RÉFÉRENT CYBERSÉCURITÉ EN TPE / PME.

Notre formation cybersécurité vous permet d'acquérir une maîtrise solide des fondamentaux de la protection numérique. De l'identification des menaces à la sécurisation des réseaux, en passant par les bonnes pratiques d'hygiène informatique et la gestion des incidents, vous apprendrez à mettre en place des mesures concrètes pour protéger efficacement vos systèmes d'information.

Durée

21.00 heures (3.00 jours)

Profils des apprenants

Pour tout le monde.

Prérequis

Aucun prérequis.

Accessibilité et délais d'accès

Pour les personnes en situation de handicap, nous étudions les actions que nous pouvons mettre en place pour favoriser leur apprentissage à travers un questionnaire avant formation. Nous nous appuyons également sur un réseau de partenaires locaux.

Qualité et indicateurs de résultats

Taux de présence VS taux d'abandon, taux de satisfaction à chaud et à froid, taux de réussite à l'évaluation finale.

OBJECTIFS PÉDAGOGIQUES.

- Identifier les enjeux et problématiques de cybersécurité
- Prendre en compte les contraintes juridiques, technologiques et organisationnelles.
- Repérer les menaces, risques et vulnérabilités : impact potentiel sur le système d'information de l'entreprise.
- Établir un état des lieux du niveau de sécurité.
- Déterminer et prioriser des actions de sécurisation
- Conformité avec les obligations réglementaires (RGPD, responsabilités légales) et les bonnes pratiques.
- Mettre en œuvre une démarche opérationnelle : prévention, sensibilisation et amélioration continue de la cybersécurité.
- Diffuser et pérenniser les bonnes pratiques : hygiène informatique et comportements des collaborateurs.
- Assurer le suivi et l'évaluation
- Observation des usages et comportements, ajustement des mesures selon retours et incidents.

CONTENU DE LA FORMATION.

Module 1 : Enjeux et cadre légal

- Comprendre les enjeux de la cybersécurité dans un contexte TPE/PME.
- Connaître les obligations réglementaires : RGPD, responsabilités légales.
- Identifier les acteurs institutionnels : CNIL, ANSSI et leurs ressources.
- Comprendre la notion de patrimoine informationnel et de cyber-risque.

Module 2 : Diagnostic et évaluation des risques

- Réaliser une cartographie du système d'information et des usages.
- Identifier les menaces et vulnérabilités les plus courantes.
- Conduire une analyse de risques adapté, exemple : méthode simplifiée type EBIOS.
- Établir un état des lieux du niveau de sécurité de l'entreprise.

Module 3 : Bonnes pratiques et hygiène numérique

- Mettre en œuvre les règles de base
- Gestion des mots de passe, mises à jour, sauvegardes.
- Sécuriser les postes de travail et les équipements mobiles.
- Protéger les communications
- VPN, chiffrement, authentification.
- Définir une politique d'accès et de gestion des droits.

Module 4 : Gouvernance et plan d'action

- Élaborer une feuille de route cybersécurité adaptée à la taille de l'entreprise.
- Prioriser les mesures correctives et préventives.
- Mettre en place une charte informatique et des supports de sensibilisation.
- Définir un dispositif de veille
- Menaces et évolutions réglementaires.

Module 5 : Gestion des incidents et continuité

- Détecter et signaler un incident de sécurité.
- Mettre en œuvre les premiers gestes de confinement et d'alerte.
- Organiser la communication interne et externe en cas d'incident.
- Construire un plan de reprise et de continuité d'activité.
- Tirer parti des retours d'expérience : amélioration des dispositifs.

Module 6 : Sensibilisation et suivi

- Déployer une culture cybersécurité au sein de l'organisation.
- Concevoir des ateliers et supports pédagogiques pour les collaborateurs.
- Suivre les usages et comportements numériques.
- Évaluer régulièrement l'efficacité des mesures mises en place.
- Piloter une démarche d'amélioration continue.

ORGANISATION DE LA FORMATION.

Équipe pédagogique

Notre équipe pédagogique maîtrise l'ensemble des sujets proposés à la formation. Nous construisons nos programmes en identifiant les besoins en compétences des futurs apprenants et en collaboration avec nos experts métiers. Axio Formation repose sur une approche personnalisée pour chaque parcours professionnel.
Nous concevons des formations qualifiantes qui non seulement répondent à vos besoins spécifiques, mais vous préparent aussi à exceller dans votre domaine.

Pour tout besoin lié à la pédagogie, notre référente est Maud : maud.hoffmann@axio-formation.com
Pour tout besoin d'ordre administratif, notre référente est Emilie : emilie.vannieuwenborg@axio-formation.com

Moyens pédagogiques et techniques

- **En présentiel** : Accueil des participants dans une salle dédiée à la formation. Documents supports de formation projetés. Etudes de cas concrets. Quizz et activités collectives en salle; Mise à disposition en ligne de documents supports à la suite de la formation
- **En distanciel** : Classes virtuelles via l'interface Digiforma. Support de formation partagé. Activités d'entrainement en synchrone

Dispositif de suivi de l'exécution de l'évaluation des résultats de la formation.

- Feuilles d'émargement
- Autoévaluation de niveau en début de formation et fin de formation
- Evaluations d'entrainement tout au long de la formation
- Questionnaire de satisfaction à chaud et à froid.

FORMATION ÉLIGIBLE AU OPCO !