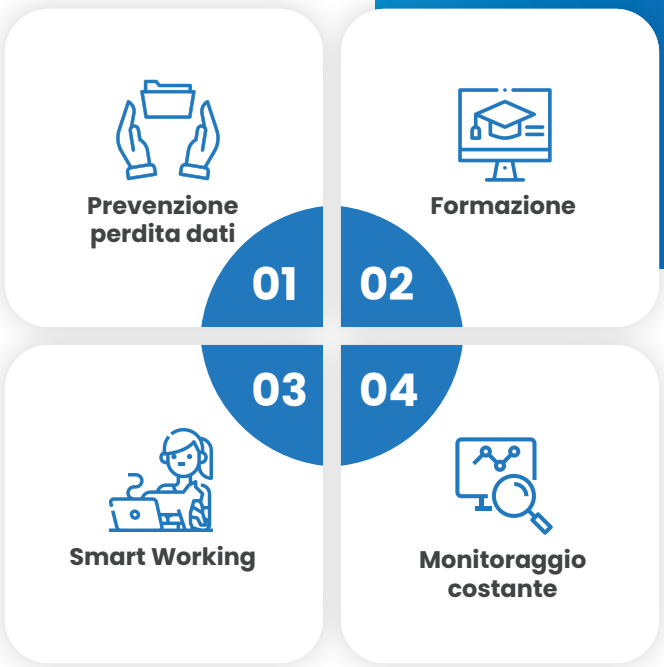
MITESYS
WE ARE TECHNOLOGY AND DESIGN

Sicurezza informatica: come proteggere la tua rete!

L'ERA DELL'INFORMAZIONE CHE STIAMO VIVENDO RICHIEDE UN FORTE CONTROLLO, STRUMENTI ADEGUATI E PERSONALE PREPARATO. LA SICUREZZA INFORMATICA CONSISTE NELL'ASSICURARE L'INTEGRITÀ, LA RISERVATEZZA E LA DISPONIBILITÀ DELLE INFORMAZIONI INDIPENDENTEMENTE DALLA DIMENSIONE E DALLA COMPLESSITÀ AZIENDALE.

Le informazioni che inevitabilmente forniamo quando utilizziamo un dispositivo elettronico, un'applicazione o un programma, servono a profilare gli utenti e forniscono indicazioni di mercato utili sia per apportare modifiche funzionali a prodotti già esistenti, sia per analizzare ed ipotizzare future tendenze e oscillazioni di mercato. Non solo, ad oggi questi big data (definiti anche il "nuovo petrolio") rappresentano una vera e propria opportunità anche per i criminali informatici.
Vi siete mai chiesti se le vostre informazioni e i vostri dati siano realmente al sicuro?
Per le aziende è fondamentale che venga implementato un disegno strategico completo, una vera e propria politica della security che deve essere considerata costantemente e aggiornata nel tempo.



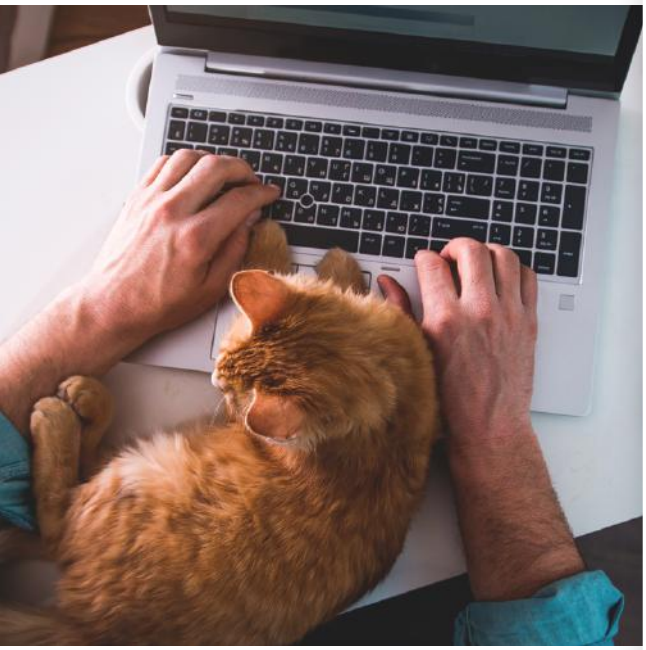
Le tre caratteristiche della sicurezza informatica

Per garantire la sicurezza informatica bisogna prendere in considerazione tre aspetti:
- la disponibilità dei dati, ovvero la salvaguardia del patrimonio informativo nella garanzia, confidenzialità e usabilità dei dati. È necessario quindi ridurre a livelli accettabili i rischi connessi all'accesso delle informazioni (furto di dati, intrusioni, etc.)
- l'integrità dei dati, cioè la garanzia che le informazioni non subiscano modifiche o cancellazioni a seguito di errori, malfunzionamento danni dei sistemi tecnologici.
- la riservatezza informatica, ovvero minimizzare i rischi connessi all'accesso o all'uso di informazioni in forma non autorizzata.

Vulnerability Assessment e Penetration Test

Il Vulnerability Assessment è una scansione delle vulnerabilità aziendali che mira ad identificare i punti deboli nel perimetro informatico e fornisce tutte le misure idonee a sanare ed evitare i rischi sul sistema di rete aziendale.

Il Penetration Test, che solitamente segue al Vulnerability Assesment, consiste nella simulazione di un vero e proprio attacco hacker al fine di testare la resistenza dell'infrastruttura. È consigliabile che entrambe queste due procedure vengano eseguite regolarmente, con test periodici.



Lo Smart Working

Sempre più realtà, per poter continuare a soddisfare le richieste aziendali, hanno dovuto approcciare a nuove soluzioni in smart working, che richiede una riorganizzazione lavorativa e una nuova implementazione dei livelli di sicurezza informatica e della protezione dei propri dati.

Le minacce informatiche a cui ci si espone lavorando da casa aumentano esponenzialmente, sia a causa dei dispositivi personali non adeguatamente protetti (a volte con sistemi operativi oblsoleti, sprovvisti di antivirus etc.) che per l'assenza di una giusta formazione, trascurando le misure di sicurezza e sottovalutando i rischi potenziali. Senza l'implementazione di una strategia di cyber security adeguata, lo smart working può trasforsi rapidamente in un enorme rischio.
Mitesys offre tutti gli strumenti e le soluzioni per lavorare in sicurezza, attraverso il backup e la gestione dei dati aziendali, l'utilizzo di piattaforme certificate per la condivisione dei documenti, verificando e implementando la sicurezza interna ed esterna, in tutto questo garantendo l'accesso a qualunque applicazione aziendale.

MITESYS TECHNOLOGIES SYSTEM SECURITY di Raspa Michele
Via Milazzo 35, 21100 Varese +39 0332 312 113
info@mitesys.it www.mitesys.it