



# CONSULENZA SPECIALISTICA IN TEMA **CYBER SECURITY**

Consorzio **GLOBAL** offre alle Imprese del settore Trasporto & Logistica consulenza specialistica in materia di Cyber Security, per supportare le Organizzazioni a proteggere i propri sistemi informatici al fine di prevenire e/o gestire attacchi informatici e/o minacce atte a compromettere la sicurezza delle informazioni e dell'operatività.

## PROCESSI, PERSONE, TECNOLOGIA

*Consulenza Specialistica in tema di Cyber Security*

### Perchè

Il moltiplicarsi degli attacchi informatici e delle minacce in grado di compromettere la sicurezza delle informazioni e dell'operatività ha reso il rischio legato alla cybersecurity una vera **emergenza per la filiera del trasporto e della logistica, considerate tra i soggetti più «sensibili» agli attacchi.**

### Come

È fondamentale e strategica l'urgenza espressa dai Paesi e dalle Aziende di tutto il mondo di proteggere i propri sistemi informatici. Per questo si sono affermati, a livello internazionale, framework adatti a guidare l'adozione di misure di sicurezza per prevenire e mitigare il rischio attraverso opportuni sistemi di governance.

I framework prevedono misure generaliste unitamente a specifiche caratteristiche derivanti dal settore di riferimento. L'obiettivo è permettere all'azienda che li adotta di identificare un livello di sicurezza target e definire una roadmap strategica per il raggiungimento di tale livello.



## CONSULENZA SPECIALISTICA IN TEMA **CYBER SECURITY**



### La metodologia di lavoro

La nostra consulenza specialistica è finalizzata ad individuare i rischi cyber dell'intera organizzazione e a definire una roadmap atta a colmare i gap identificati dal risk assessment. Il fine è garantire integrità, riservatezza e disponibilità dei dati.

A seguito dell'analisi iniziale, viene articolato un piano strategico che tiene conto di tutte le variabili che influiscono sulla sicurezza informatica: **dalla tecnologia ai processi aziendali, dal fattore umano alla governance.**

### Le fasi di progetto

Il modello metodologico di intervento prevede una serie di fasi tra di loro modulari, attivabili anche singolarmente:

- **Cybersecurity Assessment**
- **Valutazione attuale piano di gestione della sicurezza rispetto alle normative specifiche**
- **Elaborazione e messa in campo di una roadmap adeguata a colmare i gap identificati**
- **Evoluzione continua e mantenimento del livello di protezione nel tempo**
- **Azioni di formazione e comunicazione**
- **Eventuale consulenza specialistica (legale, assicurativa...)**

### Ulteriori opportunità

Le aziende che effettuano la formazione in materia di cyber possono accedere alle **detrazioni fiscali** previste dal bando **Formazione 4.0**. Poter attivare il **credito d'imposta** per le aziende è un vantaggio competitivo di grandissimo valore.

