

CYBER SECURITY PROGRAM

Progettare e attuare un Programma di Sicurezza è la **migliore strategia** per incrementare le capability aziendali di gestione della **Cyber Security**, in relazione al contesto esterno e interno. In questo modo si possono **mitigare i rischi** attraverso investimenti sinergici, allineati alle strategie del business e focalizzati sulle **aree di maggior esposizione**.

DOMANDE CHIAVE

Quali sono gli **AMBITI PRIORITARI** sui quali concentrare le risorse?

Dove trovare le **COMPETENZE SPECIFICHE** per gestire le priorità?

Data la maturità aziendale, quali azioni portano un **EFFETTIVO BENEFICIO**?

È corretto investire solo **SULL'AMBITO TECNOLOGICO**?

Come **MISURARE L'EFFICACIA** delle contromisure implementate?

INPUT E DRIVER



Contesto di business: strategie aziendali e risorse a disposizione nello sviluppo del programma

Vulnerabilità e incidenti: consapevolezza della reale esposizione ai rischi cyber

Normative, Standard e rilievi Funzioni di controllo: requisiti esterni e interni, standard di riferimento e segnalazioni di audit, risk e compliance

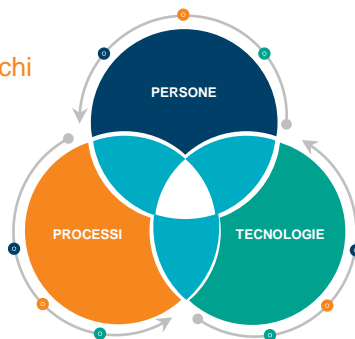
Cyber Risk Assessment: valutazione del livello di maturità sui diversi ambiti di interesse da usare come benchmark del percorso evolutivo

Trend degli attacchi cyber: evoluzione degli scenari esterni (es. incremento attacchi ransomware) per rispondere tempestivamente

Approccio Protiviti

Partendo da un'analisi del contesto, dei rischi e della maturità su temi di cyber security, il nostro approccio prevede uno sviluppo progressivo e sinergico di processi, tecnologie e persone.

Il livello di maturità viene monitorato nel continuo e le attività aggiornate ciclicamente, per tenere in considerazione i risultati ottenuti nel tempo.



Comprendere contesto
Cyber-Risk Assessment
Prioritizzazione e Pianificazione
Progettazione Processi
Valutazione e Selezione Tecnologie
Implementazione Processi e Tecnologie
Training & Awareness
Program Management & Reporting
Aggiornamento Cyber-Risk Assessment

Vantaggi e benefici di un Cyber Security Program

BUSINESS ALIGNMENT

Allineamento delle iniziative di sicurezza con la strategia di business e IT e con i requisiti emergenti

ROI

Ritorno degli investimenti in sicurezza grazie alla riduzione di costi legati a incidenti e mancate sanzioni

IMPROVING MATURITY

Crescita progressiva della maturità aziendale nella gestione della cyber security

PRIORITY MANAGEMENT

Gestione delle priorità nella realizzazione delle iniziative in concerto con la maturità e le strategie aziendali

MITIGAZIONE RISCHI

Mitigazione dei rischi grazie alla capacità complessiva di gestire le minacce di cyber security

COMPLIANCE

Monitoraggio e miglioramento continuo della compliance a normative, standard e regole interne

