Ref. formation 202404234378

Référent Cybersécurité en TPE/PME - sur mesure

Financement

Formation professionnelle continue
Non conventionnée / sans dispositif

Organisme responsable et contact

CCI BAYONNE- CENTRE CONSULAIRE FORMATION
CCI FORMATIONS BAYONNE
05.59.46.58.03
cciformations@bayonne.cci.fr

Accès à la formation

Publics visés :

Demandeur d'emploi
Jeune de moins de 26 ans
Personne handicapée
Salarié(e)
Actif(ve) non salarié(e)

Sélection :

Tests
Entretien

Niveau d'entrée requis :

Sans niveau spécifique

Conditions d'accès :

Le professionnel qui sera en mesure de conseiller sa direction en matière de cybersécurité.

Prérequis pédagogiques :

L'accès à la certification ne requiert pas d'expertise particulière. En revanche, l'importance et les enjeux attachés à la fonction, ainsi que l'objet de celle-ci, imposent que chaque candidat justifie d'un titre ou diplôme de niveau 5. A titre dérogatoire, les candidatures des professionnels ne pouvant se prévaloir d'un titre ou diplôme de niveau 5 mais justifiant d'une expérience professionnelle de 3 années minimales pourront être examinées et se voir réserver une issue positive. Toutes les candidatures font l'objet d'une évaluation, sous la forme d'un entretien téléphonique, visant à vérifier l'aptitude du candidat et l'adéquation de son projet de certification avec ses attentes professionnelles.

Contrat de professionnalisation possible ?

Non

Objectif de la formation

Acquérir des compétences en matière d 'identification et prise et compte des problématiques de cyber sécurité mais aussi d 'élaboration, mise en œuvre et animation d'une démarche de prévention et d'amélioration des pratiques de cybersécurité au sein de l'entreprise. Compétences visées : - Identifier les enjeux et problématiques d'intelligence économique et de cybersécurité touchant l'activité de l'entreprise - Identifier les risques et menaces présentant potentiellement un danger pour l'intégrité du système d'information de l'entreprise et de son patrimoine immatériel - Identifier les responsabilités juridiques de l'entreprise en matière de cybersécurité et protection des données - Analyser l'organisation interne et le système d'information de l'entreprise - Évaluer les vulnérabilités de l'entreprise et son niveau de sécurisation - Établir un état des lieux du niveau de sécurité de l'entreprise et du respect de ses obligations règlementaires - Déterminer les actions à mettre en œuvre et le type de supports à déployer - Diffuser les bonnes pratiques et règles d'hygiène fondamentales de la cybersécurité - Systématiser la mise en application des règles d'hygiène fondamentales de la cybersécurité pour l'organisation et les individus - Opérer le suivi des comportements et usages en matière de cybersécurité

Contenu et modalités d'organisation

Les enjeux de la cybersécurité et évaluation du niveau de sécurité de son entreprise (14 heures) 1. Décrire l'organisation les enjeux et les objectifs de la cybersécurité • Organisation de la cybersécurité en France • Les enjeux de la sécurité des SI • Les objectifs de sécurité • Notions de vulnérabilité, menace, attaque • Panorama de quelques menaces 2. Connaître le système d'information et ses utilisateurs 3. Identifier le patrimoine informationnel de son système d'information 4. Maitriser le réseau de partage de documents 5. Mettre à niveau les logiciels 6. Authentifier l'utilisateur 7. Sécuriser le nomadisme 8. Sécuriser les réseaux internes • Sécuriser physiquement • Contrôler la sécurité du S.I. • Lister les menaces propres aux sites Internet : Top 10 OWAPS • Appliquer une approche systémique de la sécurité/Configuration des serveurs et services • Mettre en place chiffrement, codes secrets, symétrie, clé • Utiliser des services tiers • Identifier les avantages et inconvénients de l'Utilisation d'un CMS ou développement web • Sécuriser les bases de données • Gérer les utilisateur et session • Définir PC DSS 9. Utiliser une méthode d'analyse de risques 10. Détecter puis traiter les incidents 11. Construire une méthodologie de résilience de l'entreprise 12. Traiter et recycler le matériel informatique en fin de vie Identifier la problématique de cybersécurité propre à l'entreprise et tenant compte de son environnement juridique et technologique (7 heures) 1. Décrire l'organisation les enjeux et les objectifs de la cybersécurité • Organisation de la cybersécurité en France • Les enjeux de la sécurité des SI • Les objectifs de sécurité • Notions de vulnérabilité, menace, attaque • Panorama de quelques menaces 2. Identifier les aspects juridiques de la réglementation • Connaitre les aspects juridiques et la règlementation • La protection du patrimoine immatériel 3. Identifier les obligations et responsabilités du chef d'entreprise sur son SI 4. Gérer les risques juridiques • Gérer les risques juridiques internes et externes liés au SI • S'assurer : la cyber-assurance, les risques couverts et les dommages garantis • Identifier les aspects juridiques du site e-commerce : la prospection par

…

Parcours de formation personnalisable ? **Oui** **Type de parcours** **Modularisé**

Validation(s) Visée(s)

Référent cybersécurité en TPE / PME - *Sans niveau spécifique*

MON COMPTE FORMATION Éligible au CPF

Et après ?

Suite de parcours

Non renseigné

Calendrier des sessions

Numéro Carif	Dates de formation	Ville	Organisme de formation	Type d'entrée	CPF	Modalités
00462374	du 01/01/2024 au 31/12/2024	Bayonne (64)	CCI BAYONNE-CENTRE CONSULAIRE FORMATION		MON COMPTE FORMATION	FPC