1 milioni di euro). Per altri settori gli effetti della crisi sanitaria si sono tradotti, invece, in un'accelerazione degli investimenti in ICT, come ad esempio

nella Pubblica Amministrazione Centrale (+5,2%, 2.060 milioni di euro).

Il 2020 ha accentuato il divario ancora esistente nell'adozione delle tecnologie digitali tra le aziende di medie e piccole dimensioni e le grandi organizzazioni. La spesa in digitale sostenuta dalle grandi aziende (+250 addetti) ha registrato una crescita (+1,2%, 24.998,8 milioni di euro), quella delle medie imprese (50-249 addetti) un calo (-2,4%, 7.666 milioni di euro), diminuzione ancora più marcata nelle piccole imprese (1-49 addetti, -5%, 8.847,4 milioni di euro).

Le previsioni di crescita del mercato digitale nei prossimi anni sono fortemente condizionate dall'attuazione del PNRR. Quattro gli scenari ipotizzati:

Primo scenario: una stima dell'evoluzione del mercato digitale senza alcun impatto dovuto al PNRR (crescita organica o scenario base): +3,5% (2021), +3,7% (2022), +4,1% (2023), +4% (2024).

Secondo scenario: utilizzo del 100% dell'allocazione annuale dei fondi previsti dal PNRR (profilo alto): 8,5% (2021), 8,2% (2022), 6,8% (2023), 5,1% (2024).

Terzo scenario: utilizzo del 70% dell'allocazione annuale dei fondi previsti dal PNRR (profilo medio): 7% (2021), 6,9% (2022), 6,1% (2023), 4,8% (2024).

Quarto scenario: utilizzo del 50% dell'allocazione annuale dei fondi previsti dal PNRR (profilo basso): 6% (2021), 6% (2022), 5,5% (2023), 4,6% (2024).

2.2 Orientamenti strategici e processi di innovazione

La mission dell'azienda è oggi quella di sviluppare e fornire soluzioni e servizi di Information & Comunication Technology rivolti alla Pubblica Amministrazione attraverso attività di ricerca, di consulenza e in outsourcing.

L'azienda è costantemente impegnata nella ricerca delle più recenti tecnologie e metodologie al fine di offrire servizi all'avanguardia per i suoi clienti.

In linea con questo principio investe costantemente risorse finanziarie in hardware, software e in formazione dei dipendenti affinché le competenze del suo team siano allineate con i più alti standard sul mercato.

In questa ottica l'azienda sta puntando sempre più a sviluppare un percorso di trasformazione digitale basata sull'automazione e customer centric dei suoi clienti nella direzione indicata dal piano 4.0 e sulla convergenza dei sistemi informativi tecnici, organizzativi ed amministrativi e sulla messa in rete delle attrezzature. I processi di innovazione in atto puntano sempre più a sviluppare la capacità di analisi ed interpretazione dei dati e di costruzione di una reportistica funzionale alla gestione dei rischi individuando le opportunità di sviluppo e migliorando la penetrazione nel proprio segmento di mercato ampliando la gamma di prodotti e delle soluzioni proposte ai clienti, diversificando il business in modo correlato alle capability presenti e ai fabbisogni dei clienti. Alla luce della sempre più crescente migrazione dei dati da posizioni in locale a posizioni in cloud remoto particolare attenzione viene sempre più dedicata a tutto quanto ruota intorno alla sicurezza informatica delle reti e al riconoscimento degli utenti che effettuano gli accessi ai dati.

2.3 Obiettivi aziendali e ruolo della formazione

La decisione di realizzare il piano e le attività formative in esame è strettamente correlata agli obiettivi strategici dell'azienda.

Publisys utilizza costantemente la formazione per garantire ai propri clienti servizi di qualità e mantenere dunque il proprio posizionamento di mercato. E'per questo che nel corso dell'anno organizza vari percorsi di formazione sia di carattere tecnico/specialistico sia di carattere manageriale. In relazione alle ricadute sulle performance aziendali il management di Publisys si poneva due obiettivi: da un lato acquisire maggiore consapevolezza sulla normativa legata alle nuove regole europee sulla privacy e dall'altro strutturare procedure informatiche aggiornate per prevenire ogni possibile accesso non consentito ai dati trattati.

