**Fiche de formation**

| **Titre** | Protégez vos données : La cybersécurité pour les MPME | | | |
| --- | --- | --- | --- | --- |
| **Mots clés** | Sécurité des données, cybersécurité, protection des données, sécurité de l'information, cybermenaces, violations de données, sécurité des réseaux, gestion des risques, meilleures pratiques en matière de sécurité, cyberconscience | | | |
| **Fourni par** | Des solutions informatiques pour tous | | | |
| **Langue** | Français | | | |
| **Espace de formation** | **☐ Principes fondamentaux de l'entrepreneuriat numérique dans le contexte des microentreprises**  **☐ Communication numérique et stratégie de marque**  **☐ Finance numérique**  ☒ **Cybersécurité** | | | |
| **Résultats de l'apprentissage** | **EntreComp** | | | |
| ☐ Idées et opportunités  ☒ Ressources  ☒ Into action  **Compétences spécifiques abordées :**  Mobilisation des ressources, mobilisation des autres, planification et gestion, gestion de l'incertitude, de l'ambiguïté et du risque, apprentissage par l'expérience | | | |
| **DigComp** | | | |
| ☐ Maîtrise de l'information et des données  ☐ Communication et collaboration  ☐ Création de contenu numérique  ☒ Sécurité  ☒ Résolution de problèmes  **Compétences spécifiques abordées :**  Protection des appareils, protection des données personnelles et de la vie privée, identification des besoins et des réponses technologiques | | | |
| **Niveau de compétence** | | | |
| ☐ Niveau 1  ☐ Niveau 2 | ☐ Niveau 3  ☐ Niveau 4 | ☒ Niveau 5  ☐ Niveau 6 | ☐ Niveau 7  ☐ Niveau 8 |
| **Fondation** | **Intermédiaire** | **Avancé** | **Expert** |
| **Description** | À l'ère du numérique, les données sont un atout précieux pour toutes les organisations, y compris les micros, petites et moyennes entreprises (MPME). Cependant, avec la dépendance croissante à l'égard de la technologie, le risque de cybermenaces et d'atteintes à la protection des données n'a jamais été aussi élevé.  Notre cours de formation, "Protégez vos données : La cybersécurité pour les MPME" est spécialement conçue pour permettre aux propriétaires, directeurs et employés de MPME d'acquérir les connaissances et les compétences nécessaires à la protection de leurs données précieuses et de leurs informations sensibles. | | | |
| **Objectifs d'apprentissage** | * Acquérir une compréhension globale des menaces liées à la cybersécurité et des mesures nécessaires pour protéger leurs MPME. * Disposer des connaissances et des compétences nécessaires à la mise en place d'une infrastructure informatique sécurisée. * Être capable de gérer la sécurité de l'information et de réagir efficacement aux incidents de cybersécurité. | | | |
| **Index (3 niveaux : Module-Unité-Section)** | **Module : Protégez vos données : La cybersécurité pour les MPME**  **Unité 1** : Introduction à la cybersécurité pour les MPME  Section 1.1. Comprendre la cybersécurité : définition et importance des politiques de sécurité  Section 1.2. Menaces communes de cybersécurité auxquelles sont confrontées les MPME  **Unité 2** : Mise en place d'une infrastructure TIC sécurisée  Section 2.1. Évaluer les vulnérabilités en matière de cybersécurité  Section 2.2. Utilisation efficace des solutions antivirus et antimalware  **Unité 3** : Gestion de la sécurité de l'information  Section 3.1. Pratiques et lignes directrices | | | |
| **Contenu développé** | **Module : Protégez vos données : La cybersécurité pour les MPME**  **Unité 1 : Introduction à la cybersécurité pour les MPME**  **Section 1.1.** Comprendre la cybersécurité : définition et importance des politiques de sécurité  Une politique de sécurité pour les micros, petites et moyennes entreprises (MPME) est un document formel qui décrit l'approche de l'organisation en matière de sécurité de l'information. Elle définit les règles, les lignes directrices et les responsabilités en matière de protection des actifs, des données et des systèmes de l'entreprise contre les menaces potentielles et les accès non autorisés. La politique doit être complète, claire et adaptée aux besoins et aux risques spécifiques de la MPME. Comprendre la cybersécurité et l'importance des politiques de sécurité pour les micros et petites entreprises après COVID est crucial pour plusieurs raisons :  **Sensibilisation aux cybermenaces** : La compréhension de la cybersécurité permet aux individus d'être **conscients des divers risques et menaces cybernétiques qui existent dans le paysage numérique.** Elle **les aide à reconnaître les vulnérabilités** et les faiblesses **potentielles** de leurs systèmes, de leurs réseaux et de leurs pratiques.  **Protection des données sensibles** : Les mesures de cybersécurité protègent les données sensibles et confidentielles contre l'accès non autorisé, le vol ou l'utilisation abusive. Cela est particulièrement important **pour les MPME, qui gèrent souvent des informations précieuses sur les clients, des** données financières et des éléments de propriété intellectuelle.  **Prévention des violations de données** : Les politiques de sécurité jouent un rôle important dans la prévention des violations de données et des cyberattaques. Elles **définissent des procédures et des lignes directrices visant à garantir que les données sont traitées en toute sécurité** et que les points d'entrée potentiels pour les attaquants sont réduits au minimum.  **Maintenir la continuité des activités** : La cybersécurité est essentielle au **bon fonctionnement d'une MPME**. Les politiques de sécurité aident à **identifier les risques potentiels** qui pourraient perturber les opérations commerciales et à élaborer des stratégies pour maintenir la continuité face aux cyberincidents.  **Conformité et exigences légales** : De nombreux secteurs ont des réglementations spécifiques et des exigences légales concernant la protection des données et la cybersécurité. **Comprendre la cybersécurité permet aux MPME de respecter ces réglementations, d'éviter les sanctions** et de conserver la confiance des clients et des partenaires.  **Renforcer la confiance des clients** : La démonstration d'un engagement en faveur de la cybersécurité et la mise en place de politiques de sécurité solides **peuvent renforcer la confiance des clients à l'égard d'une MPME**. Les clients sont plus enclins à faire des affaires avec des organisations qui accordent la priorité à la protection de leurs données et de leur vie privée.  **Prévention des pertes financières : les cyberattaques peuvent entraîner des pertes financières importantes pour les MPME**. La compréhension de la cybersécurité et la mise en œuvre de politiques de sécurité efficaces **peuvent contribuer à atténuer les risques financiers associés aux violations de données et autres cyberincidents.**  **Gestion de la réputation** : Une cyberattaque réussie peut **nuire à la réputation d'une MPME**, entraînant une **perte de clients et d'opportunités**. Les politiques de sécurité aident à prévenir les incidents et démontrent l'engagement de l'organisation à protéger les informations.  **Préparation aux crises** : La sensibilisation à la cybersécurité et les politiques de sécurité aident les MPME à se **préparer à des crises potentielles**, ce qui réduit le temps de récupération.  **Formation et sensibilisation des employés** : Comprendre la cybersécurité permet aux organisations de fournir une formation appropriée à leurs employés. En **informant le personnel** des meilleures pratiques, des menaces potentielles et des politiques de sécurité**, on contribue à créer une solide culture de la sécurité** au sein de l'organisation.  **Avantage concurrentiel** : Mettre l'accent sur la cybersécurité et mettre en place des politiques de sécurité efficaces peut **donner aux MPME un avantage concurrentiel**. Les **clients et les partenaires accordent souvent la priorité à la sécurité** lorsqu'ils choisissent leurs partenaires commerciaux, ce qui fait de la cybersécurité un précieux facteur de différenciation.  En conclusion, il est essentiel pour les MPME de comprendre la cybersécurité et l'importance des politiques de sécurité pour protéger leurs données, maintenir la continuité de leurs activités, se conformer aux réglementations et instaurer la confiance avec les clients et les parties prenantes. En s'attaquant de manière proactive aux cybermenaces, les MPME peuvent renforcer leur résilience et garantir un environnement numérique sûr pour leurs activités.  **Section 1.2.** Menaces communes de cybersécurité auxquelles sont confrontées les MPME  Les micros, petites et moyennes entreprises (MPME) deviennent de plus en plus des cibles pour les cybercriminels en raison de la valeur de leurs données et de leurs défenses de cybersécurité potentiellement plus faibles que celles des grandes organisations. Les menaces de cybersécurité les plus courantes auxquelles sont confrontées les MPME sont les suivantes :  **Attaques par hameçonnage** : Le phishing est une technique par laquelle les cybercriminels envoient des courriels, des messages ou des sites web trompeurs pour inciter les employés à divulguer des informations sensibles telles que des identifiants de connexion, des données financières ou des informations personnelles.  **Ransomware** : Les ransomwares sont des logiciels malveillants qui cryptent les données d'une organisation et les rendent inaccessibles jusqu'au paiement d'une rançon. Les MPME peuvent être ciblées en raison de mesures de sécurité perçues comme plus faibles.  **Infections par des logiciels malveillants** : Les MPME sont sensibles à divers types de logiciels malveillants, notamment les virus, les chevaux de Troie et les logiciels espions. Ces programmes malveillants peuvent perturber les opérations, voler des données ou obtenir un accès non autorisé aux systèmes.  **Menaces d'initiés** : Les menaces d'initiés impliquent des actions malveillantes ou des erreurs involontaires commises par des employés ou des personnes ayant accès aux systèmes, aux données ou aux réseaux d'une organisation.  **Attaques par ingénierie sociale** : L'ingénierie sociale consiste à manipuler des personnes pour qu'elles révèlent des informations confidentielles, telles que des mots de passe ou des identifiants de connexion. Cela peut se produire par le biais d'appels téléphoniques, d'interactions en personne ou des médias sociaux.  **Dispositifs IoT non sécurisés** : De nombreuses MPME utilisent des appareils de l'internet des objets (IoT), tels que des caméras ou des capteurs intelligents. S'ils ne sont pas correctement sécurisés, ces appareils peuvent devenir des points d'entrée permettant aux attaquants d'infiltrer le réseau.  **Faiblesse des mots de passe et de l'authentification** : Des pratiques inadéquates en matière de mots de passe, telles que l'utilisation de mots de passe faciles à deviner ou leur réutilisation sur plusieurs comptes, peuvent rendre les MPME vulnérables aux attaques par force brute ou au bourrage d'informations d'identification.  **Violation de données** : Les MPME collectent et stockent souvent des données précieuses sur leurs clients. Si elles ne sont pas protégées de manière adéquate, une violation de données peut entraîner une atteinte à la réputation, une perte financière et des conséquences juridiques.  **Attaques par déni de service (DoS)** : Les attaques par déni de service submergent les systèmes ou le réseau d'une organisation d'un flot de trafic, provoquant des perturbations et des temps d'arrêt.  **Absence de mises à jour et de correctifs réguliers des logiciels** : Le fait de ne pas appliquer en temps voulu les mises à jour et les correctifs de sécurité aux logiciels et aux systèmes d'exploitation peut exposer les MPME à des vulnérabilités connues.  **Préoccupations liées à la sécurité de l'informatique dématérialisée** : Le stockage de données et d'applications dans le nuage peut être pratique pour les MPME, mais il peut aussi présenter des risques de sécurité s'il n'est pas configuré et géré de manière appropriée.  **Attaques de la chaîne d'approvisionnement** : Les cybercriminels peuvent cibler les MPME comme moyen d'accéder à des organisations plus importantes en exploitant les vulnérabilités de la chaîne d'approvisionnement.  **Paramètres de sécurité mal configurés** : Des paramètres de sécurité mal configurés sur des systèmes, des applications ou des dispositifs de réseau peuvent créer des failles de sécurité involontaires.  **Manque de sensibilisation des employés à la cybersécurité** : Une sensibilisation et une formation insuffisantes des employés à la cybersécurité peuvent accroître le risque d'être victime de diverses cybermenaces.  Pour atténuer ces menaces, les MPME devraient investir dans des mesures de cybersécurité, telles que la formation régulière des employés, des contrôles d'accès robustes, des méthodes d'authentification fortes, une infrastructure TIC sécurisée, une gestion de la sécurité de l'information, des logiciels de sécurité à jour et un plan de réponse aux incidents bien défini. Des pratiques proactives en matière de cybersécurité peuvent réduire considérablement le risque d'être victime de cyberattaques et protéger les actifs précieux et la réputation de l'organisation**.**  **Unité 2 : Mise en place d'une infrastructure TIC sécurisée**  **Section 2.1.** Évaluer les vulnérabilités en matière de cybersécurité  L'évaluation des vulnérabilités en matière de cybersécurité est essentielle pour les MPME afin d'identifier les faiblesses potentielles de leurs systèmes, de leurs infrastructures TIC, de leurs réseaux et de leurs pratiques. Voici les étapes qu'une MPME peut suivre pour évaluer ses vulnérabilités en matière de cybersécurité :  **Identifier les actifs et les données** : Commencez par identifier tous les actifs, l'infrastructure TIC, les systèmes, les appareils et les données que votre MPME utilise ou stocke. Cela comprend le matériel, les logiciels, les serveurs, les dispositifs de réseau, les services en nuage et les informations sensibles.  **Procéder à une évaluation des risques** : Effectuer une évaluation complète des risques afin d'identifier les menaces potentielles, les vulnérabilités et l'impact potentiel d'un incident cybernétique sur votre organisation. Cette évaluation permettra de hiérarchiser les efforts pour traiter en premier lieu les risques les plus critiques.  **Tests de pénétration** : Envisagez d'effectuer des tests de pénétration (piratage éthique) pour simuler des cyberattaques réelles sur vos systèmes et réseaux. Cela permet d'identifier les points d'entrée potentiels et les points faibles de vos défenses de sécurité.  **Examen de la sécurité des réseaux** : Évaluez la sécurité de votre infrastructure réseau, y compris les pare-feu, les routeurs, les commutateurs et les réseaux sans fil. Assurez-vous que ces dispositifs sont correctement configurés et que des contrôles d'accès sont en place.  **Évaluer les logiciels et les applications** : Vérifiez régulièrement la présence de mises à jour et de correctifs de sécurité pour tous les logiciels et applications utilisés dans votre organisation. Les logiciels obsolètes peuvent créer des vulnérabilités que les cyber-attaquants peuvent exploiter.  **Évaluer la sécurité des terminaux** : Évaluez les mesures de sécurité des terminaux (ordinateurs portables, smartphones, tablettes) utilisés par les employés. Mettez en œuvre des logiciels antivirus et de cryptage, et appliquez des politiques d'accès aux données de l'entreprise sur les appareils personnels.  **Vérifier la sécurité physique** : Ne négligez pas la sécurité physique. Évaluez les contrôles d'accès physiques aux locaux de votre entreprise, aux salles de serveurs et aux zones sensibles où sont stockés les données et les équipements.  **Examiner le niveau de sensibilisation des employés** : Évaluez le niveau de sensibilisation de vos employés à la cybersécurité. Organisez des formations et des ateliers pour les informer des cybermenaces courantes et des meilleures pratiques en matière de sécurité des données.  **Réviser les politiques en matière de mots de passe** : Veillez à ce que des politiques de mot de passe solides soient en place, notamment en exigeant des mots de passe complexes, en changeant régulièrement de mot de passe et en ne réutilisant pas les mots de passe sur plusieurs comptes.  **Sécuriser les services en nuage** : Si vous utilisez des services en nuage, évaluez leurs caractéristiques de sécurité et assurez-vous qu'elles répondent aux exigences de votre organisation. Mettez en œuvre l'authentification multifactorielle et le cryptage pour les données sensibles stockées dans le nuage.  **Analyser les politiques de sécurité** : Réviser et mettre à jour régulièrement les politiques de sécurité. Veillez à ce qu'elles soient conformes aux normes du secteur et aux exigences de conformité. Ces politiques doivent couvrir des domaines tels que la protection des données, les contrôles d'accès, la réponse aux incidents et l'utilisation acceptable.  **Auditer les fournisseurs tiers** : Si vous travaillez avec des fournisseurs ou des prestataires de services tiers, évaluez leurs pratiques en matière de cybersécurité et leurs mesures de protection des données afin de vous assurer qu'ils n'introduisent pas de risques supplémentaires.  **Préparation à la réponse à un incident** : Évaluez le plan de réponse aux incidents de votre organisation pour vous assurer qu'il est complet et qu'il couvre les mesures appropriées à prendre en cas d'incident cybernétique.  **Audits de sécurité réguliers** : Réalisez des audits et des évaluations de sécurité périodiques afin de maintenir une compréhension continue de la position de votre organisation en matière de cybersécurité.  **Assurer la sécurité des réseaux Wi-Fi :** La sécurisation des réseaux Wi-Fi est essentielle pour empêcher les accès non autorisés et protéger les données sensibles.  Cela peut être atteint par :   * modification des informations d'identification par défaut * l'utilisation d'un cryptage fort * activation de l'accès protégé Wi-Fi 3 (WPA3) ou WPA2 avec AES (norme de cryptage avancée) pour un cryptage fort * éviter d'utiliser des méthodes de cryptage obsolètes et vulnérables telles que le WEP (wired equivalent privacy) * modifier l'identifiant de l'ensemble des services (SSID) par défaut en un nom unique qui ne révèle pas d'informations sur votre entreprise ou votre organisation * désactiver la diffusion du SSID pour rendre votre réseau moins visible pour les attaquants potentiels * la mise en place d'un réseau d'invités distinct pour les visiteurs ou les clients, qui les isole de votre réseau interne principal, à l'aide de mots de passe robustes * l'activation du filtrage des adresses mac pour n'autoriser que des appareils spécifiques avec des adresses mac préapprouvées à se connecter à votre réseau wi-fi * maintenir le firmware à jour * désactivation de la gestion à distance sur le routeur pour empêcher tout accès non autorisé depuis l'extérieur du réseau * activer le pare-feu et le cryptage du réseau * la désactivation du protocole UPNP (Universal Plug and Play) sur votre routeur, car il peut être exploité par des pirates pour ouvrir des ports et exposer votre réseau à des menaces potentielles * la surveillance de l'activité du réseau * la sécurisation de l'accès physique * la formation des employés.   **Section 2.2.** Utilisation efficace des solutions antivirus et antimalware **:**  L'utilisation efficace de solutions antivirus et antimalware est essentielle pour les micros, petites et moyennes entreprises (MPME) afin de protéger leur infrastructure, leurs systèmes, leurs réseaux et leurs données TIC contre diverses cybermenaces.  