

## Les fondamentaux de la cybersécurité pour les décideurs du secteur médico-social

### ORGANISATION :

À distance

### DATES ET HORAIRES :

### DUREE :

### LIEU

### FORMATEUR

2

### OBJECTIFS PÉDAGOGIQUES

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

### 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 réglementation 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 réglementaire et normatif (RGPD, Directive NIS II, Certification ISO 27001)
- Programmes de financement de la cybersécurité
- 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 : 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

### Partie 4 : Définir une stratégie pour assurer la résilience de l'organisation

- Notions de gouvernance, protection, défense et résilience cyber
- La cyber-résilience, une approche collaborative
- Intégrer le volet cybersécurité dans les projets de l'établissement
- Définir les ressources disponibles pour les organisations du secteur social et médico-social
- Structurer ses mesures de cybersécurité : La Politique de Sécurité des Systèmes d'Information et le projet documentaire porté par l'UNA
- Se prémunir contre les attaques et gérer une crise de cybersécurité
- Assurer la continuité et la reprise de l'activité de prise en charge des personnes accompagnées
- Promouvoir une culture de la cybersécurité : communiquer, sensibiliser, développer les compétences des équipes



## 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.