

## CAMERA DI COMMERCIO INDUSTRIA ARTIGIANATO E AGRICOLTURA DI GENOVA

Riunione della Giunta Camerale di lunedì 7 aprile 2025 - Ore 15.12

Presenti	Assenti		
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Sig. Luigi ATTANASIO	- Presidente
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Sig. Alessandro CAVO (*)	- Vicepresidente Vicario
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Dott.ssa Paola NOLI	- Vicepresidente
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Sig. Paolo CORSIGLIA	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Dott. Stefano MESSINA	
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Sig. Giovanni MONDINI	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Dott. Felice NEGRI	
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Sig. Massimiliano SPIGNO	
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Dott. Massimiliano TUMIATI	- Presidente Revisori dei Conti
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Dott. Gian Alberto MANGIANTE	- Revisore dei Conti
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Dott. Riccardo SCARPULLA	- Revisore dei Conti
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Dott. Maurizio CAVIGLIA	- Segretario Generale

\*\*\*\*

Il sig. Cavo entra alle ore 15.24 durante la trattazione della delibera n.157.

Assistono il Segretario Generale il Dirigente Vicario, Dott. Marco Razeto e la sig.ra Angela Modestini. Partecipa alla riunione l'ing. Filippo Delle Piane, in qualità di Presidente della Consulta per le infrastrutture e l'urbanistica.

N. 166 del 07.04.2025

OGGETTO: Progetto Doppia Transizione digitale ed ecologica: servizi specialistici in tema di transizione digitale su cyber sicurezza-affidamento al Centro di Competenza Start4.0. CUP I39G23000180005.

IL PRESIDENTE riferisce:

Con delibera n. 3C del 24 ottobre 2022 il Consiglio Camerale ha approvato i progetti predisposti ai sensi dell'art. 18, comma 10, della Legge 29 dicembre 1993 n. 580, come modificata dal D.Lgs. 25.22.2016 n. 219, fra i quali il progetto denominato "Doppia Transizione digitale ed ecologica".

Il progetto "Doppia Transizione" riprende e consolida le attività riferite alla transizione digitale del PID abbinandole ad altre attività relative alla transizione ecologica e green, prevedendo la realizzazione di servizi in grado di coniugare le esigenze digitali delle imprese con i principi di sostenibilità, di efficientamento energetico, di economia circolare e infine di incentivare l'adozione delle CER.

Il progetto prevede, nel triennio 2023/25, un budget di 1.730.817,00euro complessivi di cui 1.021.195,00 euro di costi esterni.

Per quanto riguarda le attività per la transizione digitale ad inizio triennio è stato rinnovato l'impegno di collaborazione tra l'Ente Camerale e il Centro di competenza per le infrastrutture strategiche Start4.0 attraverso il protocollo di intesa sottoscritto il 27 luglio 2023. Il protocollo, approvato con delibera della Giunta 199/2023 ricalca il precedente accordo di collaborazione del 2020 che ha permesso l'organizzazione di attività specialistiche di formazione e orientamento alla digitalizzazione proposte alle imprese da parte del Punto Impresa Digitale.

Di estrema importanza è la tematica della Cyber Security, più volte richiamata in vari provvedimenti dalla Giunta camerale, per la quale la collaborazione con Start4.0 è stata continuativa sin dal 2020. Da allora sono state realizzate attività di formazione specialistica prevalentemente rivolte alle imprese e al mondo associativo e professionale, ma anche di informazione e comunicazione tramite webinar e pillole video. Sono state inoltre avviate attività di *assessment* e realizzati convegni specialistici.

Per l'anno in corso è stata programmata dal Punto Impresa Digitale insieme a Start4.0 la terza edizione del corso *Cybersecurity dalla consapevolezza all'approccio specialistico*,

che ricalca come struttura quello realizzato nel 2024 e che è stato particolarmente apprezzato da parte delle imprese.

