Les fondamentaux de la cybersécurité pour le personnel de terrain du secteur médico-social

ORGANISATION :
À distance

DATES ET HORAIRES :

DUREE :

LIEU

FORMATEUR
0

OBJECTIFS PÉDAGOGIQUES

- Identifier l'écosystème de la cybersécurité en appréhendant ses enjeux et ses acteurs
- Appliquer les bons réflexes pour anticiper les cybermenaces et gérer les crises en toute sérénité
- Acter son rôle de partie prenante dans l'organisation déployée pour la gestion d'une crise de cybersécurité
- Appliquer les mesures de continuité d'activité afin d'assurer la prise en charge des personnes à domicile en situation dégradée
- Gérer la reprise des activités métiers en fin de situation dégradée

PRÉ-REQUIS

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

PROGRAMME DE LA FORMATION

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)
- Activité interactive et échanges autour de cas pratiques issus de l'activité des participants
- Transmission de l'activité à réaliser pour la prochaine demi-journée de formation.

Échanges autour de l'activité réalisée en intersession : difficultés éventuelles rencontrées et réponses attendues. Retour sur les résultats du quiz de mi-session.

Partie 3 : Sécuriser son activité et protéger les données des usagers

- Principes de base et bonnes pratiques de sécurité numérique
- Cas pratiques interactifs et mises en situation

Partie 4 : Réagir aux incidents et assurer la continuité d'activité

- Les bonnes pratiques en cas d'incident
- Organisation en cas de crise : Qui contacter et comment réagir ?
- Les principes de continuité et de reprise d'activité en cas de cyber attaque ou panne informatique
- Cas pratiques interactifs et mise en situation

MÉTHODE PÉDAGOGIQUE

WELIOM propose cette formation sous la modalité **synchrone** :

- En présentiel (dans les locaux du client ou une salle de formation à l'extérieur de ses bureaux)
- En distanciel (classe virtuelle)
- En Blended-Learning/formation mixte : du présentiel et du distanciel peuvent être envisagé sur demande.

MOYENS ET SUPPORTS PÉDAGOGIQUE

WELIOM utilise les enseignements de la **pédagogie active** pour construire ses formations, avec une juste répartition de la théorie et de la pratique.

Nos formations sont constituées 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
- Des quiz et réponses attendues

Des ressources documentaires peuvent également être mises à disposition des apprenants par le formateur.

MODALITES D'ÉVALUATION

En amont de la formation

- Une qualification du besoin est faite, par entretien avec le donneur d'ordre. Un questionnaire est également envoyé aux stagiaires avec leur convocation pour comprendre leurs enjeux et leurs attentes, prendre en compte la spécificité de leur activité mais également le niveau de maturité de leur organisation et des compétences du stagiaire sur les sujets abordés.

Au début de la formation

- Un test de positionnement identifie le niveau des apprenants sur le sujet de la formation et recueille leurs attentes.

Tout au long de la formation

- Évaluation continue des acquis avec des questions orales, des quiz, des exercices, des cas pratiques et des mises en situation.

A la fin de la formation

- Évaluation pour mesurer l'acquisition des compétences.
- Questionnaire de satisfaction à chaud afin de recueillir la satisfaction des apprenants à l'issue de la formation.
- Questionnaire de satisfaction à froid afin d'évaluer les apports ancrés de la formation et leurs mises en application dans la vie professionnelle, ou les impacts sur le projet professionnel en cas de recherche d'emploi.