Référent Cybersécurité pour les TPE/PME

Objectifs

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.

Compétences

- Connaissance de la stratégie de l'entreprise, de son organisation, de ses métiers et des enjeux
- Connaissance du système d'information, de son architecture et des interfaces en applications
- Sens de la confidentialité, intégrité et éthique
- Rigueur, capacité d'anticipation et sens de la méthode afin de mettre en place des programmes de sécurité efficients
- Pédagogie pour expliquer aux utilisateurs les règles à respecter pour ne pas mettre en danger le système d'information de l'entreprise
- Diplomatie, écoute, sens du dialogue, persuasion, pour convaincre les utilisateurs des risques encourus et du bien-fondé des procédures mises en place
- Résistance au stress pour faire face à des situations de crise (intrusion, virus,…) et prioriser les actions à mener.
- Curiosité pour se tenir au courant des nouveaux risques et des nouvelles parades
- Force de proposition pour faire évoluer la stratégie, ainsi que les pratiques
- Capacité à travailler et à s'adapter à tous les niveaux d'interlocuteurs de l'entreprise en adaptant son langage et son niveau d'explication à la population avec laquelle il est amené à travailler

Public

- Dirigeants, cadres, responsables informatiques, mais aussi tout public en recherche de double compétence ou en reconversion.
- Pré requis : Avoir une bonne connaissance de l'informatique, des systèmes Windows et Internet (navigateurs, réseaux sociaux).
  Il est recommandé d'avoir des connaissances sur l'organisation d'un système d'information.

Informations pratiques

- Évaluation des acquis, attestation de formation, certificat de compétences
- Durée : 35 heures réparties en 5 jours
- Tarif : 1 800 € net de TVA
- Possibilité de prise en charge par les fonds de formation, compte CPF

Dates et lieux :

- 8, 9, 10 et 29, 30 avril 2019

- CCI Bordeaux Gironde:
  17 Place de la Bourse
  33076 Bordeaux Cedex

Contact : Sylvie Dubois
05 56 79 50 34
sdubois@bordeauxgironde.cci.fr

Les intervenants

- Des experts techniques : avocat, consultants cybersécurité & Cyberdéfense.

Outils pédagogiques

- Alternance de cas pratiques et de cours théoriques
- Travaux de groupe
- Interactions collectives, séances de questions / réponses
- Partages d'expériences
- Exercices de mise en application individualisés et personnalisés
- Supports pédagogique (vidéos, PowerPoint)
- Malette du référent (tutoriels, guides pratiques, contacts…)

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…)
• Maîtriser 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
• Maîtriser 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 • Le droit de la propriété intellectuelle lié aux outils informatiques • Traitement et recyclage du matériel informatique en fin de vie • Aspects juridiques assurantiels (définitions /enjeux/propriétés de sécurité des SI ; responsabilités/réglementations/préservation de la preuve ; offre assurantielle) • Aspects juridiques SI (SI et Risques: sécuriser/détecter/gérer ; responsabilités et non-conformité des infrastructures) • Aspects juridiques et contrats (externalisation partielle/intégrée ; choix du prestataire de service ; protection du patrimoine économique /données; obligations ; RGPD). • Aspects juridiques e-commerce (règles de sécurité et de gestion des sites web ; le 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 système d'information 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 et session **Evaluation des compétences**