LC FORMATIONS
CONSEIL & DEVELOPPEMENT

PROGRAMME DE FORMATION

CYBER SÉCURITÉ

DOCUMENT REMIS AU STAGIAIRE
AVANT SON INSCRIPTION

CONTACT / RENSEIGNEMENT :

CASTILLON LAURÈNE, 06.69.23.18.16
CONTACT@LC-FORMATIONS.FR

FORMATION CYBER SÉCURITÉ

OBJECTIFS PROFESSIONNELS :

Identifier les enjeux et les risques de la CyberSécurité et en comprendre les principes
- Renforcer les compétences en sécurité informatique.
- Protéger les systèmes d'information contre les cyberattaques.
- Participer au développement de la sécurité des entreprises.

CATÉGORIE ET BUT

La catégorie prévue à l'article L.6313-1 est : Action de formation

Cette action a pour but (article L.6313-3) : De favoriser l'adaptation des travailleurs à leur poste de travail, à l'évolution des emplois ainsi que leur maintien dans l'emploi et de participer au développement de leurs compétences en lien ou non avec leur poste de travail.

PUBLIC

Le public concerné est : Tout public intéressé par la sécurité informatique.

PRÉ-REQUIS

Aucun pré-requis nécéssaire.

DURÉE

Cette formation se déroulera en 125 heures sur 15 jours.

Horaires et Dates : Voir convention de formation.

TARIF

SUR DEMANDE

Organisme de formation net de TVA.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription est réputée acquise lorsque : La convention de formation est signée.
Les délais d'accès à l'action sont : 15 jours avant de le début de l'action de formation.

FORMATION CYBER SÉCURITÉ

MOYENS PÉDAGOGIQUES, TECHNIQUES ET D'ENCADREMENT

MÉTHODES ET OUTILS PÉDAGOGIQUES

Cours théoriques et pratiques sur ordinateur. Utilisation de maquettes techniques et d'exercices pratiques. Programme de formation détaillé remis aux stagiaires. L'organisation pédagogique repose sur l'individualisation accompagnée avec présence pédagogique constante du formateur.

- **Cours théoriques et pratiques sur ordinateur:** Les stagiaires auront des sessions théoriques suivies de mises en pratique immédiates pour consolider leurs connaissances.
- **Outils pédagogiques:** Utilisation de maquettes techniques et d'exercices pratiques pour l'apprentissage.
- **Supports pédagogiques:** Programme de formation détaillé remis aux stagiaires.

SUPPORTS PÉDAGOGIQUES : Vidéos en ligne et leçons diverses

PRISE EN COMPTE DU HANDICAP : Les personnes en situation de handicap physique peuvent tout à fait rejoindre notre formation. Merci de nous contacter pour toute situation particulière.

ELÉMENTS MATÉRIELS DE LA FORMATION

Equipements divers mis à disposition : un ordinateur avec connexion internet sera mis à disposition du stagiaire.
Documentation : Le formateur s'appuiera sur des articles disponibles en ligne.

COMPÉTENCES DES FORMATEURS

Le formateur référant possède les qualités nécessaires à la mise en place d'un parcours modulaire. Il a un rôle de formateur accompagnateur. Il réajuste en permanence le contenu de la formation en fonction des avancées du stagiaire. Il reste à l'écoute des besoins et répond au mieux aux attentes.

La formation sera assurée par Monsieur Pierre Martin, expert en Cybersécurité.

FORMATION CYBER SÉCURITÉ

→ CONTENU DE LA FORMATION

PARTIE 1 - INTRODUCTION À LA CYBERSÉCURITÉ (5H)

- Comprendre les bases de la cybersécurité
- Évolution des menaces et des attaques informatiques
- Principaux concepts et termes de la cybersécurité

PARTIE 2 - ANALYSE DES RISQUES ET MENACES (15H)

- Analyse des risques informatiques
- Identification des menaces et vulnérabilités
- Mise en place de stratégies de mitigation

PARTIE 3 - POLITIQUES ET PROCÉDURES DE SÉCURITÉ (10H)

- Établir des politiques de sécurité efficaces
- Mise en place de procédures de gestion des incidents
- Alignement des politiques avec les objectifs de l'entreprise

PARTIE 4 - SÉCURISATION DES SYSTÈMES D'INFORMATION (10H)

- Sécurisation des réseaux et systèmes
- Utilisation des pare-feu et des systèmes de détection d'intrusion
- Bonnes pratiques de sécurité informatique

PARTIE 5 - GESTION DES IDENTITÉS ET DES ACCÈS (20H)

- Gestion des accès et des identités
- Mise en place de contrôles d'accès
- Techniques d'authentification sécurisée

PARTIE 6 - CRYPTOGRAPHIE ET SÉCURITÉ DES DONNÉES (15H)

- Principes de la cryptographie
- Utilisation des techniques de chiffrement
- Sécurisation des données sensibles

FORMATION CYBER SÉCURITÉ

→ CONTENU DE LA FORMATION

PARTIE 7 - SÉCURITÉ DES APPLICATIONS (20H)

- Bonnes pratiques de développement sécurisé
- Tests de sécurité des applications
- Protection contre les attaques de type injection

PARTIE 8 - SURVEILLANCE ET DÉTECTION DES INCIDENTS (10H)

- Surveillance des systèmes et des réseaux
- Techniques de détection des incidents
- Utilisation des outils de gestion des incidents

PARTIE 9 - RÉPONSE AUX INCIDENTS ET GESTION DE CRISE (15H)

- Mise en place d'un plan de réponse aux incidents
- Gestion des crises informatiques
- Communication en situation de crise

PARTIE 10 - AUDIT ET CONFORMITÉ (5H)

- Techniques d'audit de sécurité
- Conformité aux normes et régulations
- Amélioration continue des processus de sécurité

FORMATION CYBER SÉCURITÉ

SUIVI ET ÉVALUATION

EXÉCUTION DE L'ACTION

Les moyens permettant de suivre l'exécution de l'action sont :

- Feuilles de présence émargées par les stagiaires et le formateur
- Attestation remise aux stagiaires ayant suivi la formation avec assiduité

MODALITÉS D'ÉVALUATION DES RÉSULTATS (OU D'ACQUISITION DES COMPÉTENCES)

Les moyens mis en place pour déterminer si le stagiaire a acquis les connaissances ou les gestes professionnels précisés dans les objectifs sont :

- Questions orales et exercices pratiques validant les acquis tout au long de la formation
- QCM

LC FORMATIONS

CONSEIL & DEVELOPPEMENT