



FORMEZVOO

VOTRE RÉUSSITE, NOTRE PRIORITÉ

**INTÉGRER LA
CYBERSÉCURITÉ
DANS SON ENTREPRISE**

PRÉSENTATION DE LA FORMATION

Intitulé de la formation : Intégrer la cybersécurité dans son entreprise

Durée : 2 jours (14 heures)

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

- Comprendre les enjeux et les impacts des menaces numériques sur l'entreprise.
- Identifier les vulnérabilités et les risques en matière de sécurité informatique
- Mettre en place des mesures et des outils pour sécuriser les données, les employés et l'infrastructure.
- Sensibiliser les équipes aux bonnes pratiques en cybersécurité pour anticiper les risques et renforcer la protection de l'entreprise.

PUBLIC CIBLE

- Dirigeants et décideurs souhaitant intégrer la cybersécurité dans leur stratégie.
- Responsables informatiques et administrateurs réseau.
- Managers et responsables d'équipe souhaitant protéger leurs collaborateurs et leurs données.
- Toute personne impliquée dans la sécurité numérique au sein de l'entreprise.

PRÉREQUIS

- Dirigeants et décideurs souhaitant intégrer la cybersécurité dans leur stratégie.
- Responsables informatiques et administrateurs réseau.
- Managers et responsables d'équipe souhaitant protéger leurs collaborateurs et leurs données.
- Toute personne impliquée dans la sécurité numérique au sein de l'entreprise.

PROGRAMME DE FORMATION

1. Comprendre la cybersécurité et ses enjeux :

- Introduction aux concepts clés de la cybersécurité.
- Les menaces numériques : types d'attaques et leurs impacts sur l'entreprise.

2. Identifier les risques et les vulnérabilités :

- Analyse des points faibles des systèmes informatiques et des processus.
- Identification des menaces internes et externes.

3. Mettre en place des mesures de protection :

- Sécuriser les données : cryptage, sauvegarde et gestion des accès.
- Mise en œuvre d'outils de sécurité : antivirus, pare-feu, et solutions de détection des intrusions.

4. Sensibiliser et former les collaborateurs :

- Les bonnes pratiques en matière de cybersécurité au quotidien.
- Prévention des attaques via phishing, ransomware, et autres menaces courantes.

5. Elaborer une stratégie de cybersécurité :

- Développer un plan de gestion des incidents et de reprise après sinistre.
- Suivre et adapter les mesures de sécurité en fonction des évolutions technologiques.

6. Etudes de cas et mises en situation :

- Analyse de scénarios réels d'attaques et de leurs conséquences.
- Ateliers pratiques pour tester et renforcer les défenses de l'entreprise.

MÉTHODES PÉDAGOGIQUES

- Apports théoriques sur les concepts fondamentaux de la cybersécurité.
- Etudes de cas réels pour comprendre les impacts des menaces numériques.
- Exercices pratiques pour analyser les vulnérabilités et mettre en œuvre des solutions.
- Discussions interactives et partage de bonnes pratiques pour renforcer l'apprentissage.

MODALITÉS D'ÉVALUATION

- Auto-évaluation en début et fin de formation.
- Exercices pratiques pour valider les acquis et tester les solutions mises en place.
- Quiz final pour mesurer les connaissances et compétences développées.

ACCESSIBILITÉ

La formation est accessible aux personnes en situation de handicap. Un aménagement spécifique peut être étudié selon les besoins.

MODALITÉS D'INSCRIPTION

- Inscription possible par email (contact@formezvoo.com) ou en contactant directement l'organisme au 09 70 70 01 03
- Convocation et informations pratiques transmises avant le démarrage de la formation