EDS
CONSEIL & ORGANISME DE FORMATION

CYBER ATTAQUES, CYBER FRAUDE ET RGPD (LA PROTECTION DES DONNÉES)

2 jours - 14 heures

Contact : Eric Dissane

OBJECTIFS DE LA FORMATION :

- Connaître les différents outils pour gérer ces risques.
- Les actions à mettre en œuvre à la suite d'une attaque informatique
- Connaitre les mesures de prévention contre les risques cyber
- Planifier et organiser ses actions en cas de cyberattaque

OBJECTIFS PEDAGOGIQUES :

L'exercice de l'activité de référent santé nécessite la mise en œuvre de sept domaines de compétences :

1 - Distinguer les nouveaux risques informatiques et identifier les différentes formes d'attaques
2 - Connaître les différents outils pour gérer ces risques
3 - Actions à mettre en œuvre à la suite d'une attaque informatique
4 - Maîtriser la cartographie des risques numériques
5 - Connaitre les mesures de prévention contre les risques cyber
6 - Savoir comment réagir à un contrôle de la Cnil à la suite d'une une violation de données personnelles rendue possible par l'exploitation d'une faille de sécurité par les pirates informatiques
7 - Planifier et organiser ses actions en cas de cyberattaque

INTER-ENTREPRISE & INTA-ENTREPRISE
FRANCE METROPOLITAINE

10 STAGIAIRES MAXIMUM
INDIVIDUALISATION : OUI

PUBLIC : TOUS LES UTILISATEURS AYANT ACCÈS AU SYSTÈME D'INFORMATION VIA UN POSTE INFORMATIQUE.
PRE-REQUIS : AUCUN

DÉLIVRANCE DE L'ATTESTATION DE COMPÉTENCE À L'ISSUE DE LA FORMATION

MÉTHODES PEDAGOGIQUES :

• Apports théoriques et pratiques sous forme d'échanges interactifs avec les participants
•Nombreux exemples pratiques
• Travaux de recherches et exercices pratiques
• Support de cours formation organisation du travail
• Quiz en cours de formation
• Évaluation des acquis en fin de formation

MOYENS PEDAGOGIQUES :

Animation participative

ÉVALUATION & ATTESTATION des COMPÉTENCES :

Quiz en cours et fin de formation

MOYENS D'ENCADREMENT :

D'une part « avec le formateur » pour favoriser l'échange entre les différentes parties.
D'autre part « sans le formateur » pour laisser la possibilité aux apprenants de s'exprimer librement et d'exposer les éventuelles difficultés rencontrées.

PROGRAMME DE LA FORMATION :

1. La typologie des risques : approche par la statistique, identification des risques, les secteurs exposés au travers d'exemples survenus récemment, l'évolution, l'enjeu et les cibles, les techniques

2. Glossaire et stratégies d'attaques et le télétravail, cette nouvelle source de vulnérabilité aux risques cyber

3. La réglementation : législation française et directives européenne) avec les impacts sur l'assurabilité

4. Protection de la vie privée : la RGPD, la maîtrise des règles essentielles et rôle de la CNIL

5. Comment se prémunir (mode de prévention et mesures de protection), rôle de l'assistance (la gestion de crise) et organiser ses actions en cas de cyber attaques

6. Les solutions disponibles sur le marché pour se couvrir en cas d'attaque cyber de la rançon à la perte d'image et perte financière …(le transfert du risque)