Formation SSI : Sensibilisation aux bonnes pratiques cybersécurité pour les professionnels de santé

CONTACT REFERENT

- Commercial@ageris-group.com
- +33 3 87 62 06 00

MODALITES D'ACCES

- Inscription en réservant votre place sur une session disponible ou par téléphone au +33 3 87 62 06 00, par mail, par le formulaire de contact. Vous recevrez un devis à nous retourner avec votre accord pour confirmer votre inscription.

DELAI D'ACCES

- La durée estimée entre la demande du stagiaire et le début de la formation est de 7 jours (peut être raccourci pour le mode distanciel)

ACCESSIBILITE AUX PERSONNES EN SITUATION D'HANDICAP

- Accessible à distance pour les personnes à mobilité réduite
- Pour connaître l'accessibilité aux salles de formation, vous pouvez nous joindre au +33 3 87 62 06 00

REFERENCE

- SSISENSISANTE

TARIF

- 890 € HT

DUREE DE LA FORMATION

- 1 jour – 7 heures

DATES DES SESSIONS

- Voir site internet

FINANCEMENT

- OPCO

FORMULE INTRA-ENTREPRISE

Formulaire : soumettez votre projet

RESSOURCES PEDAGOGIQUES

- Alternance théorie et étude de cas pratiques
- Exemples concrets
- Evaluation des compétences par des quizz en cours
- Support de cours remis au stagiaire par mail en fin de formation
- Outil distanciel : teams

PRESENTATION DE LA FORMATION

Sensibiliser ses agents/salariés à la cybersécurité aide l'établissement à réduire les risques liés au facteur humain et à instaurer une culture sécurité durable dans tous les services. Cette sensibilisation cible les comportements à risque, comme cliquer sur un lien dans un courriel d'hameçonnage ou télécharger une pièce jointe malveillante. A l'aide de très nombreux exemples concrets, ce STAGE PRATIQUE propose aux participants d'adopter les bonnes pratiques pour limiter les risques d'erreur ou de malveillance.

OBJECTIFS DE CETTE FORMATION

A l'issue de cette formation, le stagiaire aura les compétences pour :

- Détecter les actes malveillants et limiter les risques juridiques et opérationnels en adoptant les bons comportements
- Protéger les informations confidentielles et sensibles
- Réagir de manière adaptée en cas de cyberattaque

PUBLIC

Tous les agents/salariés d'une structure publique ou privée de la santé

PREREQUIS

Aucun prérequis n'est nécessaire.

PROGRAMME DETAILLE

1. **Introduction**
- Qu'est-ce-que la cybersécurité ?
- Protéger les actifs de l'organisation

2. **Les menaces**
- La cybercriminalité
- Les acteurs malveillants
- Les insiders

3. **Les enjeux pour l'organisation et mon activité**
- Les risques et impacts sur l'organisation
- Les obligations réglementaires sur la protection des données (RGPD)
- Le secret médical

4. **Les bonnes pratiques de sécurité**
- La charte informatique et sa portée juridique
- La gestion des mots de passe
- Les emails et le phishing
- La messagerie sécurisée MSSANTE et APICRYPT
- Les mesures de protection des équipements (antivirus, les mises à jour, le verrouillage de session, etc.)
- La séparation des usages professionnels et personnels
- La protection des données patients et de santé
- DMP : le dossier médical partagé
- TCHAP : messagerie instantanée du secteur public
- Comment réagir face à une cyberattaque ?

Formation SSI : Sensibilisation aux bonnes pratiques cybersécurité pour les professionnels de santé

POUR ALLER PLUS LOIN

- RGPD – Conformité et sécurité des traitements de données de santé
- RGPD - Le cadre juridique et réglementaire de la recherche clinique

PLUS D'INFOS

- Contactez-nous par le formulaire de contact ou par mail ou par téléphone au +33 3 87 62 06 00

5. **Conclusion**
- Rappel des responsabilités

MODALITES D'EVALUATION

Validation des connaissances et compétences par un quizz à la fin de chaque chapitre.