Le nuove regole europee sulla privacy sono divenute operative il 25 maggio. I cambiamenti imposti dal GDPR rappresentano in questa fase un grande impegno per le imprese come Publisys che operano nel campo della progettazione e realizzazione di sistemi informatici per la Pubblica Amministrazione. Proprio secondo quanto previsto dalla normativa, l'organizzazione dovrà prestare maggiore attenzione alla creazione dell'informazione digitale per far sì che vi sia protezione dei dati fin dalla sua creazione e progettazione ("*Data Protection by Design and by Default*").

Per non perdere mercato con le PA e non incorrere in sanzioni di grave entità, l'azienda aveva la necessità di formare il proprio personale affinchè fosse in grado di attuare strumenti tecnici e organizzativi per soddisfare i requisiti previsti dal nuovo regolamento UE sulla privacy.

In aggiunta era necessario che il personale fosse in grado di definire, in via preventiva, gli elementi aziendali maggiormente sensibili ai cyber attacchi così da proteggere in modo efficace l'intero ecosistema aziendale nelle aree di interazione con terze parti. L'azienda ha pertanto effettuato un'analisi preventiva volta sia a ridefinire gli ambiti e le attività sui cui assicurare un livello di protezione adeguato, sia a stabilire i reali punti di debolezza su cui intervenire. Una maggiore e totale consapevolezza nei confronti della cybersecurity diventa un imperativo se devono essere protetti anche i clienti e i dipendenti aziendali (privacy e tutela dei dati sensibili). Inoltre, la protezione preventiva della rete da compromissioni risulta meno costosa delle misure adottate a seguito del verificarsi di un incidente in termini di ripercussioni finanziarie e legali, danni alla reputazione, sanzioni amministrative e costi per ripristinare le violazioni.

2.4 La formazione nel periodo di emergenza sanitaria da Covid-19 e per il prossimo futuro

Durante il periodo dell'emergenza sanitaria non sono state svolte attività di formazione ma la definizione di nuovi fabbisogni è stata in costante sviluppo.

2.5 Considerazioni riepilogative

La Publisys rappresenta un'eccellenza nel panorama aziendale lucano per la velocità con la quale è diventata una tra le imprese leader nel settore ICT. La mission di Publisys è quella di erogare

servizi di information & communication technology attraverso la realizzazione di progetti di system e business integration, di attività di outsourcing e consulenza tecnologica. Conoscenze specialistiche, alta competenza, eccellenza dei servizi offerti, una struttura interna flessibile e capillare sono il potenziale competitivo di Publisys, chiamato ad operare su mercati tecnologicamente avanzati ed in costante evoluzione. La Pubblica Amministrazione Locale rappresenta il mercato "core" di Publisys, che interviene sull'organizzazione e le architetture informatiche aziendali per orientarne il cambiamento. Data la criticità e sensibilità dei dati gestiti dai clienti della Publisys e in considerazione degli aggiornamenti normativi, si è reso necessario costruire un percorso formativo che andasse a rafforzare le competenze in tema di cyber sicurezza così da strutturare procedure in grado di prevenire, per quanto possibile, eventuali violazioni dei sistemi informatici.

3.Il Piano formativo

3.1 L'analisi del fabbisogno, metodologie e risultati

L'analisi del fabbisogno è stata realizzata attraverso un confronto tra i referenti aziendali, i destinatari della formazione e i consulenti esterni incaricati di gestire il percorso formativo.
Attraverso interviste ai lavoratori e ai responsabili aziendali sono state individuati gli obiettivi che si intendeva raggiungere, le criticità da superare, i ruoli professionali da coinvolgere.
Con il supporto dell'ente di formazione si sono pertanto definiti i gap di competenza di tipo tecnico e normativo e inquadrati gli aspetti da attenzionare.

Successivamente sono stati raccolti dati e informazioni significativi relativamente al contesto organizzativo aziendale ed alle aspettative connesse agli interventi e azioni prescelte. L'obiettivo di questa linea di attività era dunque quello di raccogliere le esigenze di nuove professionalità e formazione espresse dall'azienda e di mettere a sistema l'insieme delle informazioni così da costruire un'offerta adeguata.

