CCI FORMATION
AIX-MARSEILLE-PROVENCE

Digital | Webmarketing | Informatique | Numérique

REFERENT CYBERSECURITE EN TPE/PME

En résumé

Code RNCP / RS

RS5568

Référence

NC

Ces dernières années en France, les cybermenaces ont augmenté de 400%. En effet, 50% des entreprises déclarent avoir constaté une augmentation significative des attaques suite à la généralisation du télétravail. Selon le dernier rapport d'activité de la CNIL, les PME et les micro-entreprises représentent 69% des notifications de violations de données personnelles notamment liées à du piratage informatique. Selon le Baromètre de la CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) 2023, plus d'une entreprise sur deux a été victime de cybercriminalité au cours de l'année 2021. L'impact sur le chiffre d'affaires est important puisqu'il représente une perte moyenne d'environ 27%. Ces chiffres montrent l'importance pour une entreprise de former un référent cybersécurité pour protéger efficacement son savoir-faire. La cybercriminalité est un fléau pour les entreprises et les attaques ne cessent de croître. Pour protéger efficacement votre savoir-faire, il est essentiel de former un référent cybersécurité au sein de votre entreprise. Ce professionnel sera en mesure de définir une politique de sécurité, mettre en œuvre et suivre la politique de sécurité, organiser des formations pour rappeler aux collaborateurs les enjeux de la cybersécurité et de la protection des données, assurer les veilles technologiques et juridiques sur la cybersécurité et suivre et évaluer de façon périodique l'efficacité des actions menées.

Ne laissez pas votre entreprise être vulnérable aux attaques.
Formez un Référent Cybersécurité dès maintenant.

Cette formation en cybersécurité certifiante est conçue pour apporter une réponse aux entreprises face aux cybermenaces. Sur le modèle de formation continue diplômante et sans prérequis nécessaires, ce programme propose des modules courts pour tous niveaux axés sur la pratique. Cette formation en cybersécurité à Marseille ou à distance vise à réduire les vulnérabilités des TPE/PME.

Objectifs

Objectif global :

À la fin de la formation, le participant devra être en mesure d'initier et de pérenniser au sein de la TPE/PME la démarche de prévention en matière de cybersécurité visant à préserver et protéger son patrimoine immatériel d'actes d'hostilité, dans le respect de la règlementation :

- Identifier et prendre en compte les problématiques de cybersécurité de l'entreprise en lien avec l'environnement juridique et technologique
- Evaluer les usages et le niveau de sécurité de l'entreprise
- Elaborer, mettre en œuvre et animer une démarche de prévention et d'amélioration des pratiques de cybersécurité au sein de l'entreprise

Objectifs opérationnels :

- Identifier les enjeux et problématiques de la cybersécurité
- Identifier les risques et menaces et déterminer des solutions permettant de protéger l'entreprise
- Identifier les responsabilités juridiques de l'entreprise en matière de cybersécurité
- Analyser l'organisation interne et le système d'information de l'entreprise
- Evaluer les vulnérabilités de l'entreprise et son niveau de sécurisation
- Etablir 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

Programme

Identifier la problématique de cybersécurité propre à l'entreprise et tenant compte de son environnement juridique et technologique

- Décrire l'organisation les enjeux et les objectifs de la cybersécurité
- Identifier les aspects juridiques de la réglementation
- Identifier les obligations et responsabilités du chef d'entreprise sur son SI
- Gérer les risques juridiques

Evaluer le niveau de sécurité de son entreprise

- Connaître le système d'information et ses utilisateurs
- Identifier le patrimoine informationnel de son système d'information
- Maitriser le réseau de partage de documents
- Mettre à niveau les logiciels
- Authentifier l'utilisateur
- Sécuriser les réseaux internes
- Sécuriser le nomadisme
- Utiliser une méthode d'analyse de risques
- Détecter puis traiter les incidents
- Connaître les responsabilités juridiques liées à la gestion d'un SI
- Construire une méthodologie de résilience de l'entreprise
- Traiter et recycler le matériel informatique en fin de vie

Mettre en œuvre la cybersécurité : construire son plan d'action

- Construire une veille documentaire d'information et de recommandation
- Lister les métiers directement impactés par la cybersécurité
- Lister les différents métiers de prestation informatique
- Construire une méthodologie pédagogique pour responsabiliser et diffuser les connaissances et les bonnes pratiques
- Construire une méthodologie d'évaluation du niveau de sécurité
- Actualiser le savoir du référent cyber sécurité
- Classer les formes d'externalisation
- Choisir les prestataires de service

Méthodes pédagogiques

– Nombreux exercices pratiques et cas de synthèse pour acquérir les bons réflexes.
– Alternance d'apports théoriques et d'applications pratiques.
– Pédagogie active : échanges, analyses de pratiques, mises en situation, cas réels d'entreprises
– Support de formation remis aux participants.

Moyens techniques

Salles de formation équipées de postes informatiques et logiciels métiers.

Les formations en FOAD e font via une système de visio-conférence dédié (TEAMS Pédagogique)

Assistance technique assurée par un contact identifié en début de session.

Suivi d'action

Les acquis sont évalués en cours et en fin de formation notamment au travers de QCM, mises en situations, mises en pratiques, présentations qui feront l'objet d'une analyse/correction et d'un retour du formateur.
Une évaluation de satisfaction est complétée par les participants et un tour de table collectif est réalisé avec le formateur en fin de formation.

Intervenants

Formateurs Professionnels Expert cybercriminalité

Évaluation

Grille de fin de stage

Certification RGPD – Réseau Initiative Data Compétences – CCI France.
Découvrez également notre formation se mettre en conformité au RGPD.