Le attività per la realizzazione del corso, per un totale di euro 15.000,00 oltre IVA sono le seguenti:

- Evento di lancio per diffusione del corso e panoramica sull'importanza di una policy di cybber sicurezza aziendale.
- Offerta info-formativa destinata alle imprese, da somministrare in presenza o da remoto, della durata di 24 ore con i seguenti obiettivi:
  - Fornire strumenti e strategie per la sicurezza informatica in azienda
  - Conoscere i principali rischi e minacce cyber;
  - Avere consapevolezza delle normative in materia;
  - Impostare i corretti processi aziendali a protezione delle persone, dei macchinari e della continuità operativa;
  - Saper selezionare gli strumenti di protezione migliori per la propria realtà aziendale.
- Esercitazione finale sul cyberbus: a conclusione del corso i partecipanti dovranno mettere in pratica quanto appreso nelle lezioni attraverso un divertente gioco di simulazione, una "Cyber Escape Room" su quattro ruote che permette di riflettere sugli errori più comuni che si fanno in tema cybersecurity.

Le lezioni frontali saranno avviate entro il mese di maggio 2025 e le attività di promozione e comunicazione del progetto rivolto alle imprese, ad eccezione dei contenuti tecnici, saranno realizzate in collaborazione diretta con il Punto Impresa Digitale.

Il RELATORE propone di effettuare affidamento diretto tramite M.E.P.A. - Mercato Elettronico della Pubblica Amministrazione, ex art. 50 comma 1 lett. b) del D. Lgs. n. 36/2023 a Start4.0 per le attività sopra descritte, per euro 15.000,00 oltre IVA e di nominare la Dott.ssa Paola Carbone Responsabile Unico del progetto ai sensi dell'art. 15 e Allegato I.2 del D.Lgs. 36/2023.

LA GIUNTA CAMERALE

Udita l'esposizione del Relatore;

Condivisa la necessità di predisporre specifiche attività specialistiche a favore delle MPMI;

Visto il protocollo di intesa sottoscritto con il Centro di Competenza Start4.0, con il quale le parti hanno dichiarato il reciproco interesse a collaborare all'attuazione di progetti comuni che favoriscano la digitalizzazione e la crescita innovativa del territorio, comprese attività specialistiche di formazione in tema di cyber sicurezza;

Considerato che il Progetto Doppia Transizione Digitale ed Ecologica è attivo per il triennio 2023 - 2025 e che la terza edizione del Corso di formazione rivolto amme MPMI sarà realizzata nel periodo maggio - luglio 2025;

Unanime,

d e l i b e r a

-di stanziare un importo di 15.000,00 oltre IVA a copertura dei servizi specialistici realizzati da Start 4.0 in tema di cyber sicurezza per il periodo maggio - luglio 2025;

- di imputare l'onere di € 18.300,00 IVA compresa sul conto 330002 "Interventi Economici Doppia Transizione" al Centro di Costo DD02 "Doppia Transizione digitale ed ecologica;

- di nominare la Dott.ssa Paola CARBONE, Responsabile Unico del progetto ai sensi dell'art. 15 e Allegato I.2 del D.Lgs. 36/2023;

- di demandare al Segretario Generale l'adozione degli atti conseguenti.

Allegato

Il Presidente  
f.to Sig. Luigi Attanasio

Il Segretario Generale  
f.to Dott. Maurizio Caviglia



Per copia conforme ad uso amministrativo  
Il DIRIGENTE VICARIO  
Dott. Marco RAZETO



Alla c. a. Dott.ssa P. Carbone  
Spett.le Camera di Commercio di Genova

**OGGETTO: Offerta per corso di formazione in materia di Cybersecurity della durata di 24 ore**

Facendo seguito alle Vostre richieste, si invia l'offerta relativa ai servizi in oggetto.

Con la speranza di aver saputo cogliere le Vostre esigenze, il nostro team è a disposizione per ogni ulteriore dettaglio e/o approfondimento.

