**SABATO 18 MAGGIO 2024**

**CORSO 8**
13:30 - 18:30

## PRINCIPI E STRATEGIE DI GESTIONE DELLA SICUREZZA INFORMATICA APPLICATA ALL'AMBITO DEI DISPOSITIVI MEDICI

### Docenti
Maurizio Rizzetto (Comitato ICT - AIIC)
Paolo Piaser (Azienda Sanitaria Friuli Occidentale)
Andrea Assunto (CISO Fondazione IRCCS Policlinico San Matteo)

### Responsabile scientifico
Andrea Gelmetti (Comitato ICT - AIIC)

### Obiettivi del corso
- Fornire un aggiornamento generale sul quadro legislativo, normativo e regolamentale italiano, europeo ed internazionale relativo all'impatto degli adempimenti richiesti in termini di cybersecurity nella gestione delle Tecnologie Sanitarie in una Azienda Sanitaria, pubblica o privata.
- Analizzare le problematiche legate alle prescrizioni per il trattamento sicuro dei dati personali nell'utilizzo dei dispositivi medici dal punto di vista della cybersecurity. Verranno presentate diverse esperienze e metodologie di analisi, valutazione e gestione legate agli adempimenti richiesti, compresi gli adeguamenti per le Tecnologie Sanitarie. Verrà presentato una simulazione di attacco contestualizzata ad un ambiente ospedaliero che coinvolga sia dispositivi medici sia sistemi IT.
- Rappresentare l'importanza del ruolo e la 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, il tutto con particolare riferimento alle fasi Identify, Protect e Detect del framework NIST.

**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 pilastri imprescindibili 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**

- Slides di presentazione
- Documenti cartacei appositamente preparati;
- Sitografia (link di riferimento consigliati dal docente per approfondimento);

**Costi e agevolazioni**

- € 15 per tutti gli iscritti al XXIV convegno nazionale AIIC ed i soci AIIC in regola con il pagamento delle quote per l'anno 2024
- € 120 per i non iscritti al XXIV 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. È stato richiesto accreditamento con un corrispettivo di 5 CFP (Crediti Formativi Professionali)

**Programma (preliminare)**

**13.30 – 13.40** Saluti e introduzione al corso (*Andrea Gelmetti*)

**13.40 – 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 con particolare riferimento a NIS e NIS2.

**16.30 – 18.15** Applicazioni pratiche in ambito ospedaliero: strumenti a supporto della gestione integrata e sicura dei dispositivi medici in rete.

**18:15 – 18:30** Domande e discussione con i partecipanti al corso (*Tutti i docenti e il Responsabile Scientifico*)

**Test finale**