Naturalmente l'analisi del fabbisogno è stata strettamente collegata alle scelte strategiche d'impresa, all'impatto delle tecnologie sul business e alle scelte organizzative aziendali.

Sono state pertanto individuate le figure professionali che operano nelle differenti aree e le competenze necessarie a garantire il raggiungimento degli obiettivi.

In sintesi si è effettuata:

- l'analisi del contesto;
- la rilevazione delle criticità organizzative e produttive aziendali, delle figure/posizioni critiche e dei bisogni formativi correlati;
- Il raffronto tra bisogni formativi percepiti, attraverso l'analisi della domanda e i bisogni rilevati a livello individuale;
- l'incrocio tra fabbisogni formativi rilevati e offerta formativa;
- l'analisi delle competenze in ingresso in fase di orientamento;
- l'individuazione delle competenze critiche o emergenti.

3.2 Il processo formativo, dalla progettazione alla valutazione degli esiti

Dall'analisi della documentazione e dalle interviste effettuate è emerso in modo chiaro che ogni fase dell'attività formativa è stata approfondita adeguatamente.

Per quanto riguarda le metodologie didattiche la formazione è stata effettuata in aula per trasmettere contenuti teorici, alternandola alla modalità di training on the job.

Individuare i docenti è stata sicuramente la fase più complicata poiché skills di questo tipo non sono comuni: ne consegue che anche le tariffe orarie dei docenti sono piuttosto elevate e non trovano riscontro nei massimali previsti dagli avvisi di sistema.

In base agli obiettivi strategici individuati sono state fornite indicazioni e suggerimenti relativi all'orientamento pratico delle docenze ed all'utilizzo di metodi didattici di tipo applicativo.

Il management aziendale ha monitorato, con il supporto dell'ente di formazione, tutta l'attività formativa, acquisendo di volta in volta feedback al termine di ogni incontro al fine di far emergere ulteriori esigenze di formazione ed approfondimento.

Dalle interviste realizzate è emerso che gli allievi hanno generalmente apprezzato le attività formative cui hanno partecipato.

3.3 Considerazioni riepilogative

La rilevanza della proprietà intellettuale e del conseguente vantaggio competitivo vale anche per il settore IT, che si attesta come il secondo comparto più colpito da attacchi a livello globale. Perseguendo una sempre più elevata innovazione, una

collaborazione più aperta ed una maggiore competitività, questo settore, infatti, espone intrinsecamente l'infrastruttura alla vulnerabilità e una mancata integrazione della cyber security nella cultura organizzativa e nei processi aziendali incide negativamente sulla produttività e sulla redditività aziendale.
Risulta pertanto necessario sviluppare un percorso di continua formazione aziendale che mantenga sempre ai massimi livelli le procedure e le policy da adottare in azienda.
Il processo formativo è stato gestito in modo ottimale: dalla definizione dei fabbisogni alla individuazione dei destinatari, alla erogazione fino alla valutazione dei risultati.

Da evidenziare sicuramente la fase di erogazione che essendo stata sviluppata in parte in aula e in parte *on the job* ha riscosso molto successo tra i partecipanti che hanno sottolineato l'utilità di avere un docente di elevata competenza nel settore.

4.L'impatto della formazione

4.1 L'impatto della formazione

L'impatto della formazione è stato decisamente rilevante.
In primo luogo, la formazione ha avuto il merito di sensibilizzare le risorse umane sul tema della sicurezza informatica, ponendo attenzione in particolare alla tutela dei dati sensibili trattati. Grazie alla formazione, sono stati forniti contenuti adeguati sui rischi che ogni utente corre relativamente alla sicurezza delle informazioni su supporti informatici e grazie ad esempi pratici sono state acquisite le modalità ottimali da adottare per garantirne l'inviolabilità.

Violazioni di dati, malware, ransomware, phishing, DDoS, social engineering, sono in cima alle preoccupazioni di qualsiasi società che si occupi di gestione di dati sensibili come la Publisys. Per contrastare le minacce però, le sole soluzioni tecnologiche non bastano ed è solo con un efficace programma di formazione che è possibile integrare risorse aziendali (e quindi competenze), processi e tecnologia così da essere in grado di rispondere ai diversi tipi di minacce.
I lavoratori, a seguito dell'azione formativa hanno acquisito un'approfondita competenza giuridica sull'argomento e la capacità di coordinamento e verifica di attività che comportano il rischio di divulgare dati che potenzialmente possono nuocere materialmente o moralmente ai soggetti interessati.