In attesa di cortese riscontro, si porgono

Cordiali saluti,  
**Centro di Competenza START 4.0**  
Prof.ssa Paola Girdinio  
Presidente

Genova, 01/04/2025

## PREMESSA

---

### IL CENTRO DI COMPETENZA START 4.0

Il Centro di Competenza Start 4.0, con sede a Genova, è uno degli 8 soggetti a livello nazionale nati dal Piano Industria 4.0 nel 2019. Nel 2023 è stato rifinanziato dal Ministero delle imprese e del Made in Italy, a valere sul Piano Nazionale di Ripresa e Resilienza (PNRR).

Si tratta di un partenariato pubblico – privato, costituito attualmente da 51 tra le principali imprese ed entità pubbliche impegnate nella digitalizzazione e innovazione tecnologica del Paese. Grazie all'expertise di questo esteso network di imprese, partner e fornitori, il Centro di Competenza rappresenta uno strumento strategico per far crescere la maturità digitale del sistema economico italiano e supportare l'adozione nelle imprese di nuove tecnologie nei prodotti, nei processi e nei servizi.

Start 4.0 opera attraverso diverse tipologie di attività: piani di formazione, consulenza per l'innovazione e l'accesso ai finanziamenti, erogazione di contributi attraverso bandi, servizi di test before invest.

Uno dei pilastri dell'offerta di START 4.0 è la formazione specialistica e personalizzata sulle tecnologie abilitanti e sulla sicurezza delle infrastrutture strategiche, fondamentale base per la transizione digitale sicura e sostenibile.

### CONTESTO OPERATIVO

Secondo gli ultimi dati ISTAT, le imprese con meno di 250 dipendenti costituiscono il 99,9% del totale delle aziende italiane e sono purtroppo le principali vittime di attacchi informatici. Questo è dovuto a numerosi motivi.

In primo luogo, le PMI tendono ad avere risorse limitate per la protezione dei propri sistemi digitali, il che le rende bersagli più facili per i criminali informatici. Inoltre, la minore consapevolezza delle minacce cyber e la mancanza di strumenti avanzati di cybersecurity aumentano la loro vulnerabilità.

Le PMI sono anche il principale veicolo attraverso il quale i criminali informatici riescono a colpire e a sottrarre i dati delle grandi aziende. Questo perché spesso le PMI appartengono alla supply chain di grandi imprese e quindi un attacco a una PMI può compromettere la sicurezza di tutta la catena di fornitura. Con l'entrata in vigore della Direttiva Europea NIS2 le medie e le grandi imprese in ambito NIS 2 devono fare un'analisi della loro supply chain e la sicurezza diventa così per le PMI un grande

vantaggio competitivo su cui le grandi imprese baseranno la loro scelta per stabilire i fornitori di un servizio e/o prodotto.

È importante sottolineare che il fattore umano rappresenta il principale rischio e, come i dati dell'ultimo Rapporto CLUSIT di marzo dimostrano, ancora fragile di fronte a tecniche di ingegneria sociale. La consapevolezza dei rischi in ambito cybersecurity è la prima forma di prevenzione, ma molte PMI non investono abbastanza in formazione e sensibilizzazione del personale.

Da questo la lungimirante azione della Camera di Commercio di Genova che da tre anni mette a disposizione delle PMI un corso di cybersecurity che parte dalla consapevolezza e permette di raggiungere un livello più specialistico nell'affrontare le sfide della sicurezza cyber.

## PROPOSTA FORMATIVA

---

Descrizione del corso:

La trasformazione digitale ha creato significative opportunità per le PMI grazie ad una più efficiente ed ottimizzata gestione delle risorse interne e dei processi aziendali e questo scenario sta ulteriormente cambiando con l'introduzione di strumenti di AI. Con la connettività degli strumenti di lavoro e con il lavoro da remoto però i confini aziendali sono cambiati ed espongono a rischi nuovi per le aziende che possono compromettere gravemente l'operatività. Per poter impostare le contromisure adeguate dotandosi dei corretti sistemi di protezione, la prima e più importante forma di prevenzione è la consapevolezza delle possibili minacce.

