

**Annexe 1 au Cadre de réponse - ACM TRANSVERSES
(À fournir par module)**



**Intitulé du module : Sécuriser ses pratiques numériques
(Cybersécurité/RGPD)**

Contenu du programme de la journée

Horaires : matin : 9h00-12h30 et après-midi : 13h30-17h00

- **Accueil des stagiaires (15 min)**
 - Présentation des objectifs du module.
 - Icebreaker ludique sur la cybersécurité.
 - Test diagnostic sur la cybersécurité (positionnement)
- **Introduction à la cybersécurité en entreprise (45 min)**
 - Définition et enjeux de la cybersécurité.
 - Conséquences des cyberattaques pour une entreprise (exemples concrets avec entreprises touchées, impacts financiers et juridiques)
 - Panorama des menaces actuelles.
- **Sensibilisation au cadre réglementaire et le RGPD (30 min)**
 - Principes clés du Règlement Général sur la Protection des données (RGPD).
 - Droits et Obligations des entreprises et des employés.
 - Sanctions et responsabilités en cas de non-conformité.
 - Bonnes pratiques pour se conformer au RGPD.
- **Identifier, gérer et prévenir les risques principaux liés aux attaques numériques (2h)**
 - Techniques et détection : Hameçonnage (phishing), rançongiciels (ransomware, et malware)
 - Failles humaines : erreurs courantes et conséquences.
 - Identification des acteurs à contacter en cas de cyberattaque.
 - Bons réflexes et protocoles d'urgence.
 - Simulation d'une attaque : réaction et gestion.
- **Bonnes pratiques de sécurité et utilisation d'outils simples et efficaces (2h)**
 - Utilisation de mots de passe robustes et gestionnaire de mots de passe.
 - Sécurisation des équipements et des réseaux (Wi-Fi, mise à jour, antivirus, VPN).
 - Protection des données sensible : chiffrement des emails, limitation des accès, sécurisation des fichiers partagés.
 - Sécurisation du travail nomade.
- **Développer des réflexes sécuritaires adaptés dans son activité quotidienne (1h15)**
 - Checklist de sécurité : posture de vigilance, charte de cybersécurité...
 - Engagement personnel sur une bonne pratique à améliorer.
 - FAQ.
- **Bilan de la formation (15 min)**

Objectifs pédagogiques :

- Comprendre l'importance de la cybersécurité en entreprise.
- Sensibiliser aux réglementations en vigueur (RGPD).
- Identifier les principaux risques informatiques.
- Mettre en place les bonnes pratiques de sécurité.
- Utiliser des outils de protection efficaces.
- Gérer et prévenir les cyberattaques.
- Adopter des réflexes de sécurité au quotidien.

Public visé : Tout public

Prérequis :

Aucun prérequis nécessaire

Modalités pédagogiques :

- Une alternance d'apports théoriques et mises en application.
- Un suivi individualisé dans l'acquisition des savoirs et savoir-faire.
- Des techniques pédagogiques permettant de rythmer ou dynamiser l'animation (quiz, activités interactives, démonstrations en temps réel, etc.).
- Des techniques reposant sur des méthodes actives (mises en situation, exercices pratiques, co-productions, ateliers, etc.).
- Des techniques ludopédagogiques.
- Des techniques réflexives.

Durée de formation en heures et en jours : 7 heures – 1 jour

Organisme de formation :

IFPRA – Pôle Appel d'offres
168, rue Caponière, BP 46184
14061 Caen Cedex
Tél. 02 31 30 17 11
Mail : ifpra.ao@ac-normandie.fr