"Cybersecurity in azione: gestione e risposta agli incidenti”

Napoli

14/06/2025 dalle ore 13:30 alle ore 18:30

Docenti: *Paolo Piaser*, *Graziano De Petris*, *Esperto Cybersecurity*

Responsabile scientifico: *Mario Lugli*

Obiettivi del corso

Nell’ambito dei dispositivi medici, software o hardware che siano, le regole di safety e di security nella gestione del paziente sono state caratterizzate da direttive prima e regolamenti europei poi decisamente sbilanciati sulla safety. La recente introduzione di analoghe direttive europee e successive leggi di recepimento nazionali in ambito cybersecurity, ha riequilibrato la dimensione normativa, ma l’applicazione e il rispetto di questa molteplicità di regole richiede competenze specifiche, che chi si occupa di gestione di tecnologie biomediche non può più ignorare e delegare ai colleghi dell’ICT. Questo corso vuole quindi fornire quegli elementi utili sia per predisporre capitolati già orientati alla security dei dispositivi oltre a quanto può essere utile per prevenire un attacco hacker e, nel caso colpisca, a fronteggiarlo in modo attivo.

Razionale

In un'era in cui la digitalizzazione è pervasiva in tutti i settori, la cybersecurity è diventata una priorità assoluta, specialmente in ambito sanitario, dove la protezione dei dati sensibili è critica. Il corso si concentra sulla gestione e sulla risposta agli incidenti di sicurezza informatica, fornendo strumenti pratici e metodologie per identificare, contenere e mitigare le minacce informatiche in situazioni dove il tempo per pensare è sempre troppo poco.

Metodologia didattica

Il corso si svilupperà attraverso lezioni frontali con slide di supporto nelle quali si affronteranno temi teorici e pratici. Sarà incentivata l'interazione con l'aula nella discussione delle tematiche del corso.

Destinatari

Ingegneri clinici, personale del ruolo tecnico amministrativo, del ruolo sanitario e delle professioni sanitarie.

Materiali didattici

- slides di presentazione
- documenti cartacei appositamente preparati;
- sitografia (link di riferimento consigliati dal docente per approfondimento);
- test di valutazione.

Costi e agevolazioni

- € 15 per tutti gli iscritti al XXV convegno nazionale AIIC ed i soci AIIC in regola con il pagamento delle quote per l'anno 2025
- € 120 per i non iscritti al XXV convegno nazionale AIIC

Posti disponibili e crediti

Il corso è a numero chiuso. Saranno accettate tutte le iscrizioni in ordine cronologico fino ad esaurimento dei posti fino ad un massimo di 100 partecipanti.

E' stato richiesto accreditamento con un corrispettivo di 5 CFP (Crediti Formativi Professionali)

Programma

13:30 - 14:30:

Le dimensioni del ‘mercato’ della cybersecurity (***Esperto Cybersecurity***)

- Panoramica sugli attacchi cyber in sanità
- Le dimensioni del fenomeno
- Lo stato dell’arte delle difese delle aziende sanitarie

14:30 - 15:45:

La normativa regolatoria: dal GDPR alla NIS2 un percorso che prosegue (***Graziano De Petris***)

- Collegamenti tra GDPR e NIS 2
- L. 90/2024 e D.Lgs. 138/2024: cosa cambia nella gestione dei DM
- Il ruolo del referente della Cybersecurity, del punto di contatto, del CISO

15:45 – 17:00:

Esperienze di gestione di problemi di cybersecurity in contesto DM (***Paolo Piaser***)

17:00 – 18:00:

Simulazione di un attacco hacker: esercitazione in aula (***Esperto Cybersecurity***)

18:00 – 18:30:

Domande e discussione con i partecipanti al corso (***Docente e il Responsabile Scientifico***)

Test finale