DELIBERA N. 70

Camera di Commercio
Genova

CAMERA DI COMMERCIO INDUSTRIA ARTIGIANATO E AGRICOLTURA DI GENOVA

Riunione della Giunta Camerale di lunedì 26 febbraio 2024 - Ore 15.08

Presenti	Assenti			
*		Sig. Luigi ATTANASIO	-	Presidente
*		Sig. Alessandro CAVO	-	Vicepresidente Vicario
*		Dott.ssa Paola NOLI	-	Vicepresidente
	*	Sig. Paolo CORSIGLIA		
	*	Dott. Stefano MESSINA		
	*	Sig. Giovanni MONDINI		
*		Dott. Felice NEGRI		
*		Sig. Massimiliano SPIGNO		
*		Dott. Ruggero REGGIARDO	-	Presidente Revisori dei Conti
*		Dott. Gian Alberto MANGIANTE(*)	-	Revisore dei Conti
*		Dott. Giuseppe NOVELLI	-	Revisore dei Conti
*		Dott. Maurizio CAVIGLIA	-	Segretario Generale

****

(*) Il dott. Mangiante entra alle ore 15.35 durante la comunicazione n. 30C.

Assistono il Segretario Generale il Dirigente Vicario, Dott. Marco Razeto, e la sig.ra Angela Modestini. Partecipano alla riunione il consigliere ing. Filippo Delle Piane, in qualità di Presidente della Consulta per le infrastrutture e l'urbanistica e il consigliere dott. Alessandro Pitto, in qualità di Presidente della Consulta per il settore marittimo, portuale e logistico.

N. 70 del 26.02.2024

OGGETTO: Progetto Doppia Transizione: 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".

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 1.730.817,00 euro complessivi di cui 1.021.195,00 euro di costi esterni.

Per quanto riguarda le attività per la transizione digitale nel corso del 2023 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 *assesment* e realizzati convegni specialistici.

Per l'anno in corso è stato programmato dagli uffici camerali insieme a Start4.0 non solo di svolgere attività info-

formative di sensibilizzazione sulle tematiche di riferimento rivolte alle imprese ma anche di prevedere una attività destinata al personale e alla struttura camerale.

Sono state predisposte dal Centro di Competenza due offerte distinte (allegate alla presente proposta): la prima per un corso di formazione destinato alle imprese in materia di Cybersecurity della durata di 24 ore che ricalca la prima edizione del corso *Cybersecurity dalla consapevolezza all'approccio specialistico,* che si è tenuto nel 2022 ed ha ottenuto buon riscontro di partecipazione, e la seconda per un progetto formativo di *Cybersecurity awareness* e *cybersecurity assesment* destinato all'Ente camerale.

Le attività specialistiche dei due progetti, per un totale di euro 40.000,00 oltre IVA sono le seguenti:

1. 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.

   Costo previsto per il corso, incluse ore di progettazione e preparazione del materiale: complessivi euro *15.000,00 oltre IVA*.

   Si prevede di avviare il progetto entro il mese di maggio 2024

2. Assesment cyber dei sistemi informativi della durata di un anno e percorso per aumentare la consapevolezza della minaccia cyber:

   -Linea progettuale awareness:

   *S*i propone di utilizzare la piattaforma di Cyber Guru, più vicina a rispondere a bisogni ed esigenze della Camera di Commercio di Genova.

   Il progetto sarà seguito in ogni fase da PM di Start 4.0 e prevede tutti i livelli di governance di un progetto tecnico a tutti gli effetti con avanzamenti SAL quindicinali, Status meeting bimestrali e Steering Committee semestrale. Per ogni riunione sarà stilata una minuta con le azioni da svolgere entro il meeting successivo.

Cyber Guru offre una piattaforma di Cyber Security Awareness di grande efficacia, finalizzata a trasformare il fattore umano da anello debole della catena difensiva a prima linea di difesa contro il cybercrime anche tramite la somministrazione di finti malware al fine di aumentare la resistenza perimetrale dell'Ente agli attacchi Phishing e Smishing. L'offerta include 120 licenze.