I lavoratori intervistati hanno dichiarato che a seguito dell'intervento formativo sono state colmate le lacune sulla nuova direttiva privacy e sugli strumenti da porre in essere a tutela dei dati sensibili.

L'azienda è oggi in grado di fornire ai suoi clienti una check completa di tutti gli adempimenti da osservare e le misure di sicurezza da adottare in particolare dove vengono gestiti ed archiviati dati sensibili personali.
Grazie alla migliore strutturazione dei test informatici vengono definiti in modo più puntuale i perimetri aziendali all'interno dei quali sono presenti dati sensibili e si identificano le falle organizzative che possono portare ad una fuga impropria di informazioni.
Una corretta valutazione dei rischi, la formazione dei dipendenti, l'aggiornamento continuo e la disponibilità a

investire sono le azioni che consentono di ridurre drasticamente le probabilità di attacco.

4.2 Considerazioni riepilogative

Adottando un approccio interdisciplinare, volto cioè a trattare di cyber security secondo diverse ma complementari prospettive, l'azione formativa è riuscita ad elevare il grado di consapevolezza dei partecipanti rispetto alle emergenti sfide e opportunità scaturenti dall'uso dello spazio cibernetico.
In un mondo dove sempre più relazioni sociali ed economiche vengono traslate dal reale al virtuale la Publisys ha oggi le competenze per comprendere le principali minacce cyber e le loro basi tecnologiche, valutare e gestire efficacemente il rischio, difendere la privacy, attuare politiche efficaci per la propria organizzazione, costruire adeguati sistemi di protezione e far sì che i benefici della trasformazione digitale siano raggiungibili in un ambiente sicuro, affidabile e rispettoso dei diritti degli utenti.

5. Conclusioni

5.1 Gli elementi e/o i fattori che hanno influito positivamente sulla formazione

Diversi gli elementi e i fattori che hanno influito positivamente sulla formazione.
Sicuramente un'analisi dei fabbisogni approfondita e realizzata sul campo intervistando i diretti beneficiari.
In secondo luogo, l'elevata competenza del docente e i numerosi esempi pratici realizzati.
Tali fattori hanno fatto sì che l'azione formativa fosse perfettamente aderente alle problematiche che i consulenti

dell’impresa si trovano a dover affrontare ogni giorno e a proporre le giuste contromisure.

5.2 Le buone prassi formative aziendali

L’azione formativa esaminata ha avuto degli ottimi risultati sulle performance aziendali grazie ad un’analisi ben strutturata delle esigenze formative, aderenza dei contenuti ai fabbisogni, scelta adeguata dei docenti, alternanza ben misurata tra aula e on the job.

In un momento di altissima competitività per il settore ICT l’aver realizzato tale intervento formativo ha permesso di migliorare l’immagine sul mercato dell’azienda e la sua definizione di partner affidabile in grado di risolvere le questioni più delicate e critiche. Tutto ciò ha consentito non solo di mantenere l’occupazione presente ma di vedere con fiducia alle sfide del mercato che saranno generate dagli investimenti del PNRR.

5.3 Conclusioni

Se da un lato la transizione digitale sta portando tutte le imprese a spostare sempre più attività on line dall’altro occorre che tali processi siano gestiti nella massima sicurezza.

L’aumentare di tali criticità porta per le aziende del settore ICT una doppia sfida che porterà il moltiplicarsi delle occasioni di business.

Solo la formazione continua permetterà a tali aziende di acquisire competenze necessarie a garantire un'adeguata protezione delle infrastrutture, dei dati e delle applicazioni aziendali contro le nuove e mutevoli minacce derivanti dall’uso dei servizi in cloud e dal diffondersi delle piattaforme di mobile computing.

Acquisire competenze digitali per stare sempre al passo con le minacce informatiche, reagire rapidamente agli incidenti di sicurezza, dimostrare conformità a policy e normative di riferimento, mitigando e controllando i rischi per l'azienda: queste le sfide che l'impresa già conosce e che faranno sempre parte delle prossime azioni di formazione.