I 4 STEP PER CRESCERE IN SICUREZZA

STEP
01

Assessment Infrastrutture Informatiche E Basi Di Dati

- Analisi dell’architettura di rete
- Analisi delle basi di dati aziendali e degli asset digitali dell’azienda, anche fisici (server, PC, laptop, ecc)

STEP
02

Penetration Test

- Valutazioni della sicurezza delle infrastrutture IT e delle basi di dati in essere, al fine di verificare l'efficacia dei meccanismi difensivi e la correttezza dell'implementazione delle specifiche policy, in conformità con la nuova regolamentazione normativa (GDPR) in riferimento alla protezione dei dati personali.

STEP
03

Redazione Action Plan

- Identificazione e definizione delle azioni da implementare in azienda al fine di mettere in sicurezza le infrastrutture e le basi di dati.
- Predisposizione linee guida comportamentali per gli utilizzatori, in modo da incrementale il livello di sicurezza e la loro corretta gestione.
- Training personalizzati.

STEP
04

Information security management system (ISMS)

- Implementazione dello strumento che permette di monitorare in maniera puntuale, sistematica e continuativa tutti i processi che riguardano la sicurezza del patrimonio informativo aziendale, gestionale ed organizzativo, definendo formalmente ruoli, responsabilità e procedure per l’operatività dell’azienda stessa.
- Con l'obiettivo di essere allineati alle norme ISO 27001, ed eventualmente ottenere una certificazione, ISMS garantirà l'adeguato livello di sicurezza, al fine di preservare intergrità, riservatezza e disponibilità dei dati in possesso.