MIDI-PYRÉNÉES
Axe 11 : PROJETS : ACCOMPAGNEMENTS - FORMATIONS

Module n°3 : Mise en situation cyberattaque dans un service de génie biomédical

Contexte

À l'heure du numérique, il n'est pas un secteur qui soit épargné par la transformation digitale et numérique. Cette transformation induit également l'augmentation du risque vis-à-vis de la cybersécurité.

L'écosystème du secteur de la santé évolue considérablement avec le développement de nouveaux outils numériques et l'arrivée de nouveaux acteurs, accompagnés de leur lot d'avantages, mais aussi d'inconvénients et de risques numériques. Ces risques numériques ne sont plus aujourd'hui à prendre à la légère, en effet s'il y a 10 ans une panne informatique pouvait engendrer des désagréments passagers, elle peut aujourd'hui mettre à l'arrêt des services complets et impacter la continuité des soins.

C'est pourquoi il devient important de préparer les personnels aux cyberattaques en leur donnant un ensemble de pratiques, protocoles et méthodes à mettre en place afin de pouvoir : Anticiper et se préparer en amont d'une cyberattaque ou d'un incident technique sur le SI.

Objectifs

Comprendre à quoi sert la SSI dans un établissement de santé (protection des données, réputation de l'établissement, continuité des soins)

- Comprendre les interactions entre le service biomédical et le service sécurité informatique
- Connaître le risque de piratage des appareils médicaux
- Communiquer efficacement avec le SSI
- Savoir être vigilant lors de la maintenance des appareils médicaux (en présentiel ou à distance)
- Définir un protocole de mise au rebus des disques durs contenant des données de santé
- Etablir des protocoles d'action en cas de cyberattaque

Programme

Contenu en cours de finalisation

Programme différents selon les prestataire. Renseignements auprès de l'Anfh.

Public

Tout personnel du service biomédical

Exercice
2024

Code de formation
PAF04

Nature
AFR

Durée
7 heures

Typologie
Formation continue ou Développement des connaissances et des compétences