Il quadro normativo è in forte evoluzione soprattutto con l'introduzione di NIS2, cyber resilience act e nuovo regolamento macchine e può influire non solo sulle attività ma sulle possibilità di business perché spesso sono proprio le PMI ad essere attaccate in quanto fornitori di grandi aziende. Un asset fondamentale diventa allora la capacità di dare garanzie ai propri clienti in tema di cybersecurity per potersi assicurare le commesse.

Questo corso si pone l'obiettivo di essere la vostra prima forma di protezione e di introdurre un vantaggio competitivo dato dal valore della sicurezza aziendale.

Per un miglior coinvolgimento dei partecipanti, è previsto un laboratorio formativo finale concepito come una caccia al tesoro allestita all'interno di un pulmino denominato "Cyber Bus" con una postazione pc. Il partecipante dovrà vestire i panni di un hacker per sottrarre file riservati dal pc. Perché si può imparare molto anche divertendosi.

Si stima una classe con al massimo 40 partecipanti.

# START4.0

## Obiettivi del corso:

- Fornire strumenti e strategie per la sicurezza informatica in azienda;
- Conoscere i principali rischi e minacce cyber;
- Avere consapevolezza delle normative in materia;
- Impostare i corretti processi aziendali a protezione delle persone, dei macchinari e della continuità operativa;
- Saper selezionare gli strumenti di protezione migliori per la propria realtà aziendale.

## Metodologia didattica:

- Il corso sarà erogato da remoto con 3 lezioni in presenza (la prima, l'ultima e il workshop sul PID cyber check).
- Il Centro di Competenza mette a disposizione la piattaforma Webex per l'erogazione a distanza di formazione sincrona.
- Gamification per un miglior coinvolgimento dei partecipanti attraverso il laboratorio finale sul Cyber Bus.

## Programma del corso:

### A. I fondamentali

Gli ultimi dati sugli attacchi a livello globale e italiano

Cyberspazio

Cybersecurity definizione

Cybercrime

Darkweb

Criptovalute

Blockchain

Mondo IoT e rischi cyber

Trasformazione digitale e importanza del dato

## B. Rischi e metodiche di attacco

Attacchi significativi

La normativa in materia cyber

Il Social Engineering.

Il phishing e spear phishing.

I Dos e i Ddos.

Gli APT.

I Man in the middle.

I Ransomware.

Le minacce dall'interno.

## C. La prevenzione e le tecniche di protezione

Antivirus e Firewall

Siem

Iams

Come usare l'email in modo sicuro.

La PEC e la posta crittografata.

Costi verso analisi dei rischi

Cyberinsurance e prodotti assicurativi

La gestione del cyber risk

Le buone pratiche aziendali

Metodiche di protezione del rischio di nuova generazione

La security by design

Cyber threat intelligence

Il CERT

Il SOC

Lavoro a distanza vs smartworking

Problematiche connesse alla sicurezza del lavoro a distanza

Cosa fare per prevenire

---

## ATTIVITÀ DI PROGETTO

1. Progettazione di dettaglio del corso
2. Definizione del calendario del corso in accordo con la Committenza
3. Elaborazione dei materiali didattici
4. Selezione dei docenti approvati dalla Committenza
5. Erogazione del corso
6. Fornitura dei materiali didattici ai partecipanti
7. Registro presenze
8. Eventuali registrazioni del corso se erogato a distanza e se richieste
9. Questionario di gradimento finale

---

## TEMPISTICHE DI PROGETTO

Il progetto formativo prevede 24 ore suddivise in sessioni da 2 ore ciascuna e permette di descrivere non solo i concetti generali e fondamentali in materia di cybersecurity, ma anche la governance aziendale per le PMI illustrando, inoltre, processi e strumenti da adottare per non esporsi a rischi e minacce informatiche e non incorrere in sanzioni a causa del mancato adeguamento alla normativa.

