1ª Edizione

In qualità di Provider

asstra service

Evento realizzato in collaborazione con il Partner Scientifico

FormazioneMaggioli

Organizza il Corso di Formazione:

LA CYBERSECURITY NEL SETTORE DEL TRASPORTO COLLETTIVO

Programma 2022

Aprile→ 4, 6, 11, 12

Corso in modalità online

Con il supporto di:

asstra

PRESENTAZIONE E FINALITA'

1. OBIETTIVI DEL CORSO DI FORMAZIONE

Il mondo che ci circonda sta cambiando molto velocemente. Si sta passando da una gestione manuale a quella automatizzata e con l'aiuto delle tecnologie questo cambiamento sta avvenendo sempre più velocemente.

Il contesto sta evolvendo verso nuovi "confini" e con la possibilità di connettere le catene produttive ad internet, tutto ormai è "controllabile" tramite dispositivi elettronici e da "internet".

Nel pieno di questa rivoluzione digitale, tutte le aziende comprese quelle del trasporto pubblico locale, sono chiamate ad un cruciale cambiamento operativo di gestione e processi, trovandosi a migrare e/o sviluppare su sistemi informatici la maggior parte delle attività e dei dati aziendali.

La digitalizzazione, però, se da un lato offre immense possibilità di sviluppo, sistemi efficaci di gestione aziendale e semplificazione dei servizi, dall'altro necessita di giuste tecnologie e di adeguate implementazioni di procedure di sicurezza informatica.

All'interno di questo percorso, saranno dunque affrontati sia aspetti di innovazione tecnologica sia di sicurezza informatica e complessità normative crescenti (anche per i propri fornitori), attraversando standard di riferimento, best practice e casi pratici.

Partendo dalle basi, saranno discussi alcuni scenari per la corretta gestione della sicurezza informatica nel settore industriale e qualche caso studio di attacco informatico che ha creato non pochi disservizi ad aziende ed infrastrutture critiche.

Infine, al termine del percorso, saranno affrontati anche argomenti come la *digital trasformation* nel settore trasporti e gli standard di riferimento in ambito cyber security con particolare attenzione agli aspetti di protezione e mitigazione del rischio.

Il corso è rivolto a:

- ✓ rappresentanti delle imprese di Trasporto Pubblico che si occupano a vario titolo della gestione di tutti gli aspetti informatici e digitali;
- ✓ rappresentanti legali delle imprese di Trasporto Pubblico che si occupano a vario titolo degli aspetti normativi legati alla cybersecurity;
- ✓ rappresentanti dei Servizi ICT delle imprese di Trasporto Pubblico;
- ✓ liberi professionisti del settore.

2. STRUTTURA E CARATTERISTICHE DEL CORSO DI FORMAZIONE

L'intervento formativo è articolato in **4 moduli da 4 ore ciascuno**, per una durata complessiva di **16 ore**.

La frequenza alle lezioni è obbligatoria, in quanto requisito essenziali ai fini dell'ottenimento dell'attestato di partecipazione del corso intero o dello specifico modulo.

Alla fine del corso o dello specifico modulo sarà rilasciato un attestato di frequenza da ASSTRA Service, certificata nell'ambito della ISO 9001:2015 ai sensi della certificazione EA 37 e ES 35, utile ai fini della dimostrazione dell'aggiornamento ed arricchimento delle competenze professionali, in merito ai temi trattati. **È possibile seguire anche solo alcuni moduli per i quali sarà rilasciato l'attestato di frequenza, mentre per ottenere i CFP per gli Ingegneri è necessario seguire l'intero corso.**

Ai fini del necessario accertamento dell'efficacia formativa dei partecipanti, alla fine di ogni modulo è previsto un TEST SPECIFICO per l'autovalutazione dell'apprendimento costituito da 10 domande a risposta multipla, di cui una esatta, con l'obbligo di almeno il 75 % di risposte esatte.

I partecipanti interessati dovranno, inoltre, esprimersi su appositi modelli preimpostati sulla qualità percepita su alcuni aspetti del corso (organizzazione, docenti).

L'avvio del corso è subordinato alla iscrizione di almeno 15 partecipanti mentre per una efficace partecipazione allo stesso l'aula sarà composta da non più di 25 partecipanti.

Saranno accettate le prime 25 iscrizioni in ordine di arrivo.

3. PARTNER SCIENTIFICO: GRUPPO MAGGIOLI

Il corso sarà tenuto da Formazione Maggioli è la divisione del Gruppo Maggioli che organizza corsi e convegni rivolti alla Pubblica Amministrazione, ai liberi professionisti e alle aziende.