-Linea progettuale assessment: a complemento del progetto formativo verrà svolta un'attività di cybersecurity assessment di alto livello per la verifica del grado di maturità della server farm, un'analisi del web e del deep web per verificare l'esposizione online dell'Ente prestando attenzione particolare a eventuali e-mail compromesse ed altre vulnerabilità che richiedono interventi urgenti di adeguamento.

Le attività previste durante quest'ultima fase si compongono di:

- Interview: analisi del framework più adatto per la Committenza per identificare i gap e le criticità rilevanti
- Exposed Surface: verifica dell'esposizione generale degli asset e identificazione delle minacce a cui sono esposti;
- Reporting e Roadmap per la remediation: una volta condotto l'Assessment con tutti i controlli accessori previsti, gli analisti definiscono insieme al committente una roadmap di interventi da effettuare per migliorare la propria postura di sicurezza. L'arco temporale totale della roadmap di interventi proposti è flessibile, con step di 12, 24 o 36 mesi.

Costi previsti: linea progettuale atta ad aumentare la consapevolezza euro 14.000,00 oltre IVA; linea progettuale assessment euro 11.000,00 oltre IVA.

Si prevede di avviare il progetto entro il mese di giugno 2024

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.

Tutto ciò premesso, il Relatore propone alla Giunta camerale di stanziare l'importo di euro 40.000,00 oltre IVA a copertura dei servizi sopra descritti, da corrispondere con un anticipo del 20% per entrambe le offerte all'accettazione e, per l'80% rimanente prevedendo l'erogazione a conclusione delle attività nel primo progetto destinato alle imprese e ad

avanzamento lavori nel secondo progetto. Le due offerte saranno oggetto di affidamento diretto tramite M.E.P.A. - Mercato Elettronico della Pubblica Amministrazione, ai sensi dell'art. 50 comma 1 lett. B) del vigente Codice degli Appalti D. Lgs. 36/2023.

LA GIUNTA CAMERALE

Udita l'esposizione del Relatore;

Condivisa la necessità di predisporre specifiche attività specialistiche a favore delle MPMI e di awareness in tema di transizione digitale e cyber sicurezza;

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 ed *awareness* in tema di cyber sicurezza;

Considerato che il Progetto Doppia Transizione Digitale ed Ecologica è attivo per il triennio 2023 - 2025 e che le attività descritte in narrativa saranno realizzate nel periodo maggio 2024 - settembre 2025;

Unanime,

d e l i b e r a

-di stanziare un importo di 40.000,00 oltre IVA a copertura dei servizi specialistici realizzati da Start 4.0 in tema di cyber sicurezza per il periodo maggio 2024 - settembre 2025;

- di imputare l'onere di € 40.000,00 + IVA sul conto 330002 "Interventi Economici Doppia Transizione" al Centro di Costo DD02 "Doppia Transizione;

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

Allegati

Il Presidente
f.to Sig. Luigi Attanasio

Il Segretario Generale
f.to Dott. Maurizio Caviglia

CAMERA DI COMMERCIO INDUSTRIA ARTIGIANATO E AGRICOLTURA GENOVA

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

START4.0

Allegato alla delibera n. 70 del 26.02.2024

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, 17/10/2023

START4.0

PREMESSA

IL CENTRO DI COMPETENZA START 4.0

START 4.0 è un Centro di Competenza (CdC) ad alta specializzazione promosso dal Ministero delle Imprese e del Made in Italy (MIMIT) per facilitare l'adozione di tecnologie abilitanti di Industria 4.0; con il proprio ecosistema di innovazione e presidio tecnologico in crescita, rappresenta uno strumento strategico di supporto a imprese ed Enti per affrontare le sfide della quarta rivoluzione industriale.

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

CONTESTO OPERATIVO

Le Piccole Medie Imprese costituiscono il tessuto produttivo del Paese e, come tale, risultano l'obiettivo primario degli attacchi informatici, anche se persiste l'errata percezione che questo tipo di attacchi abbia principalmente come obiettivo le grandi imprese.

