Les fondamentaux de la cybersécurité pour les managers

Description

Dans un contexte où les cyberattaques touchent de plus en plus le secteur social et médico-social, la sécurisation des systèmes d'information et la protection des données sensibles deviennent des enjeux majeurs pour les établissements ou services sociaux ou médico-sociaux.

Cette formation a été conçue pour permettre aux dirigeants et aux managers de ces établissements et services, de développer une vision globale des enjeux de la cybersécurité, adaptée aux spécificités de leur activité.

Prérequis

Cette formation ne nécessite aucun prérequis, mais il est préconisé d'avoir suivi une formation au RGPD préalablement.

Objectifs

- Maîtriser l'écosystème de la cybersécurité en appréhendant ses enjeux et ses acteurs
- Développer une vision stratégique de la cybersécurité pour protéger efficacement son organisation
- Adopter les bons réflexes pour anticiper les cybermenaces et gérer les crises en toute sérénité
- Renforcer la résilience de son organisation grâce à une compréhension globale des risques de cybersécurité.

Contenu

Première demi-journée :

PARTIE 1 : APPRÉHENDER LE CONTEXTE ET LES ENJEUX DE LA CYBERSÉCURITÉ DANS LE SECTEUR SOCIAL ET MÉDICO-SOCIAL

- *Identifier les enjeux de la cybersécurité dans le secteur de la santé*
- *Reconnaître les risques spécifiques liés à l'activité du secteur social et médico-social*
- *Analyser les impacts des cyberattaques sur l'activité, l'organisation et sa direction*
- *Réaliser un focus sur les enjeux pour les activités d'aide et de soin à domicile*

PARTIE 2 : DÉCRIRE L'ÉCOSYSTÈME DE LA CYBERSÉCURITÉ, SA RÈGLEMENTATION ET SON FINANCEMENT

- *Gouvernance de la cybersécurité au niveau international et national : les acteurs institutionnels et leurs rôles*
- *Organisation des groupes d'attaquants et types d'attaques*
- *Notions sur l'environnement règlementaire et normatif (RGPD, Directive NIS II, Certification ISO 27001)*

- *Programmes de financement de la cybersécurité*

Deuxième demi-journée :

PARTIE 3 : PROTÉGER SON ORGANISATION DES RISQUES DE CYBERSÉCURITÉ

- *Principes de base et bonnes pratiques de sécurité numérique*
- *Typologie des incidents courants dans les ESMS*
- *Protéger les données des personnes accompagnées*
- *Protéger les actifs pour assurer la continuité de l'activité d'aide et de soin à domicile*
- *Définir des processus internes adaptés aux risques de l'activité*
- *Suivre et évaluer les performances de l'organisation en matière de sécurité*
- *Focus sur la communication en cas d'incident : anticiper la communication interne et la communication externe.*

Méthodes pédagogiques

La formation est constituée des éléments suivants :

- Un apport de connaissances sur l'ensemble des sujets abordés
- Des mises en situation et des cas concrets
- Des exercices pratiques et des quiz pour animer et favoriser l'engagement du stagiaire.

Les supports pédagogiques correspondants sont donc fournis :

- Le support de cours fourni au format numérique
- Les exercices et descriptions des cas concrets
- Les quiz et réponses attendues.

Évaluation de la formation

La validation des acquis se fait tout au long de la formation à travers des exercices d'application et des études de cas

Durée : 7 heures de formation en distanciel réparties sur 2 semaines (2 séances de 3,5 heures)
Intervenants : Consultant et formateur en SI de Santé
Publics : Directeurs

Date des formations

- 21 et 28 mai 2026 en distanciel