



MICRO IMPRESA PORTOGALLO

The risk story 2



Co-funded by the
Erasmus+ Programme
of the European Union



Micro impresa del Portogallo

Descrizione dell'azienda e della sua Supply Chain

Fondata negli anni '80, l'azienda opera nel settore dello stampaggio a iniezione di materie plastiche. Il suo core business si basa sulla produzione dei più innovativi ed efficienti sistemi aggiuntivi completamente elettrici, sviluppando diverse tecnologie che offrono soluzioni più sostenibili e flessibili ai suoi clienti.

È una società di ingegneria: trasforma le idee in prodotti. Questi sono progettati internamente in collaborazione con i clienti. L'azienda si occupa del processo di ricerca e sviluppo, ma i subappaltatori svolgono tutte le attività di produzione. Ogni subappaltatore riceve una parte dell'apparecchiatura, come un pezzo di Lego, senza conoscere il puzzle in cui tale pezzo si inserisce. Quel pezzo, insieme a molti altri, sarà incorporato nel prodotto finale.

Digitalizzazione della SC

L'azienda lavora con diversi sistemi informatici disponibili attraverso una intranet con diversi livelli di accesso, a seconda della funzione e delle responsabilità dei dipendenti. I dipendenti possono anche accedervi da remoto attraverso una VPN. Né i clienti né i fornitori hanno accesso all'intranet aziendale. L'interazione con i clienti avviene principalmente tramite e-mail, mentre un server FTP può essere utilizzato per il trasferimento di file, ad esempio per la condivisione di file di grandi dimensioni.

L'azienda utilizza un sistema ERP COTS che si integra con il sistema di gestione della produzione.

Risk Management

Esiste infatti una strategia di gestione del rischio. Tuttavia, il rischio informatico non viene considerato, nonostante la consapevolezza dell'importanza di questo rischio.

Pratiche di gestione del rischio

Dall'analisi interna ed esterna effettuata, è possibile identificare la SWOT e verificare le conseguenze e l'impatto sull'attività aziendale. L'identificazione e la valutazione del rischio vengono effettuate in una matrice. Tenendo conto della politica della qualità e dell'innovazione, si definiscono gli obiettivi e si

intraprendono le azioni per raggiungere gli obiettivi, nonché i passi necessari per affrontare i rischi identificati nella matrice.

Rischi:

Rischio operativo

L'azienda si avvale di accordi di non divulgazione per salvaguardare gli interessi dell'organizzazione e dei suoi clienti. Tali accordi possono essere estesi per integrare altre entità nel processo, come le università o - raramente, ma possibile -, quando sono in gioco sistemi complessi, i fornitori.

Per quanto riguarda i clienti, le uniche informazioni scambiate sono i requisiti del prodotto, mentre con i fornitori vengono scambiati solo i disegni tecnici. L'azienda si sente sicura dei suoi fornitori: in primo luogo, opera in un'area di business diversa da quella dei fornitori; in secondo luogo, ogni fornitore produce solo un componente dell'apparecchiatura, quindi non ha accesso all'intero progetto tecnico. L'azienda utilizza un software per analizzare i rischi dal punto di vista meccanico ed elettrico nello sviluppo di un prodotto.

Rischio finanziario

L'azienda ha un'autonomia finanziaria del 75% e non ricorre a prestiti bancari per il suo funzionamento.

Rischio di mercato

Quando l'azienda sviluppa un prodotto innovativo, prima di immetterlo sul mercato ne richiede il brevetto.

Rischio informatico

Il rischio informatico non viene considerato. Pertanto, l'azienda non è in grado di quantificare questo tipo di rischio, sebbene si percepisca una certa consapevolezza della loro potenziale gravità.

L'unico rischio identificato a livello informatico è stato l'hacking. Ma, considerando la prospettiva dell'azienda, non sarebbe così catastrofico, dal momento che le copie di sicurezza vengono effettuate quotidianamente e si trovano al di fuori dell'azienda. Inoltre, non è facile replicare un prodotto brevettato dall'azienda.

L'azienda si affida solo a una persona che gestisce i sistemi informatici. Per quanto riguarda la politica di sicurezza informatica dell'azienda, si considerano le seguenti misure preventive: nel contratto con i dipendenti si copre l'uso illegale dei dati aziendali (anche se nulla impedisce a qualcuno di scaricare dati

importanti); i backup vengono effettuati quotidianamente in un luogo esterno all'azienda; per la protezione dalle minacce si utilizzano firewall e antivirus.

C'è, infatti, una generale mancanza di conoscenza, che porta anche a svalutare tali rischi. Tuttavia, è fondamentale sottolineare che, nonostante questo tipo di rischio non sia stato finora formalmente preso in considerazione, il top management dell'azienda si è dimostrato aperto all'adozione della gestione del rischio informatico.

I rischi legati al COVID-19

Anche se alcuni dipendenti dovevano lavorare a distanza nell'azienda, si è ritenuto che, per quanto riguarda i rischi legati alla sicurezza delle informazioni, non fosse necessaria una maggiore consapevolezza. In questo senso, non sono state applicate misure aggiuntive.