carif-oref
PROVENCE
ALPES
CÔTE D'AZUR

LA PROFESSIONNALISATION 2025

S'inscrire

AXE 2 : Développer et piloter son organisme de formation

Sécuriser vos données : les techniques et bonnes pratiques en cybersécurité

Jeudi 13 et vendredi 14 novembre

A distance

Lorsque la formation est réalisée à distance, elle se déroule en **visioconférence** avec partage de documents en amont de la réalisation de l'action. Les stagiaires doivent avoir un PC avec une webcam et une connexion internet suffisante afin de pouvoir suivre la formation.

En présentiel

Lorsque la formation est réalisée en présentiel, elle se déroule au **Carif-Oref - 22 Rue Sainte Barbe 3ème étage - 13002 Marseille**.

Intervenant(e) : Stéphanie V. ou Frédéric H.

Experts du groupe Cyberwings, spécialisé dans la Cyber-sécurité (accompagnement, audit, tests de sécurité, formation)

Public :

Personne en charge du projet de certification : responsables qualité, animateur qualité, référent qualité, formateurs expérimentés, dirigeant ou responsables de structures, responsables de formation ou pédagogiques.

2 jours consécutifs soit 14 heures
Horaires : 9h-12h30/13h30-17h

Tarifs : Module gratuit

Module financé par la Région Sud Provence-Alpes-Côte d'Azur)

Délais d'inscription

Inscription possible 48h avant le début de la formation

Prérequis

Aucun

CONTEXTE

Objectifs généraux :

Ce cours de 2 jours vous permettra de connaître les risques et les conséquences d'une action utilisateur portant atteinte à la sécurité du système d'information et de comprendre les principales parades à mettre en place dans votre organisme de formation.

Objectifs opérationnels :

- Comprendre la typologie de risques liés à la sécurité SI et les conséquences possibles
- Identifier les mesures de protection de l'information et de sécurisation de son poste de travail
- Favoriser la conduite de la politique de sécurité SI de l'organisme de formation
- Comprendre le contexte juridique et comprendre les mesures liées à ce contexte à appliquer

CONTENU

MODULE 1 – Comprendre les menaces et les risques

Système d'information, Cyber-espace, Internet : quels liens et dans quels contextes d'utilisation ?
Qu'entend-on par sécurité Informatique ?
La gestion des la sécurité par les risques : Menaces, impacts, vulnérabilités
Les objectifs de la sécurité : Confidentialité, disponibilité, intégrité, traçabilité
Qu'est-ce qu'une cyber-attaque ?
La typologie de la cyber-criminalité : différence entre hacker, cyber-criminels, escrocs, opportunistes et menaces étatiques
L'équipe de sécurité du système d'information et les stratégies d'entreprise, le cas de la sous-traitance

MODULE 2 – Comprendre le contexte juridique et normatif de la sécurité

Données à caractère personnel, données à caractère personnel sensibles, données sensibles et stratégiques
RGPD et rôle de la CNIL
Les fiches de traitement et les obligations à respecter en tant qu'organisme de formation
Les acteurs de la sécurité en France
Liens avec les systèmes de management de la sécurité et plus particulièrement ISO 27001

MODULE 3 – Comprendre l'utilité d'un mot de passe fort

Qu'est-ce que l'authentification ? Pourquoi ce thème est important dans la cyber-sécurité ?
Exemple de cassage de mots de passe
Qu'est-ce qu'un mot de passe fort ?
L'intérêt de la double authentification et les solutions
Les bonnes pratiques et l'utilisation d'un gestionnaire de mot de passe

MODULE 4 – Protéger vos données

Pourquoi maîtriser vos informations sur l'Internet ?
Qu'est-ce qu'un leak ? Comment réagir face à une fuite de données ?
Exemple d'escroquerie
Qu'est-ce que l'ingénierie sociale ?
L'utilisation de l'IA dans tout çà ? Quelles bonnes pratiques à appliquer ?
Introduction au chiffrement et un exemple avec 7Zip
Les sauvegardes
Les bonnes pratiques au quotidien pour protéger vos données et détecter de l'ingénierie sociale

MODULE 5 – Hygiène numérique

Qu'est-ce qu'un logiciel malveillant ? Qu'est-ce qu'un ransomware ? Utilité des anti-virus
Qu'est-ce que le phishing et comment le détecter ?
Pourquoi mettre à jour son système ?
Pourquoi ne pas faire confiance aux périphériques USB ?
Pourquoi ne pas prêter sa session ?
Que faire en cas de compromission ?
Comment bien naviguer sur Internet (Cookie, navigation privée…) ?

MODULE 6 – Nomadisme

Définition de l'IoT et technologies sans fil
Les risques du wifi
Risques de partage de connexions
Risques en mobilité
Bonnes pratiques

MODULE 7 – Vocabulaire autour de la protection

Qu'est-ce qu'un pare-feu firewall et quel est son rôle dans l'entreprise ?
Qu'est-ce qu'un proxy et quel est son rôle dans l'entreprise ?
Les différents moyens de protection sur votre poste : EPP, EDR, firewall
L'utilité d'un VPN dans un cadre professionnel et privé

MÉTHODE ET ORGANISATION PÉDAGOGIQUE

- Session en présentiel ou en distanciel
- Exposé, interactivité, démonstrations
- Évaluation de satisfaction de fin de formation
- Attestation de fin de formation précisant les modules acquis et en cours d'acquisition
- Support de cours remis durant la session

ÉVALUATION

- Validation des acquis : test d'auto-positionnement en début et fin de formation, QCM final (validation des acquis à partir de 90 % de bonnes réponses)