Inoltre, le PMI risultano il principale veicolo attraverso il quale i criminali informatici riescono a colpire e a sottrarre i dati delle grandi aziende.

È necessario, pertanto, che le PMI si dotino di organizzazioni e sistemi che garantiscano la resilienza e la resistenza agli attacchi cyber, pena gravi ricadute sulle attività, la perdita di commesse e le sanzioni previste dalle nuove normative in materia.

A questo contesto si aggiunge un danno di immagine legato alla reputazione e alla credibilità che mina la competitività aziendale.

È pertanto opportuno che le Associazioni del territorio e le istituzioni mettano a disposizione dei loro associati e delle aziende del territorio un lungimirante progetto di Cybersecurity Awareness, riconosciuta come la prima e più significativa arma di difesa per riconoscere le minacce e non cadere in inganno, come evidenziato da ENISA (European Union Agency for Cybersecurity) nel documento "CYBERSECURITY FOR SMES" di giugno 2021.

START4.0

PROPOSTA FORMATIVA

Descrizione del corso:

La digitalizzazione e la connettività hanno creato significative opportunità di business per le PMI anche grazie ad una più efficiente ed ottimizzata gestione delle risorse interne e dei processi aziendali, ma hanno modificano i confini aziendali ed esposto a rischi e minacce significative 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.

Esistono normative cui adeguarsi che il management aziendale deve conoscere e che possono 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. Per questo è necessario dare garanzie ai propri clienti in tema di cybersecurity per potersi assicurare le commesse.

Per rimanere competitivi occorre quindi considerare la Cybersecurity come un vero e proprio asset aziendale su cui i clienti baseranno la propria scelta.

La crescita del numero di attacchi dimostra che la domanda corretta da porsi non è "se" ci attaccheranno ma "quando". Questo corso si pone l'obiettivo di essere la vostra prima forma di protezione.

Per un miglior coinvolgimento dei partecipanti, è previsto un laboratorio formativo finale concepito come una escape room 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 e trovare la combinazione della chiave per uscire dal pulmino.

Si stima una classe con al massimo 30 partecipanti.

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.

START4.0

Metodologia didattica:

Il corso potrà essere erogato da remoto, in presenza o in modalità ibrida sulla base delle esigenze espresse dalla Committenza e dai partecipanti all'attività formativa.

Il Centro di Competenza può mettere a disposizione la piattaforma Webex per l'erogazione a distanza di formazione sincrona.

Le eventuali registrazioni del corso verranno valutate sulla base delle esigenze dei partecipanti.

Gamification per un miglior coinvolgimento dei partecipanti attraverso il laboratorio finale sul Cyber Bus.

Programma del corso:

A. I fondamentali

Cyberspazio

Cybersecurity definizione

Cybercrime

Darkweb

Criptovalute

Blockchain

Mondo IoT e rischi cyber

Trasformazione digitale e importanza del dato

IoT e rischi

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.

START4.0

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

START4.0

ATTIVITÀ DI PROGETTO

Si suggerisce di procedere con un questionario di valutazione ex-ante per verificare le reali necessità dell'audience e il grado di competenze nella materia del corso per poter adeguare i contenuti alla platea di rifermento del corso.

1. Progettazione di dettaglio sulla base delle esigenze formative riscontrate nelle aziende partecipanti
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
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 formative**
- **Tutor di laboratorio**
- **Cyber Bus**

START4.0

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.

START4.0

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

La fatturazione sarà effettuata secondo il secondo piano:

- 30% all'accettazione dell'offerta;
- 70% al termine delle attività previste in offerta.

