3 jours

PROGRAMME DE FORMATION **En présentiel** **À distance**

CYBERSÉCURITÉ, LES BONNES PRATIQUES EN ENTREPRISE

OBJECTIFS DE FORMATION

À l'issue de la formation, les participants seront capables de :

- Protéger son entreprises des risques d'intrusions numériques
- Comprendre la cybersécurité
- Mettre en place un plan de prévention

PARTICIPANTS

- Aucun

PRÉREQUIS

- Avoir une bonne connaissance de l'environnement Windows ou Mac

MÉTHODES PÉDAGOGIQUES ACTIVES

- Positionnement : Questionnaire préalable envoyé au participant
- Méthodes pédagogiques interactives tenant compte de l'expérience du stagiaire
- Apports théoriques et méthodologiques illustrés par de nombreux exercices pratiques
- Mises en situation sur des cas proposés par les participants, analyse de situation pour permettre l'appropriation des méthodes et des outils
- Support individuel de formation

ÉVALUATION

- Évaluation formative réalisée par l'intervenant tout au long de la formation afin de mesurer les acquisitions et les progressions
- Évaluation des acquis
- En option : certification TOSA
- Eligible au CPF
- Certification : 551 pts/1000 minimum
- Attestation : En dessous de 551pts/1000

LES PLUS

- PAI : un plan d'actions individuel sera formalisé en fin de formation.
- Programmes ajustables à vos attentes
- Accompagnement personnalisé
- Option démarche qualité :
  SQF – Suivi Qualité Formation : Synthèse détaillée et bilan du formateur.
- Cette formation est accessible à toute personne en situation
- de handicap, contact référent handicap au 02 43 61 08 47.
- Une expertise² de nos formateurs : technique et pédagogie active

PROGRAMME DE FORMATION

1.Cyber sécurité - Management des systèmes de sécurité au sein des entreprises TPE, PME

- Les enjeux de la sécurité des systèmes d'information en 2023
- Les besoins de sécurité dans une entreprise PME
- Notions de vulnérabilité, menace, attaque – Approche IA – en 2023
- Panorama de quelques menaces en entreprise
- Le droit des (Technologies de l'Information et de la Communication)
- T.I.C. et l'organisation de la sécurité en France

2.La gestion opérationnelle de la cybersécurité au sein d'une organisation

- Intégrer la sécurité au sein d'une organisation à travers une présentation synthétique de la famille des normes ISO/IEC 27000
- Insérer la sécurité dans les projets
- Les difficultés couramment rencontrées dans la prise en compte de la sécurité
- Présentation de poste/métier liés à la DSI/cybersécurité

3.Règle de sécurité et d'hygiène informatique en entreprise

- Bien connaître les systèmes d'information
- Maîtriser le réseau (sécurité, contrôle d'accès, sécuriser votre administration, wifi ...
- Sécurité des terminaux (maj applications raisons, codes malveillants, protéger vos données, renforcer les configurations
- Sensibilisation de vos collaborateurs, utilisateurs
- Gestion des utilisateurs (mots de passe, moyens d'authentification, sensibilisation
- Sécurité physique
- Contrôler la sécurité des systèmes d'information (maintenance, assurance, support, gestion des risques, audit etc...

4.La sécurité de vos données professionnelles et personnelles - RGPD / GDPR

- Comprendre le risque numérique
- Se protéger (les bonnes pratiques de l'informatique en entreprise)
- Sensibilisation des collaborateurs aux risques
- Comment choisir des solutions IT, des experts de confiance
- Que faire en cas d'attaques, d'incident

5.Conformité RGPD - Comment intégrer les obligations RGPD dans son activité, gérer ses données et garantir le droit des personnes ?

- Les 1er étapes – où commencer ? En 6 étapes
- Désigner un pilote
- Cartographier vos traitements de données personnelles
- Prioriser les actions à mener
- Gestions des risques
- Organiser les processus internes
- Documenter la conformité