Certisure®

L'essentiel de la Cybersécurité pour les collaborateurs

+ Certification ICDL

7 heures (1 journée)

OBJECTIFS PÉDAGOGIQUES

*Cette formation est conçue pour sensibiliser les **collaborateurs d'entreprises privées ou d'organismes publics** sur le risque engendré par le numérique, par la **formation aux bases de la cybersécurité**.*
Elle expose les concepts essentiels et les techniques à maîtriser pour protéger l'entreprise en maitrisant les risques et en anticipant les dangers. Cela passe notamment par la maîtrise des techniques et applications appropriées pour conserver une connexion sécurisée au réseau, pour utiliser Internet en toute sécurité et pour manipuler les données et les informations de manière adaptée.

PUBLIC CONCERNÉ

Salariés et agents, dirigeants ou cadre de l'administration, et tout public souhaitant être sensibilisé aux risques du numérique pour les entreprises et organismes publics.

PRÉ-REQUIS

Maîtrise de base informatique et internet, lire et parler français.

DURÉE ET ORGANISATION

- *1 journée (7h)*
- *à distance ou sur place*

LIEUX DE LA FORMATION

- *A distance (visio-conférence en direct)*
- *Sur place (Régions Occitanie et PACA)*

TARIF

415,00 € par stagiaire (possibilités de financement)
Passage certification inclus

CONTACTS CERTISURE

***Tel** 04 65 84 44 34 **E-Mail** contact@certisure.com*
***Inscription et Fiche en ligne :** cliquez ici*

CENTRE D'EXAMEN HABILITÉ ICDL

PROGRAMME

1°) **Comprendre les concepts** clés relatifs à l'importance d'assurer la sécurité des informations et des données, d'assurer leur sécurité physique, d'éviter le vol de données personnelles ou stratégiques de l'entreprise ou de l'organisme public
2°) **Protéger l'ordinateur**, **Connaître les différents types de réseaux**, protéger un dispositif mobile, un réseau contre les logiciels malveillants (malware) et contre les accès non-autorisés.
3°) **Débat sur la souveraineté numérique** et cloud de confiance (SecNumCloud), Cloud Act, accès aux données et RGPD
4°) **Naviguer sur Internet** et communiquer en toute sécurité.
5°) **Comprendre les problèmes de sécurité** liés à la communication, notamment en matière de courrier électronique.
6°) **Les attaques à éviter et les moyens à mettre en oeuvre** Ramsonware, hameçonnage (phishing), fraude au Président, ingénierie sociale, fuite de données.
Cas pratiques et mises en situation.

MOYENS ET MÉTHODES PÉDAGOGIQUES

Test de positionnement initial (bilan de compétences numériques), accès plateforme en ligne pour la documentation, formateur dédié.

PROFIL DU(DES) FORMATEUR(S)

Florian DE VAULX, **ingénieur diplômé** du Conservatoire national des arts et métiers (informatique) et titulaire du Master 2 Droit de l'Internet et systèmes d'information (Université de Strasbourg).

MODALITÉS D'ÉVALUATION

L'évaluation des acquis est réalisée tout au long de la formation
+ **PASSAGE Certification ICDL** Module Sécurité TI (prévoir 1h) en savoir plus