Il pagamento è stabilito in 30 giorni fine mese data fattura.
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)

TIMBRO E FIRMA DEL CLIENTE
(PRESIDENTE)

START4.0

Alla c. a. Dott. G. Bottino

Dott.ssa Paola Carbone

Spett.le Camera di Commercio di Genova

PROT. N. 2023/433

Genova, 07/12/2023

OGGETTO: Offerta per progetto formativo di Cybersecurity Awareness e Cybersecurity Assessment

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

START4.0

PREMESSA

IL CENTRO DI COMPETENZA START 4.0

START 4.0 è un Centro di Competenza (CdC) ad alta specializzazione promosso dal Ministero delle Imprese e del Made in Italy (MIMIT) per facilitare l'adozione di tecnologie abilitanti di Industria 4.0; con il proprio ecosistema di innovazione e presidio tecnologico in crescita, rappresenta uno strumento strategico di supporto a imprese ed Enti per affrontare le sfide della quarta rivoluzione industriale.

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

La Camera di Commercio di Genova è associata al Centro di Competenza START 4.0 e da anni è partner di riferimento per la realizzazione di progetti di formazione sul territorio finalizzati alla diffusione delle competenze nell'ambito delle tecnologie 4.0 e della trasformazione digitale sicura.

CONTESTO OPERATIVO

Il Centro di Competenza START 4.0 ha elaborato una metodologia denominata Behaviour-based Cybersecurity Training (BbCT) che utilizza per tutti i progetti formativi in ambito Cybersecurity Awareness. La BbCT prende spunto dallo studio dei comportamenti e si basa sull'evoluzione in ambito cyber security e cyber safety degli studi scientifici avviati nei primi anni '70 sugli effetti positivi di feedback e rinforzi.

L'analisi comportamentale applica i principi e le leggi della scienza del comportamento, attraverso l'applicazione di un rigoroso metodo scientifico, ai problemi legati alla sicurezza nella vita lavorativa di tutti i giorni (che si applicano ugualmente alla vita privata di ciascuno di noi).

La BbCT, sfruttando le conoscenze raggiunte dalle scienze comportamentali e applicandole ai contesti della Cyber Security e della Cyber Safety, cerca di anticipare le reazioni degli utenti posti di fronte a stimoli elaborati secondo le tecniche più avanzate di social engineering.

Il modello di riferimento è quello delle conseguenze del comportamento antecedente (anche denominato Modello ABC) uno strumento che aiuta ad esaminare un comportamento per comprenderne meglio le componenti chiave, inclusi gli eventi scatenanti che lo precedono e le conseguenze che ne seguono.

Questo consente anche di indagare come mai, in determinate circostanze, non venga messo in atto un comportamento adeguato impostando strategie correttive che si fondano sull'attivazione e sulla

valorizzazione del potenziale delle persone, ultimo baluardo di difesa in caso di attacco non filtrato dai sistemi di protezione.

Essendo una metodologia data-driven, la BbCT si basa sulla raccolta di informazioni tramite una piattaforma di formazione correttamente configurata atta ad individuare le aree aziendali che necessitino di miglioramento, effettuare misurazioni oggettive e proporre azioni formative che si concentrino più sugli aspetti cognitivo-comportamentali che su aspetti legati alle competenze.

Il tutto avendo cura di creare un ambiente in cui il feedback dell'utente sia il vero scopo finale da raggiungere e l'attivazione dello stesso venga percepito come l'elemento utile e benefico alla salvaguardia della realtà in cui è inserito. È dimostrato, infatti, che l'effetto dei rinforzi positivi porti ad interiorizzare il comportamento desiderato assicurandone l'attivazione in modo stabile e duraturo nel tempo.

Dal punto di vista operativo, un progetto formativo di Cybersecurity Awareness prevede tre principali macro-fasi di attività che seguono il ciclo: valutare, istruire, rinforzare, misurare con modalità, tempi ed obiettivi differenti che si basano sull'uso di piattaforme formative abilitate da algoritmi di AI, in questo caso si propone di utilizzare la piattaforma di Cyber Guru, più vicina a rispondere a bisogni ed esigenze della Camera di Commercio di Genova.

Il progetto sarà seguito in ogni fase da PM di Start 4.0 e prevede tutti i livelli di governance di un progetto tecnico a tutti gli effetti con avanzamenti SAL quindicinali, Status meeting bimestrali e Steering Committee semestrale. Per ogni meeting sarà stilata una minuta con le azioni da svolgere entro il meeting successivo.