Da oltre un secolo il Gruppo Maggioli è riconosciuto come la principale organizzazione aziendale impegnata in un ruolo guida per chi opera nelle Amministrazioni Pubbliche e nelle professioni ad esse collegate. Attraverso le singole Divisioni che la compongono, il Gruppo Maggioli offre quotidianamente alla Pubblica Amministrazione una completa serie di prodotti, servizi, strumenti e soluzioni che contribuiscono al miglioramento dell'efficacia e dell'efficienza gestionale della realtà pubblica.

L'elevato livello dei docenti, il giusto equilibrio tra teoria e pratica, i pregevoli materiali didattici, sono il valore aggiunto che contraddistingue le oltre 800 iniziative di formazione.

Da oltre 30 anni i corsi e convegni Maggioli sono riconosciuti ed apprezzati per il rigore scientifico e il taglio operativo. Ogni anno oltre 20.000 amministratori, dirigenti e funzionari della Pubblica Amministrazione, liberi professionisti e manager di aziende private affidano la loro crescita professionale ai migliori esperti del settore scelti tra i dirigenti della P.A., docenti universitari, magistrati ordinari e amministrativi, avvocati dello Stato e specialisti di comprovata professionalità.

4. DOCENTI

Il corso si avvale di docenti di comprovata esperienza, provenienti dal Ministero delle Infrastrutture e della Mobilità Sostenibili, dal mondo accademico, e di esperti del settore. I docenti del corso sono indicati nel programma dettagliato ed è allegato un breve CV.

5. MATERIALE DIDATTICO

Il materiale didattico, distribuito a tutti i partecipanti, è costituito dalle diapositive appositamente predisposte dal docente.

6. FINANZIAMENTI

Il corso è finanziabile attraverso i FONDI INTERPROFESSIONALI per la formazione continua (es. Fonservizi e altri Fondi). Per chiarimenti su come accedere a questi fondi è possibile rivolgersi in ASSTRA Service al Dott. Domenico Scalfaro (3299026950; e-mail scalfaro@asstra.it).

7. CFP ORDINE INGEGNERI

Per il Corso, relativamente ai partecipanti con iscrizione all'ORDINE PROFESSIONALE DEGLI INGEGNERI, è stata presentata presso il CNI richiesta di accreditamento per il successivo rilascio dei Crediti Formativi Professionali (CFP). **È obbligatorio seguire tutto il corso per la sua durata.**

8. ISTRUZIONI PER IL COLLEGAMENTO

Per l'accesso al corso, ASSTRA Service provvederà ad inviare ai partecipanti, una volta attivato il corso, il link e le istruzioni per collegarsi VIA INTERNET.

DOCENTI
Claudia CIAMPI Senior ICT Security Manager, Technology Auditor, Regulatory Compliance e Risk Management Expert con più di 20 anni di esperienza professionale, ha ricoperto ruoli operativi, strategici e di alta responsabilità in contesti aziendali complessi presso primarie organizzazioni nazionali/internazionali e pubbliche amministrazioni centrali/locali. Subject Matter Expert in Information Security & Data Protection con ampia e documentata esperienza nell'applicazione delle normative nazionali, europee ed internazionali in vari settori di business. Ha ricoperto i ruoli di CISO e di Privacy Officer per grandi e medie imprese. Consolidata esperienza come Project Manager, ha gestito e guidato incarichi di Audit globali e regionali e progetti complessi di ICT Security & Compliance Governance nei settori bancario, assicurativo, sanitario, servizi ICT e TLC e della pubblica amministrazione. Esperto di Sistemi di Gestione Integrati e Senior Assessor su ISO 27001, 27017, 27018, 22301, 20000, 9001, 14001, 37001, SA8000, PCI DSS, SOX, COBIT, ITIL. Docente per Master universitari ha scritto numerosi articoli riguardo la protezione dei dati, i sistemi di gestione della sicurezza delle informazioni, le metodologie di analisi e gestione dei rischi ICT e la business continuity.
Gerardo COSTABILE Fondatore e CEO di DeepCyber srl, società del Gruppo Maggioli specializzata in cyber security. Nella sua ultraventennale esperienza, è stato Chief Security Officer presso British Telecom Italy e Head of Security & Safety a Fastweb S.p.A (Swisscom AG Group), fondatore e responsabile della practice di Forensic Technology & Discovery Services (FTDS) all'interno del Fraud Investigation & Dispute Services (FIDS) di EY (Italy e EMEIA Western Zone). Per alcuni anni CISO (Chief Information Security Officer) di Poste Italiane e cybercop del team di Antifraud & Cybercrime della Guardia di finanza di Milano. Professore a contratto alle Università degli Studi La Sapienza, Foggia e San Raffaele e membro della NY Electronic Crime Task Force degli Stati Uniti. Inventore, nel 2020, di un brevetto sulla valutazione delle vulnerabilità nei sistemi industriali (IIot, ICS, Scada).
Giorgio PIZZI Dirigente della Divisione 4 della Direzione generale per il trasporto pubblico locale, la mobilità pubblica sostenibile e gli interventi nel settore per il trasporto ferroviario regionale. Laureato in Ingegneria elettronica, negli anni ha ricoperto diversi ruoli all'interno del Ministero, ed è stato di recente nominato coordinatore della segreteria dell'Osservatorio del TPL dove sovrintende alle attività di rilevazione dei dati relativi alle imprese del trasporto pubblico locale ed alla fase di reingegnerizzazione della piattaforma informatica. Ha uno spiccato interesse per il management, l'economia delle piattaforme, la trasformazione digitale, in particolare le applicazioni delle nuove tecnologie nel settore dei trasporti ed i loro "risvolti", in tema di cybersecurity, big data, piattaforme digitali. È stato relatore e docente in numerosi convegni nazionali e internazionali. Autore di diverse pubblicazioni relative al tema della Cybersecurty nei sistemi di trasporto.
Francesco SCHIFILLITI Esperto in information security, digital forensic e cyber threat intelligence per importanti compagnie. È stato Manager della practice di Forensic Technology & Discovery Services (FTDS) all'interno del Fraud Investigation & Dispute Services (FIDS) di EY. Specializzato in Malware e Memory Analysis, OSINT, Tecniche per la Intelligence Investigation, Incident Responding Techniques e Cyber Threat Intelligence. Laureato in Informatica all'Università di Catania e docente in corsi e master di digital e malware forensics.

