PROGRAMME DE FORMATION

Élaborer et mettre en œuvre une démarche de cybersécurité

DURÉE : 1 jours | 14 heures
MODALITÉ D'ORGANISATION : Mixte

Informations

PUBLIC VISÉ

Responsables RSE, DPO, juristes, responsables informatiques et dirigeants chargés d'encadrer les usages de l'IA.

OBJECTIFS PÉDAGOGIQUES

Définir une politique de cybersécurité adaptée à l'entreprise ; Former et sensibiliser les collaborateurs aux bonnes pratiques.
Identifier les risques et vulnérabilités spécifiques à l'organisation ; Assurer le suivi et l'amélioration continue de la démarche cybersécurité.
Mettre en œuvre des mesures de sécurité techniques et organisationnelles.

PRÉREQUIS

Avoir suivi la formation « Cybersécurité : sensibilisation » ou avoir le niveau équivalent.

ACCESSIBILITÉ

Si vous êtes en situation de handicap, merci de nous contacter afin que nous puissions vous accompagner et vous orienter au mieux dans votre demande et vos démarches.

Modalités pédagogiques

MODALITÉS

Formation dispensée en présentiel ou à distance (sur demande) par un formateur expert dans ce domaine : apports théoriques, exercices de mise en situation professionnelle.
Programme, supports et fiches pratiques remis aux stagiaires. Supports pédagogiques utilisés : vidéos, documents PDF, PowerPoint et quiz.

MOYENS ET SUPPORTS PÉDAGOGIQUES

Formation dispensée en présentiel ou à distance (sur demande) par un formateur expert dans ce domaine : apports théoriques, exercices de mise en situation professionnelle.

MODALITÉS D'ÉVALUATION ET DE SUIVI

Avant la formation : audit des besoins et du niveau
En cours de formation : Évaluation en continu de la compréhension et de l'assimilation des savoirs et savoir-faire par le formateur lors de mises en situation et cas pratiques.
À la fin de la formation : évaluation de la compréhension et de l'assimilation des savoirs et savoir-faire par le formateur, évaluation des acquis : Quiz/QCM de fin de module.
Formation qualifiante : certificat de réalisation en fin de formation

Contenu pédagogique

01 - Introduction et tour de table

- Présentation des étapes et thématiques abordées : sommaire du module/parcours de formation.
- Validation des objectifs avec chaque apprenant.
- Tour de table guidé : échanges et positionnement des acquis et des besoins de chacun.

02 - Évaluation des risques et vulnérabilités

- Méthodes d'analyse des risques : identification des actifs critiques et des données sensibles.
- Cartographie des menaces et scénarios d'attaque : atelier pratique, diagnostic sécurité.

03 - Politique et mesures de cybersécurité

- Définition de règles et procédures internes : sécurité des systèmes, réseaux et applications.
- Gestion des accès, mots de passe et authentifications : sauvegarde, plan de reprise et plans d'incident.

04 - Mettre en place la cybersécurité

- Charte informatique et guides pratiques.
- Communication interne et bonnes pratiques : simulations et exercices, phishing, intrusion, gestion d'incidents.

05 - Suivi et amélioration continue

- Audit interne et indicateurs de sécurité : mise à jour des procédures et contrôle des mesures.
- Retour d'expérience et planification de la sécurité.

06 - Valider les acquis et clôturer la formation

- Bilan et évaluation finale de la formation.
- Enquête de satisfaction à chaud.

Modalités d'évaluation

Avant la formation : audit des besoins et du niveau

En cours de formation : Évaluation en continu de la compréhension et de l'assimilation des savoirs et savoir-faire par le formateur lors de mises en situation et cas pratiques.

À la fin de la formation : évaluation de la compréhension et de l'assimilation des savoirs et savoir-faire par le formateur, évaluation des acquis : Quiz/QCM de fin de module.

Formation qualifiante : certificat de réalisation en fin de formation