Cyber Guru offre una piattaforma formativa di Cyber Security Awareness di grande efficacia, finalizzata a trasformare il fattore umano da anello debole della catena difensiva a prima linea di difesa contro il cybercrime.

Grazie alla sua piattaforma SaaS, interamente progettata e sviluppata in Italia, e ai suoi percorsi formativi basati su un approccio metodologico esclusivo, consente alle organizzazioni pubbliche e private di formare e addestrare i propri dipendenti ad un utilizzo corretto delle tecnologie digitali, aumentando il livello di protezione di individui e organizzazioni.

La piattaforma Cyber Guru è stata progettata e realizzata per massimizzare l'efficacia del contributo formativo, minimizzando l'effetto dispersivo e annullando i costi di gestione. Questo ha contribuito a far sì che oggi sono circa 400 le aziende che hanno scelto la piattaforma di training di Cyber Guru con oltre 650.000 utenti coinvolti attivamente, e più di 5.000.000 h di lezioni fruite.

La piattaforma si compone di tre soluzioni:

1. **Cyber Guru Awareness** (CGA): piano di formazione in modalità "e-learning" composto da 12 moduli tematici all'anno per tre anni che successivamente possono confluire nel cyber campus per il mantenimento e l'aggiornamento continuo della conoscenza cyber acquisita.

2. **Cyber Guru Phishing** (CGP): sistema di apprendimento esperienziale fortemente automatizzato, che ha lo scopo di aumentare la resistenza dell'organizzazione agli attacchi Phishing e Smishing e che produce risultati efficaci grazie alla sua metodologia avanzata, pensata per mantenere "allenate" due importanti caratteristiche difensive umane: la **prontezza** e la **reattività.**

3. **Cyber Guru Channel** (CGC): percorso di formazione basato su una metodologia induttiva costituito da episodi video di alta qualità, realizzati con tecniche di produzione avanzata tipiche delle serie TV. Grazie a tecniche di storytelling particolarmente coinvolgenti si sviluppa negli utenti la consapevolezza del rischio cyber con 12 episodi per ogni annualità.

1. Soluzione Cyber Guru Awareness (CGA)

Cyber Guru Awareness si fonda su metodologie di formazione avanzate che tengono conto delle modalità di apprendimento digitale che risultano maggiormente efficaci su soggetti adulti. CGA è stato progettato per coinvolgere tutta l'organizzazione in un percorso di apprendimento educativo e stimolante, che si caratterizza per un approccio "a rilascio costante e graduale":

- la formazione impegna il partecipante per pochi minuti a settimana, ma con un percorso diviso in annualità, che mantiene elevata l'attenzione del partecipante ogni qualvolta interagisce con le tecnologie digitali;
- tutte le lezioni sono disponibili in formato multimediale, con la possibilità di fruire dei contenuti sia in formato video sia in formato testuale;
- la fruizione è possibile da differenti tipologie di device (PC, smartphone, tablet) ed in qualsiasi orario;
- il linguaggio utilizzato risponde a un criterio divulgativo, pensato per essere efficace su personale con differenti livelli di competenza sui temi della Cyber Security;
- ogni lezione è corredata da test di valutazione del livello di apprendimento;
- il corso usa una metodologia di gamification, corredata da premi e riconoscimenti, che stimola l'apprendimento e premia l'impegno dei discenti a prescindere dal loro livello di partenza;
- è prevista la possibilità di inserire gli utenti in team, stimolando una sana competizione e riducendo conseguentemente l'esigenza di dover intervenire maggiormente con azioni atte a sollecitare la partecipazione;
- in una logica di efficientamento dei processi cognitivi ogni modulo formativo è auto-consistente e affronta uno specifico argomento;
- i moduli formativi vengono erogati con la frequenza standard di uno ogni mese e sono costituiti da 3 lezioni con relativi test e documenti di supporto e approfondimento.