Voici quelques bonnes pratiques pour utiliser efficacement les solutions antivirus et antimalware :  **Choisissez une solution complète** : Choisissez un logiciel antivirus et antimalware complet et réputé qui offre une protection en temps réel, des mises à jour régulières et des analyses fréquentes pour détecter et supprimer les logiciels malveillants.  **Maintenir le logiciel à jour** : Veillez à ce que les logiciels antivirus et antimalware soient à jour avec les dernières définitions de virus et mises à jour de la base de données. C'est essentiel pour détecter les menaces nouvelles et émergentes et s'en protéger.  **Activer l'analyse en temps réel** : Activez les fonctions d'analyse en temps réel du logiciel antivirus pour vérifier automatiquement si les fichiers, les téléchargements et les pièces jointes aux courriels contiennent des logiciels malveillants au fur et à mesure qu'ils sont consultés.  **Programmer des analyses régulières** : Configurez des analyses programmées pour qu'elles s'exécutent à des moments opportuns où le système est le moins susceptible d'être utilisé, par exemple en dehors des heures de bureau.  **Activer les mises à jour automatiques** : Activez les mises à jour automatiques du logiciel antivirus et du système d'exploitation pour garantir une protection continue contre les menaces les plus récentes.  **Effectuer des analyses complètes du système** : Effectuez régulièrement des analyses complètes du système afin de vérifier minutieusement tous les fichiers, y compris ceux qui se trouvent dans les zones les moins fréquemment consultées.  **Mettre en quarantaine et isoler les menaces** : Configurer le logiciel antivirus pour qu'il mette en quarantaine ou isole les menaces détectées, afin d'éviter qu'elles ne se propagent ou ne causent d'autres dommages.  **Analyser les périphériques externes** : Scannez tous les périphériques externes, tels que les clés USB ou les disques durs externes, avant d'accéder aux fichiers afin d'empêcher l'introduction de logiciels malveillants dans le réseau.  **Sensibiliser les employés** : Sensibiliser les employés à l'importance de la protection antivirus et antimalware et les former à la prudence en ce qui concerne les pièces jointes, les téléchargements et les liens afin d'éviter d'introduire par inadvertance des logiciels malveillants.  **Mettre en œuvre une protection des points finaux** : Envisagez d'utiliser des solutions de protection des points d'accès qui offrent une défense multicouche contre divers types de menaces, y compris les ransomwares et les exploits de type " zero-day ".  **Gestion centralisée** : Si vous gérez plusieurs systèmes, utilisez des outils de gestion centralisée pour surveiller et contrôler les logiciels antivirus et antimalware sur tous les appareils à partir d'une interface unique.  **Maintenance régulière du système :** Effectuez régulièrement des tâches de maintenance du système, telles que le nettoyage et la défragmentation du disque, afin d'optimiser les performances du système et d'améliorer l'efficacité des analyses antivirus.  **Surveiller les alertes et y répondre** : Configurer le logiciel antivirus pour qu'il envoie des alertes en cas de détection de menaces, répondre rapidement à ces alertes et les examiner pour prendre les mesures qui s'imposent.  **Évaluations périodiques de la sécurité** : Effectuer des évaluations et des audits de sécurité périodiques afin d'évaluer l'efficacité des solutions antivirus et antimalware et d'identifier les domaines susceptibles d'être améliorés.  **Stratégies de sauvegarde et de récupération des données :** Mettez en œuvre une stratégie de sauvegarde régulière des données afin de garantir la sécurité des fichiers importants en cas d'infection grave par un logiciel malveillant ou d'attaque par un ransomware. Établissez un calendrier de sauvegarde de routine pour vous assurer que les données critiques sont sauvegardées régulièrement. En fonction du volume de données et de la fréquence des changements, des sauvegardes quotidiennes, hebdomadaires ou mensuelles peuvent être appropriées. En outre, les MPME peuvent utiliser des solutions de sauvegarde automatisées pour réduire le risque d'erreur humaine et s'assurer que les sauvegardes sont systématiquement effectuées sans intervention manuelle. N'oubliez pas de stocker les données de sauvegarde dans plusieurs emplacements physiques afin d'atténuer le risque de perte de données en cas de vol, d'incendie ou d'autres catastrophes affectant un seul emplacement. En plus des sauvegardes sur site, les sauvegardes en nuage constituent une solution rentable et fiable. Les sauvegardes en nuage offrent une évolutivité, une accessibilité et une redondance des données aisées.  N'oubliez pas que la cybersécurité est un processus continu. Des évaluations régulières, une surveillance continue et des mesures rapides pour remédier aux vulnérabilités sont essentielles pour protéger votre MPME contre les cybermenaces en constante évolution.  **Unité 3 : Gestion de la sécurité de l'information**  **Section 3.1.** Pratiques et lignes directrices  La gestion de la sécurité de l'information est cruciale pour les micros, petites et moyennes entreprises (MPME) afin de **protéger leurs données sensibles**, de **maintenir la confiance des clients** et de **sauvegarder leurs opérations commerciales.**  Voici quelques lignes directrices et pratiques clés que les MPME peuvent suivre pour gérer efficacement la sécurité de l'information :  **Évaluation des risques** : Procéder à une évaluation approfondie des risques afin d'identifier les vulnérabilités et les menaces potentielles pour la sécurité de l'information. Comprendre les types de données traitées par l'organisation, les risques associés à chaque type de données et l'impact d'une violation de la sécurité.  **Politiques et procédures de sécurité** : Élaborer et mettre en œuvre des politiques et des procédures complètes de sécurité de l'information qui couvrent des domaines tels que le traitement des données, les contrôles d'accès, la gestion des mots de passe, la sauvegarde des données et la réponse aux incidents.  **Formation des employés** : Former tous les employés aux meilleures pratiques en matière de sécurité de l'information, aux protocoles de protection des données et à la manière de reconnaître les menaces de sécurité telles que les attaques par hameçonnage et d'y répondre. La formation des employés à la cybersécurité est essentielle pour une stratégie de défense complète. Les attaques d'ingénierie sociale et le phishing sont des menaces courantes ciblant les MPME. Les employés doivent être en mesure d'identifier et d'atténuer les risques en reconnaissant les courriels de phishing, en traitant les pièces jointes suspectes et en mettant en œuvre des protocoles d'authentification des courriels. En ce sens, la sécurité des mots de passe joue un rôle crucial dans la protection des données sensibles. Les employés doivent connaître les pratiques de création de mots de passe forts, de mise en œuvre de l'authentification multifactorielle (AMF) et de gestion des politiques de mot de passe au sein de l'organisation.  **Contrôles d'accès** : Mettre en place des contrôles d'accès pour s'assurer que seul le personnel autorisé a accès aux données sensibles. Utilisez le contrôle d'accès basé sur les rôles pour restreindre l'accès en fonction des rôles et des responsabilités professionnelles.  **Traitement sécurisé des données** : Établir des lignes directrices pour le traitement sécurisé des données, à la fois sous forme numérique et physique. Cela comprend le stockage approprié, le cryptage et l'élimination sécurisée des informations sensibles.  **Mises à jour et correctifs réguliers des logiciels** : Maintenir tous les logiciels, y compris les systèmes d'exploitation, les applications et les outils de sécurité, à jour avec les derniers correctifs et mises à jour pour remédier aux vulnérabilités connues.  **Pare-feu et logiciels antivirus** : Déployer des pares-feux et des logiciels antivirus/antimalware réputés pour se protéger contre les menaces extérieures.  **Configuration sécurisée du réseau** : Configurez les réseaux de manière sécurisée, y compris les réseaux Wi-Fi, afin d'empêcher les accès non autorisés et l'interception des données.  **Sauvegarde et récupération des données** : Sauvegarder régulièrement les données critiques et tester le processus de restauration des données pour assurer la continuité de l'activité en cas de perte de données ou de cyberattaque.  **Plan d'intervention en cas d'incident** : Élaborer un plan d'intervention clair qui décrit les mesures à prendre en cas d'atteinte à la sécurité ou à la protection des données. Attribuez des rôles et des responsabilités au personnel clé pour une gestion efficace des incidents. Il est essentiel de se préparer et de réagir efficacement aux incidents de cybersécurité pour minimiser les dommages et atténuer les risques.  **Gestion des fournisseurs** : Si la MPME fait appel à des fournisseurs ou à des prestataires de services tiers, il convient de s'assurer que leurs pratiques en matière de sécurité de l'information sont conformes aux normes de votre organisation.  **Contrôle et audit continus** : Mettre en œuvre une surveillance continue et des audits de sécurité périodiques afin de détecter et de traiter de manière proactive les problèmes de sécurité potentiels.  **Respect de la confidentialité des données** : Se tenir au courant des lois et réglementations relatives à la confidentialité des données qui s'appliquent aux activités de la MPME. Respecter les exigences en matière de protection des données et informer les clients sur les pratiques de traitement des données.  **Sensibilisation à la sécurité et culture de la sécurité** : Favoriser une culture de sensibilisation et de responsabilité en matière de sécurité parmi les employés. Encourager le signalement des incidents et des problèmes de sécurité.  **Examens réguliers de la sécurité** : Procéder régulièrement à des examens de la sécurité et à des évaluations des risques afin d'identifier les menaces émergentes et les domaines susceptibles d'être améliorés.  En gérant de manière proactive la sécurité de l'information, les MPME peuvent réduire le risque de violation des données, protéger les informations sensibles et instaurer la confiance avec les clients et les partenaires, contribuant ainsi au succès à long terme de l'entreprise. | | | |
