CODICE ATTIVITÀ 09AN21

CORSO DI FORMAZIONE

«Sicurezza Informatica e CyberSecurity»
LIVELLO INTERMEDIATE

4/8/10/11 giugno 2021, in modalità telematica

CONSORZIO INTERUNIVERSITARIO SULLA FORMAZIONE

CoInFo

La proposta formativa: obiettivi e destinatari

Il Corso di formazione si propone di definire i profili di sicurezza dei componenti ICT della Pubblica Amministrazione con particolare riferimento alle amministrazioni universitarie. A valle di una specifica analisi del rischio, si forniranno i principali riferimenti tecnici e normativi che le pubbliche amministrazioni devono affrontare anche rispetto alla prevenzione e al trattamento degli incidenti di sicurezza informatica. Contestualmente si identificheranno gli attuali scenari in funzione dello stato dell'arte ICT, riguardo agli obblighi di sicurezza previsti dal Regolamento UE 2016/679 – GDPR, con l'obiettivo di fornire indicazioni per il contenimento dei rischi e le misure minime ed idonee in riferimento alla normativa nazionale ed europea. Sono previsti due diversi livelli di approfondimento uno introduttivo alla problematica (Basic) e uno di approfondimento (Intermediate).

Il Corso di formazione è rivolto a tutto il personale dipendente delle Università italiane interessato ai temi in oggetto.

La struttura del percorso formativo

Il Corso di formazione, erogato interamente a distanza (tramite la piattaforma di Microsoft Teams) ha una durata di **12 ore di formazione**, distribuite in 4 giornate di 3 ore ciascuna, con il seguente orario: 9.30 – 12.30.

SESSIONE FORMATIVA

Social Engineering (es. Phishing). I Ransomware.

Social Engineering. Il Phishing e lo Spear phishing:: esempi e possibili tecniche di difesa. Link ingannevoli/malevoli. Tecniche di OSINT (Open Source Intelligence). Il phishing attraverso le PEC. Ransomware. Attacchi famosi: da WannaCry a NotPetya. Come difendersi dai Ransomware: la prevenzione. Cosa fare se siamo stati colpiti da un ransomware: le opzioni possibili. Implicazioni giuridiche per le vittime dei ransomware: profili di responsabilità derivanti dal pagamento di riscatti. Responsabilità per il dipendente che causa un attacco ransomware aziendale

4 giugno 2021

h. 9.30-12.30

La struttura del percorso formativo

SESSIONE FORMATIVA

La vulnerabilità delle e-mail.

Attacchi attraverso la posta elettronica. L'importanza della protezione del proprio account e-mail. Business Email Compromise (BEC). Le truffe "The Man in the Mail" e "CEO fraud". Spoofing. Gli strumenti informatici per proteggersi dallo spoofing: SPF, DKIM e DMARC. La crittografia dell'e-mail: PEC e posta crittografata: caratteristiche, utilizzi e differenze. Come funziona e come si usa la PGP (Pretty Good Privacy).

8 giugno 2021

h. 9.30-12.30

La struttura del percorso formativo

SESSIONE FORMATIVA

Password e Autenticazione forte (2FA, SCA).
Definizione di password sicure. Le domande di (in)sicurezza. I Password Manager. Il Password management nelle aziende. L'autenticazione a due fattori (MFA: Multi factor authentication).

Panoramica sulle principali tecniche di cyber attacco.
Gli attacchi DDoS e le Botnet. I rischi dell'IoT (Internet delle cose) in ambito professionale. APT (Advanced Persistent Threat). Attacchi "man-in-the-middle". Il protocollo HTTPS. I Keylogger.

10 giugno 2021

h. 9.30-12.30

La struttura del percorso formativo

SESSIONE FORMATIVA

I rischi aziendali.
La “deperimetralizzazione”: il “Teorema del Fortino”. Il pericolo arriva soprattutto dall’interno. I rischi causati dagli utenti interni: malicious insider, utenti compromessi ed accidentali. I rischi dello Shadow IT. I pericoli generati dallo Smart Working. Il desktop remoto (RDP): quando serve e come utilizzarlo. Le VPN (Virtual Private Network): quali scegliere e come impostarle. Proteggere la privacy nelle riunioni online: le misure da adottare nell’uso delle piattaforme di Web meeting. Come gestire correttamente il Backup. NAS e sistemi RAID: cosa sono e come usarli per conservare in sicurezza i nostri dati. L’importanza degli aggiornamenti di sicurezza. Utilizzo e limiti degli Antivirus. Vulnerability Assessment e Penetration Test.