PROGRAMMA

MODULO 1 – Quadro di riferimento normativo MODALITÀ ONLINE*		
4 aprile 2022		
9,00	Appello per la registrazione dei partecipanti ed apertura del corso	*ASSTRA SERVICE*
9,15/ 13,15	• Normativa nazionale ed europea sulla cyber security: lo stato dell'arte e applicazioni pratiche • La gestione delle terze parti: outsorcing e cyber security. • Panoramica sui principali standard e come utilizzarli a supporto dell'information Security (ISO 27001, Misure minime AGID, Framework Nazionale per la Cybersecurity, OWASP, Cloud Control Matrix, Mitre Attack) • Elementi da considerare in una Linea Guida per la Security by design e by default	**Dott.ssa Claudia Ciampi** *Senior ICT Security Manager, Technology Auditor, Regulatory Compliance e Risk Management Expert*
13,15	TEST SPECIFICO per autovalutazione apprendimento	
13,45	Conclusione Modulo 1	

***

MODULO 2 – Organizzazione e Fattore umano MODALITÀ ONLINE*		
6 aprile 2022		
9,00/ 13,00	• I dieci step della cyber security nelle organizzazioni • Il fattore umano nella cyber security • Risk Identification, Risk Assessment, Risk Management e Risk Control e Monitoring • Sicurezza delle reti: cenni	**Dott. Gerardo Costabile** *Fondatore e CEO di DeepCyber srl*
13,00	TEST SPECIFICO per autovalutazione apprendimento	
13,30	Conclusione Modulo 2	

***

*** Durante tutto il corso sarà presente il Tutor Asstra Service per la verifica delle presenze.**

MODULO 3 – Vulnerabilità, Sicurezza e Contromisure MODALITÀ ONLINE*		
11 aprile 2022		
9,00/ 13,00	• Sicurezza delle reti: introduzione • Minacce, Vulnerability management e possibili contromisure	**Dott. Gerardo Costabile** e **Dott. Francesco Schifilliti** *Information security, digital forensic e cyber threat intelligence*
13,00	TEST SPECIFICO per autovalutazione apprendimento	
13,30	Conclusione Modulo 3	

***

MODULO 4 – Sistemi di controllo e Analisi del rischio MODALITÀ ONLINE*		
12 aprile 2022		
9,00/ 12,00	• Operational technology, sistemi di controllo nei sistemi di trasporto e loro vulnerabilità • Architettura e superficie di attacco di alcuni sottosistemi • Integrazione della cybersecurity nell'analisi del rischio per la safety	**Ing. Giorgio Pizzi** *Ministero delle Infrastrutture e della Mobilità Sostenibili*
12,00	TEST SPECIFICO per autovalutazione apprendimento	
12,30	Conclusione Modulo 4	

12,30/ 13,30	• Caso applicativo	

*** Durante tutto il corso sarà presente il Tutor Asstra Service per la verifica delle presenze.**