

SCHEDA PERCORSO FORMATIVO

Titolo del corso

CYBERSECURITY PER LE IMPRESE

Descrizione del corso e obiettivi

Il corso ha l'obiettivo di offrire una formazione base ma completa in materia di sicurezza informatica, illustrando minacce comuni, contromisure tecnologiche e buone pratiche organizzative e comportamentali, anche alla luce delle normative vigenti.

Attraverso sei moduli complementari, i partecipanti acquisiranno strumenti concreti per:

- Comprendere i rischi informatici in ambito industriale e le soluzioni tecniche e organizzative per ridurli.
- Acquisire competenze base sui sistemi di difesa e sulle minacce informatiche.
- Apprendere come integrare le norme di legge (es. GDPR, NIS2) nei processi aziendali.
- Migliorare i comportamenti quotidiani dei dipendenti rispetto alla sicurezza informatica

Struttura del corso

Modulo 1 – Cybersecurity in azienda: rischi, scenari e cultura organizzativa

Focus: introduttivo e comportamentale

Contenuti:

- Concetto di cybersecurity: differenze tra IT e OT
- Le principali minacce: phishing, ransomware, social engineering
- Rischi specifici per la manifattura: fermo produzione, furto di dati, sabotaggio digitale
- Comportamenti errati più diffusi e buone pratiche quotidiane
- La responsabilità condivisa: tutti sono parte del sistema di difesa

Modulo 2 – Sicurezza tecnica: asset, reti, dispositivi, dati

Focus: tecnico

Contenuti:

- Rilevazione e mappatura degli asset critici
- Segmentazione delle reti: IT/OT separation
- Sicurezza dei dispositivi: workstation, server, controller industriali
- Sicurezza dei dati: backup, cifratura, accessi

Modulo 3 – Policy aziendali, gestione utenti e formazione interna

Finanziato dall'Unione europea – Next Generation EU

Focus: organizzativo

Contenuti:

- Redazione di policy interne (accesso, password, uso dispositivi)
- Autenticazione forte e gestione delle identità (IAM, MFA)
- Ciclo di vita degli utenti (onboarding, offboarding)
- Formazione continua e sensibilizzazione del personale
- Simulazioni di phishing e campagne di awareness

Modulo 4 – Compliance normativa: GDPR, NIS2 e responsabilità aziendali

Focus: legale / compliance

Contenuti:

- GDPR: principi, accountability, data breach, misure tecniche e organizzative
- NIS2: a chi si applica, obblighi minimi e impatto per le PMI industriali
- Audit, DPIA, registro trattamenti: cosa serve davvero
- Il ruolo del DPO e della sicurezza “by design”
- Come evitare sanzioni e dimostrare la conformità

Modulo 5 – Incident response, continuità operativa e comportamento in caso di attacco

Focus: organizzativo, tecnico, comportamentale

Contenuti:

- Che cos'è un incidente informatico
- Il piano di risposta: ruoli, escalation, comunicazione interna
- Business Continuity e Disaster Recovery Plan
- Come riconoscere un attacco e cosa (non) fare
- Simulazione di un caso reale di gestione incidente (tabletop exercise)

Modulo 6 – Attacchi e difese

Focus: tecnico

Contenuti:

- Quali sono gli attacchi
- Quali sono i meccanismi di difesa
- Aggiornamenti
- Vulnerabilità dei sistemi industriali

Durata

La durata totale del percorso è di 24 ore, suddivise in n. 8 giornate da 3 ore ciascuna.

Finanziato dall'Unione europea – Next Generation EU

Data	orario	Ore
martedì 14 ottobre 2025	10:00-13:00	3
mercoledì 15 ottobre 2025	10:00-13:00	3
lunedì 20 ottobre 2025	10:00-13:00	3
mercoledì 22 ottobre 2025	10:00-13:00	3
martedì 28 ottobre 2025	10:00-13:00	3
mercoledì 29 ottobre 2025	10:00-13:00	3
martedì 4 novembre 2025	10:00-13:00	3
mercoledì 5 novembre 2025	10:00-13:00	3
TOTALE ORE		24

Il calendario può subire variazioni

Destinatari

Tipologia destinatari: Il corso è riservato a **dipendenti, amministratori o soci** di società, in particolare:

E' rivolto a figure professionali che operano all'interno di imprese strutturate (costituite in forma societaria, come Srl, Spa, etc.), con particolare attenzione a quelle attive nei settori industriali e manifatturieri, dove l'esposizione ai rischi informatici è crescente.

Sono destinatari ideali del percorso:

- **Dipendenti aziendali**, in particolare coloro che:
 - Lavorano in reparti IT, manutenzione, produzione o logistica.
 - Gestiscono dati sensibili, processi digitalizzati o dispositivi connessi in rete.
 - Sono coinvolti nella gestione dei sistemi informativi o dei flussi documentali aziendali.
 - Operano in smart working o con accessi da remoto ai sistemi aziendali.
- **Responsabili di funzione**, tra cui:
 - IT Manager, Operation Manager, Plant Manager, Responsabili della Qualità o Sicurezza.
 - Referenti interni per la compliance normativa (GDPR, NIS2).
 - Responsabili HR o di formazione interna, coinvolti nella diffusione della cultura della sicurezza informatica.
- **Amministratori, soci e titolari d'impresa**, interessati a:
 - Comprendere l'impatto organizzativo, economico e giuridico di eventuali incidenti informatici.
 - Integrare strategie di cybersecurity nella governance e nella pianificazione aziendale.
 - Assolvere agli obblighi di accountability e prevenzione imposti dalla normativa vigente.

Numero Massimo: 25 partecipanti

Modalità

Online (FAD Sincrona)

Livello

Base

In collaborazione con:



Attestato di partecipazione

Artes 4.0 e Stargate Consulting & Training

Prezzo

Il percorso formativo rientra nelle agevolazioni previste dal PNRR da erogare alle PMI, perciò l'imponibile del costo del corso verrà finanziato in una misura variabile dal 50% al 100% a seconda della tipologia dell'azienda partecipante.

Scopri la scontistica riservata alla tua azienda scrivendoci!

(É previsto uno sconto del 100% per le Piccole Imprese, dell'80% per le Medie Imprese, del 50% per le Grandi Imprese).

Costo del corso: Euro 1.600,00 (+ IVA22%)

Verrà applicato uno sconto in fattura pari al finanziamento.

L'IVA è in ogni caso a carico dell'impresa e dovrà essere pagata dall'impresa.

L'importo dell'IVA e la quota parte eventualmente non finanziata dovranno essere pagati prima dell'inizio del corso.

Verranno prese in considerazione le richieste di iscrizione inoltrate entro **il 20/09/2025.**