La soluzione gestisce con un **forte livello di automatismo** il piano di studi per ogni utente, trasferendo in tal modo al contesto della formazione a distanza l'applicazione dei principi cardine dell'apprendimento che ne determinano il successo nei contesti tradizionali delle scuole ed università. Applicando concetti consolidati in andragogia e nella **Teoria del Carico Cognitivo** sviluppata da John Sweller, tutti i contenuti ed i concetti formativi sono posti in una sequenza

ottimale che riduce l'effetto di affaticamento e ottenere il massimo rendimento dai meccanismi di memorizzazione dell'essere umano.

Cyber Guru Awareness applica i principi della **progressione**, del **mantenimento** e dell'**aggiornamento**: agli utenti che hanno raggiunto la conclusione del percorso di apprendimento in ambito Cyber la soluzione propone moduli appositamente sviluppati per mantenere alto il livello di conoscenza acquisito e per aggiornare le nozioni al variare delle tecniche di attacco e delle minacce. I moduli in questione assumono la forma di Serious Game e video interattivi con logiche "learning by doing".

2. Soluzione Cyber Guru PHISHING (CGP)

Cyber Guru Phishing (di seguito CGP) è una soluzione innovativa di training anti-phishing e anti-smishing che produce risultati efficaci grazie alla sua particolare metodologia di addestramento esperienziale. Avvalendosi di un'**automazione spinta e di un algoritmo proprietario di machine learning**, CGP si rivolge a tutto il personale, a prescindere dal livello di competenza cyber dell'utente. Essa consente di **mantenere "allenate"** due importanti caratteristiche difensive umane: la **prontezza** e la **reattività**. Questo risultato viene raggiunto mediante la simulazione di attacchi di Phishing e Smishing cui vengono sottoposti tutti gli utenti con un ritmo definibili dall'organizzazione e che normalmente si attesta su un invio al mese per ogni utente.

Il motore di gestione è in grado di adattare le simulazioni in modo automatico, **riducendo l'intervento umano alla sola fase di approvazione della campagna**. I messaggi e SMS scelti dal sistema hanno differenti argomenti e livelli di difficoltà, calibrati in funzione delle reali capacità di ognuno di essi, e sono inviati agli utenti in giorni e orari differenti per minimizzare l'effetto "passaparola".

L'utente che dovesse cadere nella simulazione è accompagnato tramite una specifica "landing page" dinamica verso un percorso progressivo di apprendimento nel quale riceverà indicazioni utili per affinare la sua capacità di riconoscimento degli attacchi.

La soluzione dispone di **strumenti di visualizzazione grafica dei risultati e di indagine avanzati**, un vero e proprio strumento di business intelligence che permette alle figure responsabili di osservare la progressione degli utenti e individuare aree dell'organizzazione più vulnerabili, sulle quali è possibile attivare percorsi di remediation automatici o manuali.

CGP si propone pertanto come la naturale integrazione ai programmi formativi della linea Cyber Guru, aumentando la reattività dell'individuo di fronte ad attacchi basati su tecniche di Phishing. Considerando che i maggiori pericoli per la sicurezza delle organizzazioni sono "in agguato" nelle caselle e-mail dei loro dipendenti e collaboratori, le simulazioni di attacco Phishing, messe in atto da Cyber Guru Phishing, "personalizzate" sulla base delle caratteristiche peculiari di ogni singolo utente, preparano dipendenti e collaboratori a modificare i comportamenti e ad individuare con prontezza mail di phishing.

START4.0

3. Soluzione Cyber Guru CHANNEL (CGC)

Cyber Guru Channel è una soluzione che pubblica su base mensile video di alta qualità, della durata di 5-8 minuti l'uno, che presentano casi di attacchi/frodi cyber improntati su casi e tecniche reali. I format utilizzati sono diversi (Cyber Detective, Break News, Sit-Com). Ogni video è dotato di un documento di approfondimento che analizza più nel dettaglio il tema cyber affrontato nel video.

