competᵉ
A TESISQUARE® ECOSYSTEM COMPANY

WHITEPAPER

FORMAZIONE, CONSAPEVOLEZZA E GOVERNANCE DEL RISCHIO

Perché oggi il fattore umano è una misura organizzativa da governare.

Nel 2026 non dovremmo più chiederci «*Abbiamo erogato il corso?*», bensì porci una domanda molto più rilevante: «*Le persone della nostra organizzazione sono davvero in grado di riconoscere i rischi e prendere decisioni corrette nei contesti in cui operano ogni giorno?*»

Le aziende hanno investito enormemente in tecnologie di sicurezza, monitoraggio e protezione.

Eppure, una parte significativa degli incidenti continua a nascere da comportamenti umani: un clic su un messaggio credibile, una password riutilizzata, un allegato condiviso in fretta, un uso inconsapevole di strumenti di intelligenza artificiale.

È qui che **la formazione cambia natura**.
Non si tratta più di un'attività accessoria né di una voce di compliance da chiudere periodicamente bensì di una **misura organizzativa** con cui l'azienda rafforza la propria capacità di prevenire errori, ridurre esposizioni e costruire una cultura del rischio più matura.

Questo whitepaper nasce per rispondere a una domanda pratica: perché oggi cyber awareness, formazione privacy e AI literacy devono essere governate come un processo continuo?

Quali elementi rendono davvero efficace un piano formativo?

compet·e
A TESISQUARE® ECOSYSTEM COMPANY

INDICE

Introduzione	**4**
Il fattore umano | **Perché la tecnologia da sola non basta**	**5**
Le norme che cambiano prospettiva | **GDPR, NIS2 e AI Act**	**6**
Formazione come processo continuo | **Dall'obbligo all'efficacia**	**7**
Percorsi diversi per rischi diversi | **Non tutte le persone hanno gli stessi bisogni**	**8**
AI literacy e cyber awareness | **Le nuove priorità formative**	**9**
Come organizzare un piano efficace | **Le domande da porsi**	**10**
Checklist pratica | **Come capire se la formazione funziona davvero**	**10**
Una proposta concreta | **Academy, aula e FAD on demand**	**12**
Prossimi passi	**13**

compet·e
A TESISQUARE® ECOSYSTEM COMPANY

INTRODUZIONE

Quando si parla di gestione del rischio, l'attenzione si concentra spesso su tecnologie, processi, controlli e sistemi di monitoraggio.

Tutti elementi essenziali, ma non sufficienti da soli a garantire comportamenti corretti nel lavoro quotidiano.

Le persone prendono continuamente decisioni che possono ridurre o aumentare il livello di esposizione dell'organizzazione: aprire o meno un allegato, verificare un destinatario, usare correttamente un sistema di AI, riconoscere un'anomalia o seguire una procedura: è in questi passaggi quotidiani che il **fattore umano** entra nella **governance del rischio**.

> **"Il tuo firewall più importante è già in azienda: sono le persone."**