| **5 entrées de glossaire** | **Internet des objets (IoT).** L'internet des objets, ou IdO, est un système de dispositifs informatiques, de machines mécaniques et numériques, d'objets, d'animaux ou de personnes interconnectés, dotés d'identifiants uniques (UID) et capables de transférer des données sur un réseau sans nécessiter d'interaction entre humains ou entre humains et ordinateurs.  Source : TechTarget TechTarget <https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT>  **Déni de service (DoS).** Le déni de service est un type de cyberattaque conçu pour désactiver, arrêter ou perturber un réseau, un site web ou un service. En général, un logiciel malveillant est utilisé pour interrompre ou inhiber le flux normal de données entrant et sortant d'un système afin de rendre la cible inutilisable ou inaccessible pendant un certain temps. Un exemple d'attaque DoS : lorsqu'un site web est consulté massivement et de manière répétée à partir de différents endroits, empêchant les visiteurs légitimes d'accéder au site web.  Source : Trend Micro Trend Micro <https://www.trendmicro.com/vinfo/us/security/definition/denial-of-service-dos>  **Authentification multi-facteurs.** L'authentification multifactorielle (AMF) est une méthode d'authentification qui exige de l'utilisateur qu'il fournisse au moins deux facteurs de vérification pour accéder à une ressource telle qu'une application, un compte en ligne ou un réseau privé virtuel (VPN). L'AMF est un élément essentiel d'une politique solide de gestion des identités et des accès (IAM). Plutôt que de demander un nom d'utilisateur et un mot de passe, l'AMF exige un ou plusieurs facteurs de vérification supplémentaires, ce qui réduit la probabilité de réussite d'une cyberattaque.  Source : Onelogin <https://www.onelogin.com/learn/what-is-mfa>  **Service Set Identifier (SSID).** (Service Set IDentifier) Nom attribué à un réseau Wi-Fi (sans fil). Tous les appareils du réseau doivent utiliser ce nom sensible à la casse pour communiquer par Wi-Fi. Il s'agit d'une chaîne de texte d'une longueur maximale de 32 octets. Les routeurs et les points d'accès sans fil sont dotés d'un SSID par défaut, qui peut être le nom du fabricant, comme "linksys" ou "netgear", ou simplement "default". Certains appareils utilisent leur numéro de modèle comme SSID. À l'aide d'un navigateur Web, le SSID (et le mot de passe) peut être modifié manuellement dans les paramètres de configuration de l'appareil.  **Source : PcMag** [**https://www.pcmag.com/encyclopedia/term/ssid**](https://www.pcmag.com/encyclopedia/term/ssid)  **Universal Plug and Play (UPnP).** UPnP (Universal Plug and Play) est un protocole de mise en réseau qui permet aux appareils de se découvrir mutuellement et de se connecter sans nécessiter de configuration manuelle ou d'intervention de l'utilisateur. Le protocole automatise toutes les étapes nécessaires à la reconnaissance et à la communication entre les appareils d'un même réseau.  Source : PhoenixNap <https://phoenixnap.com/blog/what-is-upnp>  **Exploits du jour zéro** : Un exploit de type "zero-day" (0day) est une cyberattaque ciblant une vulnérabilité logicielle inconnue de l'éditeur du logiciel ou des vendeurs d'antivirus. L'attaquant repère la vulnérabilité du logiciel avant toute partie intéressée par son atténuation, crée rapidement un exploit et l'utilise pour une attaque. Ces attaques ont de grandes chances de réussir car les défenses ne sont pas en place. Les attaques de type "zero-day" constituent donc une grave menace pour la sécurité.  Source : Imperva Imperva <https://www.imperva.com/learn/application-security/zero-day-exploit/>  **Ransomware** : Les ransomwares sont des logiciels malveillants qui empêchent ou limitent l'accès des utilisateurs à leur système, soit en verrouillant l'écran du système, soit en verrouillant les fichiers de l'utilisateur jusqu'à ce qu'une rançon soit payée. Les familles de ransomwares les plus modernes, regroupées sous le nom de cryptoransomwares, chiffrent certains types de fichiers sur les systèmes infectés et obligent les utilisateurs à payer une rançon par le biais de certaines méthodes de paiement en ligne afin d'obtenir une clé de déchiffrement.  Source : Trend Micro **Trend Micro** [**https://www.trendmicro.com/vinfo/us/security/definition/ransomware**](https://www.trendmicro.com/vinfo/us/security/definition/ransomware) | | | |
