PROGRAMME DE FORMATION

# Référent cybersécurité en TPE/PME

*Cybersécurité & Protection des données*

| RÉFÉRENCE | VERSION | ÉDITION | DOMAINE |
|---|---|---|---|
| WF-0459 | V2026-005 | 3 novembre 2026 | Cybersécurité & Protection des données |

| DURÉE | MODALITÉ | PROGRAMME | SANCTION |
|---|---|---|---|
| 21 h | Distanciel asynchrone (e-learning) | 4 modules<br>12 leçons | Attestation<br>et certificat de réalisation |

## Objectifs pédagogiques

Définir les missions, les limites et la lettre de mission du référent cybersécurité dans une petite structure.

Reconnaître les menaces les plus fréquentes contre les TPE-PME et leurs signaux d'alerte.

Réaliser l'inventaire des équipements, comptes, données et prestataires, et un autodiagnostic de sécurité priorisé.

Mettre en place, avec la direction et le prestataire, les mesures essentielles : authentification, mises à jour, sauvegardes, sécurité de la messagerie et des paiements.

Rédiger la charte d'usage, organiser la sensibilisation des collaborateurs et encadrer les prestataires et services en ligne.

Appliquer les premiers réflexes face à un incident, puis piloter un plan d'action et en rendre compte à la direction.

# L'essentiel de la formation

## Public visé

Dirigeants, assistants de direction, responsables administratifs, salariés polyvalents ou responsables informatiques non spécialistes désignés pour coordonner la cybersécurité d'une TPE, d'une PME, d'une association ou d'un cabinet, souvent en lien avec un prestataire informatique.

## Prérequis

- Aucun prérequis en sécurité informatique. Utiliser couramment un ordinateur, une messagerie et des services en ligne.
- Connaître l'organisation de sa structure (activités, outils, prestataires) ou pouvoir se la faire décrire.
- Disposer d'un ordinateur avec une connexion internet, d'un tableur et d'un traitement de texte.

## Modalités et déroulement

Formation à distance, en ligne, de 21 h. Le fil rouge suit Hugo, négociateur de l'Agence Delmas nommé référent cybersécurité sans être informaticien. L'apprenant construit, leçon après leçon, les outils de sa propre structure (ou de l'agence fictive) : inventaire, autodiagnostic, règles d'authentification, procédure de paiement, charte, plan de sensibilisation, fiche réflexe, plan d'action. Plus de la moitié du temps est consacrée à ces mises en situation corrigées (études de cas, analyses d'erreurs, scénarios de décision, rédactions, jeux de rôle) ; les apports courts renvoient aux guides publics de l'ANSSI et de Cybermalveillance.gouv.fr. Accompagnement par un formateur par messagerie.

## Méthodes pédagogiques

- Positionnement en début de parcours
- Mises en situation et scénarios à décisions
- Études de cas
- Production de livrables professionnels
- Quiz et QCM d'auto-évaluation
- Accompagnement et retours du formateur

Répartition du temps de formation : **16 %** théorique · **60 %** pratique · **24 %** évaluation

## Moyens pédagogiques et techniques

- Plateforme de formation en ligne, accès individuel à distance
- Quiz et exercices interactifs en ligne
- Correction des productions sur grille de critères
- Messagerie avec le formateur

## Modalités d'évaluation

Positionnement initial non éliminatoire ; corrections détaillées des cas et scénarios ; livrables vérifiés sur grille critériée ; quatre quiz de module ; évaluation finale composée d'un cas pratique (diagnostic et plan d'action d'une structure fictive) et d'un questionnaire. Seuil de réussite interne : 70 %. Aucune certification ni habilitation n'est délivrée.

## Sanction

Une attestation de fin de formation et un certificat de réalisation sont remis au participant sous réserve de la réalisation du parcours.

Cette formation n'est pas présentée comme préparant à une certification enregistrée : elle ne comprend ni inscription ni présentation à des épreuves de certification, et n'ouvre droit à aucune délivrance de certification ni au financement par le CPF.

## Modalités et délais d'accès

La demande d'inscription peut être effectuée par téléphone, par courrier électronique ou au moyen du formulaire en ligne.

Un entretien ou un questionnaire de positionnement permet de vérifier l'adéquation de la formation avec les besoins, le niveau initial et les prérequis du candidat.

L'inscription devient définitive après validation du dossier administratif, acceptation des documents contractuels et, le cas échéant, confirmation du financement.

Les accès à la plateforme sont généralement activés sous 48 à 72 heures ouvrées après validation complète du dossier.

Les formations à distance sont proposées en entrées et sorties permanentes, sous réserve des délais ou dates imposés par le financeur ou le certificateur.

## Accessibilité aux personnes en situation de handicap

Vidéos sous-titrées et transcrites, fiches compatibles avec les lecteurs d'écran, navigation au clavier, captures d'écran d'exercice accompagnées d'une description textuelle. Référent handicap joignable à handicap@will-formation.com pour étudier toute adaptation (durée, supports, modalités d'évaluation).

## Tarif de la formation

Prix : **1 840 €**

Financement : prise en charge possible par les organismes financeurs, selon les critères d'éligibilité applicables.

Qualiopi processus certifié

La certification qualité a été délivrée au titre de la catégorie d'action suivante : ACTIONS DE FORMATION. Certificat QUA25070009. WILL FORMATION — Société par actions simplifiée à associé unique au capital de 30 000 € — NDA 11757059675 (cet enregistrement ne vaut pas agrément de l'État) — SIRET 893 713 180 00014 — 01 85 09 25 99 — info@will-formation.com — www.will-formation.com

# Programme détaillé

4 modules, 12 leçons — durée totale 21 h.

### 01 Le rôle de référent et l'état des lieux

1. Le rôle du référent cybersécurité dans une TPE/PME
2. Connaître les menaces qui visent les petites structures
3. Inventorier et diagnostiquer sa structure

### 02 Mettre en place les mesures essentielles

1. Comptes, mots de passe et double authentification
2. Postes, mobiles, mises à jour et réseau
3. Sauvegardes, messagerie et sécurité des paiements

### 03 Sensibiliser et encadrer les usages et les prestataires

1. Charte d'usage et règles du quotidien
2. Sensibiliser les collaborateurs
3. Encadrer prestataires, services en ligne et accès à distance

### 04 Réagir à un incident et piloter la sécurité dans la durée

1. Premiers réflexes et signalement d'un incident
2. Construire le plan d'action et le tableau de bord
3. Rendre compte à la direction et faire vivre la démarche