Référent Cybersécurité en TPE / PME

Réf. EIN021

Public	Pré-requis	Durée	Coût
Dirigeant(e), manager, responsable informatique ou toute personne qui sera en mesure de conseiller sa direction en matière de cybersécurité	Connaissance de base en informatique Il est recommandé d'avoir des compétences	4 jours soit 28 heures	1 200 € HT 1 440 € TTC

Nature de la sanction : Attestation de fin de formation & Attestation d'évaluation des acquis

Pédagogie

▶ Résultats attendus

Disposer des compétences nécessaires en matière de cybersécurité afin d'être référent dans une TPE /PME

▶ Objectifs pédagogiques

Identifier et analyser des problèmes de cybersécurité dans une perspective d'intelligence et de sécurité économiques

Connaître les obligations et responsabilités juridiques de la cybersécurité

Identifier et comprendre les menaces liées à l'utilisation de l'informatique et des réseaux internet, réseaux privés d'entreprises ou réseaux publics

Mettre en œuvre les démarches de sécurité inhérentes aux besoins fonctionnels

Savoir présenter les précautions techniques et juridiques à mettre en place pour faire face aux attaques éventuelles

▶ Méthodes pédagogiques

Tous les points sont illustrés au travers d'exercices adaptés et mis en pratique par le stagiaire aidé, si besoin, par le formateur

Calendrier 2021

▶ Agen

- 25-26 mai et 01-02 juin

▶ Intervenant

- Frédéric GOUTH

Lieux aménagés et modalités adaptées pour faciliter l'accès et l'usage aux personnes en situation de handicap.

Qualiopi processus certifié
RÉPUBLIQUE FRANÇAISE

SUD MANAGEMENT ENTREPRISES

Référent Cybersécurité en TPE / PME

Réf. EIN021

PROGRAMME

Cybersécurité : notions de base, enjeux & droit commun	• Les enjeux de la sécurité des SI • Les propriétés de sécurité • Aspects juridiques et assurantiels • Le paysage institutionnel de la cybersécurité
L'hygiène informatique pour les ordinateurs	• Connaitre le système d'information et ses utilisateurs • Identifier le patrimoine informationnel de son ordinateur • Maitriser le réseau de partage de documents • Mettre à niveau les logiciels • Authentifier l'utilisateur • Nomadisme et problématiques liées au BYOD (Bring your Own Devices)
Gestion & organisation de la cybersécurité	• Présentation des publications et recommandations • Présentation des différents métiers de l'informatique (infogérance, hébergement, développement, juriste, etc.) • Méthodologie pédagogique pour responsabiliser et diffuser les connaissances ainsi que les bonnes pratiques internes • Maitriser le rôle de l'image et de la communication dans la cybersécurité • Méthodologie dévaluation du niveau de sécurité • Actualisation du savoir du référent en cybersécurité • Gérer un incident, procédures judiciaires
Protection de l'innovation & cybersécurité	• Les modalités de protection du patrimoine immatériel de l'entreprise • Droit de la propriété intellectuelle lié aux outils informatiques • Cyber-assurance • Cas pratique
Administration sécurisée du système d'information (SI) interne d'une entreprise	• Analyse de risque (Expression des besoins et identification des objectifs de sécurité-EBIOS) • Méthode harmonisée d'analyse des risques – MEHARI) • Principes et domaines de la SSI afin de sécuriser les réseaux internes • Détecter un incident • Gestion de crise • Méthodologie de résilience de l'entreprise • Traitement et recyclage du matériel informatique en fin de vie • Aspects juridiques
La cybersécurité des entreprises ayant externalisé tout ou partie de leur SI	• Les différentes formes d'externalisation • Comment choisir son prestataire de service ? • Aspects juridiques et contractuels
Sécurité des sites internet gérés en interne	• Menaces propres aux sites Internet • Approche systémique de la sécurité. • Configuration des serveurs et services • HTTPS et infrastructure de gestion de clés (IGC) • Services tiers • Avantages et limites de l'utilisation d'un CMS et/ou développement Web • Sécurité des bases de données • Utilisateurs et sessions • Obligations juridiques réglementaires

Qualiopi processus certifié
RÉPUBLIQUE FRANÇAISE