---

## RISORSE DI PROGETTO

Le figure operative messe a disposizione dal Centro di Competenza START 4.0 che seguiranno il progetto nelle fasi descritte, saranno le seguenti:

- **Training Manager**
- **Tutor formativo**
- **Tutor di laboratorio**

## - Cyber Bus

### SEDI DI LAVORO

Le attività di cui sopra verranno svolte sia da remoto che presso la sede del Cliente, secondo il piano di lavoro che verrà concordato con il responsabile tecnico designato dal Cliente.

In ogni caso il Cliente riconosce al team di progetto il diritto di accesso alla propria sede durante il normale orario lavorativo o in ogni momento necessario ai fini della esecuzione del presente accordo, secondo modalità e tempi concordati con il responsabile designato dal Cliente.

### PROPOSTA ECONOMICA

---

Il costo della gestione annuale del progetto formativo è di **Euro 15.000 oltre IVA.**

Ogni variazione sulla pianificazione, sulle specifiche tecniche o nella composizione del team lato Cliente potrebbe comportare una revisione della proposta che, nel caso, sarà sottoposta al Cliente per approvazione.

Se durante l'attività dovessero sorgere delle richieste speciali che modifichino l'obiettivo o l'ambito, sarà nostra premura comunicarvelo tempestivamente in modo da identificare le azioni correttive.

### CONDIZIONI PRELIMINARI - RISERVATEZZA

---

START4.0 si impegna ed impegna il proprio personale a non rivelare a terzi, sia durante le attività previste sia in seguito, qualsiasi informazione riservata relativa ai servizi, ai piani, all'attività e all'organizzazione della Camera di Commercio di Genova di cui possa venire a conoscenza nell'ambito delle attività sopra descritte.

START4.0 si rende disponibile sin da ora a siglare uno specifico accordo di confidenzialità tra le parti prima dell'avvio delle attività.

Il presente documento (ed eventuali allegati) resta di proprietà di START 4.0 e può essere comunicata a terze parti o riprodotta solamente previo il consenso scritto da parte di START 4.0 che si riserva inoltre il diritto di richiederne il qualsiasi momento la restituzione.

## OBBLIGHI DELLA COMMITTENZA

---

Il Cliente si impegna a:

- Identificare ed indicare un referente per gli aspetti progettuali, responsabile delle comunicazioni ufficiali fra le aziende, e della validazione delle attività tecniche e progettuali;
- Fornire tempestiva validazione ai deliverable, secondo i piani concordati e in modo da permettere lo svolgimento delle attività secondo gli stessi;
- Mettere a disposizione le strutture aziendali e le funzioni organizzative necessarie al corretto svolgimento delle attività;
- Fornire, al personale di progetto impegnato nell'attività, un adeguato ambiente di lavoro e le istruzioni inerenti alle norme sulla sicurezza del lavoro in uso presso le sedi del Cliente;
- Garantire l'accesso ai suoi sistemi informativi limitatamente alle necessità del progetto.

## MODALITÀ DI FATTURAZIONE E CONDIZIONI DI PAGAMENTO

---

I termini di pagamento delle fatture sono stabiliti in 30 giorni fine mese dalla data di fattura, emessa al termine dell'attività formativa.

La fatturazione sarà effettuata secondo il secondo piano:

- 40% all'accettazione dell'offerta;
- 60% al termine delle attività previste in offerta.

In caso di ritardo nel pagamento del corrispettivo saranno dovuti gli interessi moratori ai sensi del D.lgs. n.231 del 2002, comma 1 dell'art.5.

## ACCETTAZIONE OFFERTA

DATA ACCETTAZIONE:

**START 4.0  
(PRESIDENTE)**



Firmato digitalmente da:  
GIRDINIO PAOLA  
Firmato il 01/04/2025 15:51  
Seriale Certificato: 3543549  
Valido dal 01/05/2024 al 01/05/2027  
Info: Camere Qualified Electronic Signature CA

**TIMBRO E FIRMA DEL CLIENTE  
(PRESIDENTE)**