L'intera struttura degli episodi è progettata per ottenere due importanti risultati lavorando sulla componente psicologica degli utenti:

- **Superare il pregiudizio diffuso tra i non addetti ai lavori del "a me non può accadere"**. Per mezzo dell'immedesimazione con i protagonisti, l'utente si renderà conto in modo diretto e naturale di quanto possa essere facile diventare vittima o inconsapevole complice di attacchi cyber.
- **Stimolare l'attenzione verso argomenti non sempre considerati "facili"** utilizzando tecniche di narrazione multimediale che tutti riconoscono e verso le quali si è predisposti ad un ascolto attivo.

Anche in questo caso la soluzione **gestisce in modo automatico** la distribuzione degli episodi con un ritmo di uno al mese. Gli episodi di Cyber Guru Channel non richiedono il superamento di un test per avanzare nel percorso di apprendimento. Oltre al problema strettamente tecnico però, il progetto ha necessità di una forte progettazione dal punto di vista della formazione nella scelta delle domande di assessment, nella definizione delle campagne di phishing e nell'assegnamento dei moduli di formazione (con tanto di relativo assegnamento automatico).

A completamento del progetto, risulta necessario, al termine delle attività previste di cui sopra, sviluppare un'attività di cybersecurity assessment di alto livello, volta a valutare ulteriori dettagli di rischio sulla configurazione di alcuni sistemi fondamentali della CCIAA.

Start 4.0 ha le competenze per poter supportare la Camera di Commercio nella definizione dell'interoprogetto formativo.

PROPOSTA PROGETTUALE

La presente proposta prevede la definizione e lo sviluppo del progetto formativo, a partire dal seguente nucleo di attività:

1. Project management del progetto formative con metodologia BbCT;
2. Definizione e schedulazione del/i questionario/i di assessment;
3. Definizione e schedulazione della/e campagna/e di phishing/smishing;
3. Definizione della reportistica per assessment/campagne di phishing-usb/risultati dei training;
4. Definizione del percorso formativo con la selezione dei corsi in termini di contenuti e di tipologia per la massimizzazione del risultato formativo mantenendo un impegno dei partecipanti contenuto ma continuo e costante;

5. Project management del progetto formativo;
6. Piattaforma di formazione con 120 licenze per coprire le esigenze della Camera di Commercio;
7. Supporto tecnico per tutta la durata del progetto sulla piattaforma;
8. A complemento del progetto formativo verrà svolta un'attività di cybersecurity assessment di alto livello per la verifica della rete della CCIAA, un'analisi del deep web e del web per verificare l'esposizione online degli utenti della Camera di Commercio, eventuali email compromesse ed altre vulnerabilità che richiedono interventi urgenti di adeguamento.

ATTIVITÀ DI PROGETTO

- Meeting di progetto con SAL quindicinale, Status meeting bimestrale e Steering Committee semestrale;
- Scelta domande per contenuto e tipologia e creazione di N° 2 Assessment/questionari (1 inizio percorso e 1 fine percorso);
- Definizione template e contenuto per la creazione N° 3 Campagne di phishing (1 a quadrimestre);
- Definizione template e contenuto per la creazione N° 2 Campagne di smishing (1 a semestre);
- Assegnazione prima manuale e poi automatica di 10 corsi/anno sulla base dei risultati delle campagne di assessment e di phishing;
- Creazione della reportistica per ogni tipologia di attività: assessment, campagne di phishing e smishing sui 20 cellulari aziendali, risultati di fruizione del training;
- Project management del progetto formativo;
- Security Assessment cosiddetto Esteso che unisce il tradizionale Security Assessment a una serie di ulteriori check sulla configurazione di alcuni sistemi fondamentali della CCIAA.

Le attività previste durante quest'ultima fase, si compongono di:

1. Interview: analisi del framework più adatto per la Committenza per identificare i gap e le criticità rilevanti tra quelli elencati:
    i. NIST Cybersecurity Framework (CSF);
    ii. ISO/IEC 27001;
    iii. GRC – Governance Risk Compliance;
    iv. Framework Nazionale di Cybersecurity e Data Protection;
    v. NERC Critical Infrastructure Protection (CIP) ;
    vi. ISA/IEC 62443;
    vii. ISO/SAE 21434.

