MARTINIQUE
Axe 5 : Prévention des risques majeurs et gestion des situations exceptionnelles

Renforcement de la Cybervigilance : acquérir les bons réflexes

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 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).

Renseignements complémentaires

Durée : 1 jour

Contact : Marie-Annick GINAPÉ 0596421060

Exercice
2026

Nature
AFN

Organisé par
Déméter Santé - Crisalyde

Typologie

Formation continue ou Développement des connaissances et des compétences