Devenez référent Cybersécurité

CCI Bordeaux Gironde
Présentiel / E-learning

35 heures

2000 € net de Tva
Possibilité de prise en charge CPF-OPCO

Formation certifiante
#DATAcompétences

SecNumedu
ANSSI
Formation labelisée par l'ANSSI

CONTACT

Virginie Sioulone - 05 56 79 44 80
competences@bordeauxgironde.cci.fr

BORDEAUXGIRONDE.CCI.FR

CCI BORDEAUX GIRONDE

CCI N° déclaration d'existence 75331044233 - N°TVA FR 61 130 022 858 - N°SIRET 130 022 858 000 18 -NAF 8542 Z

Devenez référent cybersécurité dans vote TPE-PME

Objectif

Former des référents en Cybersécurité capables de :
• Identifier et analyser les problèmes de cybersécurité dans une perspective de sécurité économique,
• Connaitre les obligations et les responsabilités juridiques,
• Identifier et comprendre les menaces liées à l'utilisation de l'informatique et des réseaux internet,
• Mettre en œuvre les démarches de sécurité inhérentes aux besoins fonctionnels,
• Savoir présenter les précautions techniques et juridiques pour faire face aux attaques.

Public

Dirigeants, cadres, responsables informatiques, mais aussi tout public en recherche de double compétence ou en reconversion.

Pré requis

Cette formation ne nécessite pas de prérequis

Modalités et délai d'accès

Entretien préalable
La demande doit être faite, au minimum, 48 heures avant le démarrage de la formation (jours ouvrés) sous réserve d'accord de financement et de place disponible

Accueil et accès des publics en situation de handicap :

Contactez notre Référent Handicap :
Pascale BENOTTEAU
pbenotteau@bordeauxgironde.cci.fr

Méthodes et outils pédagogiques

Alternance de cas pratiques et de cours théoriques
Interactions collectives, séances de questions / réponses
Partages d'expériences
Exercices de mise en application individualisés et personnalisées / Support pédagogique

Modalités d'évaluation

QCM, étude de cas
Certificat de compétences (descriptif sur www.francecompétences.fr)

Intervenants

Des experts techniques : consultants cybersécurité & cyberdéfense.

CCI BORDEAUX GIRONDE

Mise à jour avril 2021

PROGRAMME

Module 1 : Notions de base, enjeux et principales menaces
- Définition
- Les enjeux de la sécurité des SI
- Les objectifs de sécurité

Module 2 : L'hygiène informatique pour les utilisateurs
- Connaître le système d'information et ses utilisateurs
- Identifier le patrimoine informationnel de son système d'information (brevets, codes sources…)
- Maitriser le réseau de partage de documents
- Mettre à niveau les logiciels
- Authentifier l'utilisateur
- Le nomadisme

Module 3 : Gestion et organisation de la Cybersécurité
- Présentation des publications / recommandations des différents métiers de l'informatique
- Méthodologie pédagogique pour responsabiliser et diffuser les connaissances et les bonnes pratiques
- Maitriser le rôle de l'image et de la communication dans la cybersécurité
- Méthodologie d'évaluation du niveau de sécurité
- Actualisation du savoir du référent cyber sécurité
- Gérer un incident/ procédures judiciaires
- RGPD : processus méthodologique

Module 4 : Aspects juridiques et réglementation, protection de l'innovation
- La protection du patrimoine immatériel de l'entreprise
- Droit de la propriété intellectuelle lié aux outils
- Traitement et recyclage du matériel en fin de vie
- Aspects juridiques assurantiels
- Aspects juridique SI (Risques, responsabilités et non-conformité des infrastructures)
- Aspects juridiques et contrats (externalisation partielle / intégrée : choix du prestataire de service ; protection du patrimoine économique / données RGPD)
- Aspects juridique e-commerce (règles de sécurité et de gestion des sites web ; e-commerce/protection/loi)
- Cas pratiques

Module 5 : Administration sécurisée du système d'information (SI) d'une entreprise
Analyse du risque – Principes et domaines de la SSI afin de sécuriser les réseaux internes

Module 6 : Gestion du SI externalisé
- Les différentes formes d'externalisation
- Comment choisir le prestataire de services

Module 7 : Sécurité des sites internet gérés en interne
- Menaces propres aux sites internet
- Approche systémique de la sécurité
- Configuration des serveurs et services
- HTTPS et infrastructures de gestion de clef / Services tiers
- Avantages et limites de l'utilisation d'un CMS et ou développement web
- Sécurité des bases de données
- Utilisateurs session