| **5 questions d'auto-évaluation à choix multiples** | **Question 1. Qu'est-ce qu'une politique de sécurité ?**  Option a : Il s'agit d'un document informel qui décrit l'approche de l'organisation en matière de  la sécurité de l'information  Option b : il s'agit d'un document formel qui fixe les règles, les lignes directrices et les responsabilités.  pour protéger les actifs, les données et les systèmes de l'entreprise contre les menaces potentielles et les risques d'abus.  accès non autorisé  Option c : Une politique visant à protéger uniquement les actifs de l'entreprise  Option d : Les trois options sont correctes  **Option correcte : b**  **Question 2. Pourquoi est-il important de comprendre la cybersécurité et la sécurité ?**  **politiques ?**  Option a : La compréhension de la cybersécurité permet aux individus d'être conscients des différentes menaces qui pèsent sur la sécurité de l'information.  les cybermenaces et les risques qui existent dans le paysage numérique  Option b : les mesures de cybersécurité protègent les données sensibles et confidentielles contre  l'accès non autorisé, le vol ou l'utilisation abusive  Option c : Les politiques de sécurité jouent un rôle important dans la prévention des atteintes à la protection des données et dans l'amélioration de la qualité des données.  cyber-attaques  Option d : Les trois réponses sont correctes  **Option correcte : d**  **Question 3. Veuillez indiquer la réponse qui est vraie :**  Option a : Les cyberattaques peuvent entraîner des pertes financières négligeables pour les MPME.  Option b : une cyber-attaque réussie peut nuire à la réputation d'une MPME, ce qui peut entraîner une perte de revenus.  la perte de clients et d'opportunités  Option c : Sensibiliser le personnel aux meilleures pratiques, aux menaces potentielles et à la sécurité  les politiques contribuent à créer une forte culture de la sécurité au sein de l'organisation  Option d : Souvent, les clients et les partenaires n'accordent pas la priorité à la sécurité lorsqu'ils choisissent un produit ou un service.  les partenaires commerciaux, faisant de la cybersécurité un facteur de différenciation précieux  **Option correcte : b et c**  **Question 4. Veuillez indiquer les menaces de cybersécurité les plus courantes pour les MPME.**  Option a : Traitements d'initiés, infections et paramètres de sécurité bien configurés  Option b : violations de données, faiblesse des mots de passe et de l'authentification, infections par des logiciels malveillants  Option c : Attaques par hameçonnage, attaques de la chaîne d'approvisionnement, dispositifs IdO non sécurisés  Option d : Toutes les réponses sont incorrectes  **Option correcte : b et c**  **Question 5. Quelles mesures une MPME peut-elle prendre pour évaluer sa cybersécurité ?**  **vulnérabilités ?**  Option a : Vérifier la sécurité physique, examiner la sensibilisation des employés et faire le point  Politiques en matière de mots de passe  Option b : identifier les actifs et les données, procéder à une évaluation des risques et vérifier l'état physique des actifs et des données.  Sécurité  Option c : Assurer la sécurité du réseau wi-fi, test de pénétration et évaluation  Logiciels et applications  Option d : Les trois réponses sont correctes  **Option correcte : d** | | | |
| **Bibliographie et autres références** | Conseil Forbes Tech. (2023, 25 mai). Petit mais puissant : Cybersecurity Best Practices for SMEs. Forbes. <https://www.forbes.com/sites/forbestechcouncil/2023/05/25/small-but-mighty-cybersecurity-best-practices-for-smes/?sh=44510c371a33>  Devonshire Green (n.d.). L'importance de la cybersécurité pour les PME. Devonshire Green. <https://www.devonshiregreen.uk/the-importance-of-cybersecurity-for-smes/>  Agence de l'Union européenne pour la cybersécurité (ENISA). (2021). Cybersécurité pour les PME : défis et recommandations. ENISA. <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes/@@download/fullReport>  Agence de l'Union européenne pour la cybersécurité (ENISA). (2021). Guide de cybersécurité pour les PME. ENISA. <https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes/@@download/fullReport>  Ministère de l'économie et de la compétitivité (Espagne). (2021). Plan de numérisation pour les PME [PDF]. Gouvernement de l'Espagne. <https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/210902-digitalisation-smes-plan.pdf>  Yerik Afrianto Singgalen. (2021, août). Exploration de la sensibilisation des MPME à la cybersécurité et de la gestion des risques : Information Security Awareness. ResearchGate. <https://www.researchgate.net/publication/353622348_Exploring_MSMEs_>  Sensibilisation à la cybersécurité et gestion des risques Sensibilisation à la sécurité de l'information | | | |
| **Matériel connexe** | DREAM\_WP3\_Cybersécurité\_ITSFA\_FR | | | |
| **Vidéo (le cas échéant)** | [lien] | | | |