START4.0

2. Exposed Surface: verifica dell'esposizione generale degli asset e identificazione delle minacce a cui sono esposti;
3. Reporting e Roadmap per la remediation: una volta condotto l'Assessment con tutti i controlli accessori previsti, gli analisti definiscono insieme alla CCIAA una roadmap di interventi da effettuare per migliorare la propria postura di sicurezza. L'arco temporale totale della roadmap di interventi proposti è flessibile, con step di 12, 24 o 36 mesi.

Un'opzione alternativa alla fase due,"exposed surface", potrebbe consistere nella valutazione dell'implementazione di ulteriori attività, tra cui: 2.bis (in alternativa alla fase 2 prevista dal piano precedente) User Behavior: verifica sulla preparazione effettiva della popolazione aziendale sulla cybersecurity; (tale attività potrebbe favorire l'implementazione di un programma di formazione o campagne test)

- AD Admin: controllo degli account privilegiati presenti sull'Active Directory;
- Firewall Assurance: controllo sulla configurazione e sulle regole impostate sui firewall;
- DNS Verify: verifica delle query DNS, alla ricerca di potenziale traffico dannoso;
- Vulnerability Management: controllo e rilevazione delle vulnerabilità presenti nell'infrastruttura;

Per misurare l'esposizione cyber iniziale e target del Cliente, rappresentativo della maturità in tema di sicurezza, si userà il parametro **Security Maturity Factor (SMF)**.

Tale indice è calcolato individuando gli aspetti critici che influenzano la postura di sicurezza, attribuendo loro un peso a seconda della loro gravità. L'SMF rappresenta una valutazione quantitativa sintetica di tali aspetti.

L'SMF viene calcolato allo startup del servizio per valutare la situazione di partenza e per identificare il target desiderato alla fine del percorso. Periodicamente, per tutta la durata del servizio, il SMF verrà ricalcolato per mostrare i progressi conseguiti.

TEMPISTICHE DI PROGETTO

Il progetto di Cybersecurity Awareness e cybersecurity assessment avrà la durata di **1 anno** e verrà concordata in dettaglio con la Committenza nel suo piano di attività in modo da accompagnare nel cambiamento impattando il meno possibile sull'operatività del cliente finale.

È importante sottolineare che la temporizzazione delle attività descritte è puramente indicativa poiché alcune attività potrebbero essere anticipate e posticipate dalla Committenza sulla base di quanto ritenuto più opportuno per la miglior riuscita del progetto.

L'inizio delle attività con il kick-off meeting è da intendersi a 15 giorni dall'accettazione della presente offerta.

La durata del progetto richiede inoltre la completa disponibilità del cliente a fissare tempestivamente gli incontri necessari a raccogliere le informazioni utili al progetto e a dare riscontro alle eventuali ulteriori richieste.

RISORSE DI PROGETTO

La figura operativa messa a disposizione dal Centro di Competenza START 4.0 che seguirà il progetto nelle fasi descritte, sarà la seguente:

- **Project & Training Manager**
- **Tutor formativo**
- **Cybersecurity expert**

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 di cybersecurity awareness è di **Euro 14.000 oltre IVA.**

Il costo delle attività di cybersecurity assessment è di **Euro 11.000 oltre IVA.**

Il costo totale delle attività è pari ad Euro 25.000 oltre IVA e prevede il piano formativo di cybersecurity awareness e il piano di cybersecurity assessment con le attività descritte ai punti 1,2 e 3 (o il alternativa le attività previste ai punti 1, 2bis e 3).

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.

START4.0

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

La fatturazione sarà effettuata secondo il secondo piano:

- 30% all'accettazione dell'offerta;
- 70% al termine delle attività previste in offerta;

Il pagamento è stabilito in 30 giorni fine mese data fattura.

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.

START 4.0

ACCETTAZIONE OFFERTA

DATA ACCETTAZIONE:

START 4.0
(PRESIDENTE)

TIMBRO E FIRMA DEL CLIENTE
(PRESIDENTE)