

## CORSO 4 - "CYBERSECURITY E DISPOSITIVI MEDICI: LA SICUREZZA CHE VERRA' "

**10 maggio 2023**  
**ore 13:30 - 18:30**

### **Docenti:**

Maurizio Rizzetto (GdL ICT - AiIC)  
Paolo Piaser (Azienda Sanitaria Friuli Occidentale)  
Andrea Assunto (CISO Fondazione IRCCS Policlinico San Matteo)

### **Responsabile scientifico:**

Andrea Gelmetti (GdL ICT - AiIC)

### **Obiettivi del corso**

- Illustrazione generale del quadro legislativo, normativo e regolamentale italiano, europeo ed internazionale relativo all'impatto degli adempimenti richiesti dalle normative in termini di cybersecurity nella gestione delle Tecnologie Sanitarie in una Azienda Sanitaria, pubblica o privata.
- Descrizione delle problematiche legate alle prescrizioni per il trattamento sicuro dei dati personali dal punto di vista della cybersecurity e presentazione delle esperienze e metodologie di analisi, valutazione e gestione legate agli adempimenti richiesti, compresi gli adeguamenti per le Tecnologie Sanitarie.
- Importanza del ruolo e responsabilità dell'Ingegnere Clinico all'interno del team di lavoro aziendale che coinvolge necessariamente altre figure tecnico-professionali nelle differenti fasi di analisi, valutazione e gestione degli adempimenti richiesti dalle normative attuali e di prossima attuazione in termini di cybersecurity.
- Fornire un quadro complessivo delle implicazioni tecnico-informatico-organizzative derivanti dai requisiti legislativi, normativi e regolamentali, al fine di contribuire a rendere gli Ingegneri Clinici sia consapevoli delle problematiche e dei rischi connessi alle prescrizioni per il trattamento dei dati personali sia in grado di analizzare, valutare e realizzare possibili percorsi per gli adeguamenti relativi alla cybersecurity.
- Illustrazione delle applicazioni pratiche in ambito ospedaliero con la descrizione dettagliata degli strumenti a supporto della gestione integrata e sicura dei dispositivi medici in rete.

### **Razionale**

Cybersecurity è sinonimo di sicurezza informatica e comprende la parte dell'Information Security (sicurezza delle informazioni ovvero minacce alla privacy, sicurezza informatica, etc.) che dipende esclusivamente dalle tecnologie informatiche.

Chi si occupa di Cyber Security deve individuare le minacce, le vulnerabilità e i rischi collegati a tutti gli asset informatici presenti al fine di prendere tutte le precauzioni possibili per proteggere i dati da attacchi e mitigare gli effetti di eventuali violazioni alla rete o ai sistemi informatici.

Si intende far emergere come il valore del dato e la necessità di garantire la continuità di erogazione dei servizi siano i pilastri che debbono essere sempre tenuti come riferimento per le scelte tecnologiche ed organizzative che si intende implementare dell'Azienda Sanitaria.

### Metodologia didattica

Il corso si svilupperà attraverso una lezione frontale con slide di supporto nelle quali si affronteranno temi teorici e pratici, incentivando l'interazione dell'aula nella discussione delle tematiche del corso.

### Destinatari

L'incontro formativo è rivolto agli Ingegneri Clinici e tecnici biomedici operanti nei settori pubblici e privati afferenti alle funzioni di Ingegneria Clinica, Operations Management, Information & Communication Technology, Innovation Manager, Responsabile per la Transizione Digitale, Risk Management, Referenti Privacy ed ai Medici di Direzione di Presidio.

### Materiali didattici

Durante le ore di formazione e immediatamente dopo lo svolgimento delle stesse verrà rilasciato il materiale didattico di riferimento relativo agli argomenti trattati durante il corso. Oltre alla copia in formato cartaceo ed elettronico del materiale didattico, verranno forniti i link ai siti web di interesse e di supporto per chi desiderasse approfondire ulteriormente gli argomenti trattati.

### Costi e agevolazioni

- € 15 per tutti gli iscritti al XXIII convegno nazionale AIIC ed i soci AIIC in regola con il pagamento delle quote per l'anno 2023
- € 120 per i non iscritti al XXIII 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.

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

### Programma (preliminare)

- **13.30 – 14.30:** Introduzione e descrizione dello scenario. Il ruolo dell'Ingegnere Clinico nel mondo della Cybersecurity
- **14.30 – 16.30:** Il quadro normativo di riferimento ed i principali adempimenti in ambito sanitario
- **16.30 – 18.30:** Applicazioni pratiche in ambito ospedaliero: strumenti a supporto della gestione integrata e sicura dei dispositivi medici in rete