ALPES
Axe 3 : ADAPTATION AUX ACTUALITES REGLEMENTAIRES

Renforcement de la cybervigilance : actions de sensibilisation et de gestion des incidents liés au risque cyber

Contexte

L’écosystème du secteur de la santé évolue considérablement, le développement de nouveaux outils numériques et de nouveaux acteurs, accompagnés de leur lot d’avantages et de risques numériques. Ces risques numériques ne sont plus à prendre à la légère, en effet une panne informatique peut aujourd'hui mettre à l’arrêt des services complets et impacter la continuité des soins. Face à ces risques nouveaux, les agents de la fonction publique hospitalière sont les premiers impactés. En réponse à ces risques croissants, il convient pour chaque agent de renforcer sa capacité à faire face aux risques et aux attaques en renforçant ses compétences en cybervigilance. Le but de cette journée de formation et de permettre aux agents de connaitre les risques et les types d’attaques et de savoir y faire face tout en s’insérant de manière efficiente dans la politique de sécurité informatique de leur établissement.

Objectifs

- Comprendre à quoi sert la Sécurité des Système d’Information (SSI) dans un établissement de santé (protection des données, réputation de l’établissement, continuité des soins).
- Comprendre son rôle dans la sécurité informatique de son établissement.
- Connaitre et détecter les différents types de menaces (motivations des cybers criminels, victimes potentielles, etc.).
- Développer un esprit critique et devenir vigilant.
- Connaitre les actions concrètes mobilisables à son niveau (points de vigilances et bonnes pratiques).

Public
Tout agent de la FPH

Exercice
2025

Nature
AFR

Organisé par
Déméter Santé

Typologie
Formation continue ou Développement des connaissances et des compétences

Modules

- **Cybervigilance : actions de sensibilisation et de gestion des incidents**
  Durée : 7 heures
- **Renforcement de la cybervigilance - Actions de sensibilisation et de gestion des incidents liés au risque cyber**
  Durée : 7 heures