11 giugno 2021

h. 9.30-12.30

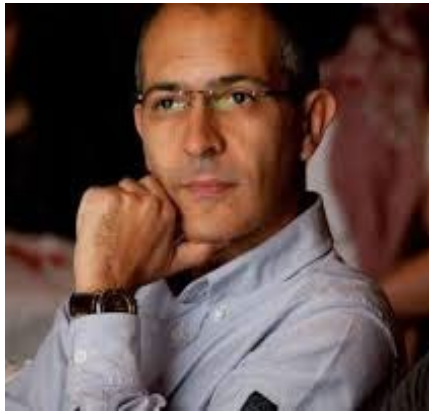
VALUTAZIONE FINALE

30 minuti a disposizione

I relatori

Prof. Sebastiano BATTIATO, Università degli Studi di Catania

Sebastiano Battiato è nato a Catania nel 1972. Ha conseguito la Laurea in Scienze dell'Informazione (summa cum laude) nel 1995 e il dottorato di Ricerca in Matematica Applicata ed Informatica nel 1999. Dal 1999 al 2003 ha coordinato e diretto il gruppo di ricerca "Imaging" c/o STMicroelectronics a Catania. Dal 2004 presta servizio presso il Dipartimento di Matematica ed Informatica dell'Università di Catania come ricercatore (fino al 2010) da Professore Associato (fino al Settembre 2016) e da Professore Ordinario in Informatica (dal 1 Ottobre 2016). I suoi interessi di ricerca includono il miglioramento di qualità e la compressione di segnali multimediali, i sistemi di imaging legati al mondo embedded, il multimedia forensics e la Computer Vision applicata in contesti industriali e consumer. Delegato del Rettore alla didattica corsi Post-Laurea e Dottorato dal 2013 al 2016. Membro del Comitato Esperti Terza Missione (CETMB) per conto dell'ANVUR (biennio 2015-2016). Presidente del corso di Studi in Informatica triennale dell'Università di Catania dal 2012 al 2017. Dal 2017 riveste il ruolo di coordinatore scientifico del Dottorato in Informatica dell'Università degli Studi di Catania (XXXIII ciclo). Dal 2014 Scientific Advisor della startup ParkSmart srl. Dal 2016 è Founder e Scientific Advisor di iCTLab - spin-off dell'Università di Catania che opera nel campo della Digital Forensics.



Ing. Oliver GIUDICE, iCTLab

Oliver GIUDICE è PhD in informatica con specializzazione nello studio di applicazioni avanzate di Multimedia Forensics che vanno dalla ricostruzione della storia delle immagini digitali all'automatizzazione delle analisi balistiche forensi. Co-Founder di iCTLab SRL spin-off dell'Università di Catania e ricercatore informatico presso la Banca d'Italia, svolge seminari nel settore dell'informatica forense in ambito accademico nazionale e internazionale.

L’approccio del Percorso

Si riportano, a seguire, i tratti caratterizzanti del Corso di formazione:

METODOLOGIA DIDATTICA	L’azione formativa sarà condotta tramite webinar in diretta streaming. La piattaforma utilizzata per l’erogazione del Corso di formazione sarà Microsoft Teams.
VALUTAZIONE FINALE	Al termine del Corso di formazione è prevista una **valutazione finale.** Potranno accedere alla valutazione finale coloro che avranno frequentato non meno dell’80% del monte ore di formazione totale. La prova sarà svolta on-line, il test di valutazione sarà composto da 10 quesiti a risposta multipla vertenti sugli argomenti trattati. Il superamento della prova sarà certificato mediante il rilascio di un **attestato**.
IL COORDINAMENTO	Il coordinamento progettuale è affidato al **Dott. Armando CONTI**, Università degli Studi di Catania

Informazioni utili

REFERENTE ORGANIZZATIVO	**Dott.ssa Doris MICIELI** – CO.IN.FO. – 011/8129782 – doris.micieli@coinfo.net – iniziative@coinfo.net
QUOTA DI PARTECIPAZIONE INDIVIDUALE	Università consorziate: **€ 700,00** Enti non consorziati: **€ 800,00** La quota di partecipazione individuale è esente IVA ai sensi dell'art. 10, DPR 633/72
MODALITÀ DI ISCRIZIONE	Le **richieste di iscrizione** dovranno pervenire compilando il modulo di iscrizione on-line. Si ricorda che è necessario inserire il codice attività presente nel frontespizio della brochure. Per ragioni di carattere organizzativo non sono ammesse rinunce nei 7 giorni precedenti l'inizio del Corso di formazione. Sono invece sempre possibili eventuali sostituzioni.
SCADENZE E ATTIVAZIONE	I posti disponibili per la partecipazione al Corso di formazione sono **30**. Le iscrizioni dovranno pervenire entro il **26 maggio 2021**. Entro la stessa data la Segreteria del CO.IN.FO. comunicherà l'attivazione del Corso di formazione sul sito istituzionale del Consorzio.
VERSAMENTO DELLA QUOTA DI PARTECIPAZIONE	Il versamento della quota di partecipazione dovrà pervenire al Consorzio **entro 30 giorni** dalla data di ricevimento fattura, che sarà emessa a conclusione del Corso di formazione. La domanda di iscrizione impegna l'Università richiedente al pagamento della/e relativa/e quota/e.

Contatti

Co.In.Fo.

Sede Legale c/o Università degli Studi di Torino
Via Giuseppe Verdi, 8 – 10124 Torino

Tel. 011/8129782 Fax 011/8140483

E-MAIL: segreteria@coinfo.net
PEC: coinfo1@pec.it

SITO WEB: www.coinfo.net

Segreteria organizzativa e amministrativa

Via Giambattista Bogino, 2 – 10124 Torino

rosanna.audia@coinfo.net

doris.micieli@coinfo.net

mara.micieli@coinfo.net

Codice Fiscale e iscrizione Reg. Imprese di Torino 97556790018

Partita IVA 06764560014