LIVRE BLANC

TECH TIME 2 SKILL

Cofinancé par
l'Union européenne

AVERTISSEMENT

Le projet Tech Time 2 Skill a été lancé en janvier 2023 par un consortium de trois organismes de formation : Simplon.co en France, Becode en Belgique et Factoría F5 en Espagne, en collaboration avec des entreprises partenaires et des associations professionnelles (PIMEC, Agoria, Agence du Numérique dans le cadre de Digital Wallonia et Microsoft).

Cofinancé par l'Union européenne. Les points de vue et opinions exprimés sont toutefois uniquement ceux des auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour la santé et le numérique (HaDEA). Ni l'Union européenne ni la HaDEA ne peuvent en être tenues responsables.

AVANT-PROPOS

La pandémie du COVID-19 a agi comme un puissant catalyseur de la transformation numérique de l'Europe. Selon McKinsey, la COVID-19 a accéléré l'adoption des technologies numériques en Europe d'environ sept ans. Rien qu'entre décembre 2019 et juin 2020, le nombre d'entreprises proposant des produits et services au moins partiellement numérisés a augmenté de 16 %. À la mi-2020, une entreprise sur deux s'était déjà engagée dans la voie de la transformation numérique.

Un autre changement radical est survenu avec l'émergence de l'IA générative, notamment le lancement de ChatGPT en novembre 2022. Cette évolution n'était pas prévue lors de la conception initiale du projet, mais elle a rapidement redéfini les attentes du marché et les besoins en compétences. En conséquence, notre contenu de formation a évolué pour aborder l'utilisation pratique et responsable de l'IA générative dans les PME, garantissant ainsi la pertinence et l'applicabilité du programme pour les apprenants et les employeurs.

Dans ce contexte de changements rapides, Tech Time 2 Skill aide depuis près de trois ans les particuliers et les petites et moyennes entreprises (PME) à comprendre l'IA et la cybersécurité et à transformer cette compréhension en mesures concrètes.

Le projet est cofinancé par l'Union européenne dans le cadre du programme « Le programme pour une Europe numérique » (DIGITAL) et mis en œuvre avec le soutien de HaDEA, l'Agence exécutive européenne pour la santé et le numérique. Le programme DIGITAL renforce les capacités numériques essentielles de l'Europe (dans les domaines de l'IA, de la cybersécurité, du cloud computing et de la microélectronique) et encourage leur utilisation efficace dans des secteurs clés tels que l'énergie, le climat et l'environnement, l'industrie manufacturière, l'agriculture et la santé. Son objectif : accélérer la reprise et stimuler la transformation numérique en cours en Europe.

Ce livre blanc présente le parcours Tech Time 2 Skill d'une manière directement applicable par les praticiens. Il rassemble des leçons pratiques, des témoignages humains et des outils prêts à l'emploi, distillant ce que nous avons construit, ce qui a changé et comment d'autres peuvent adapter l'approche à leur propre contexte.

En bref : Tech Time 2 Skill démystifie l'IA et la cybersécurité pour les lieux de travail réels et ce livre blanc présente les méthodes et les idées qui ont fonctionné.

APERÇU DU PROJET

Partout en Europe, les petites et moyennes entreprises (PME) sont confrontées à un défi commun : comment rester en phase avec l'accélération de la transformation numérique alors qu'elles ne disposent pas des ressources internes, du temps ou de l'expertise dont bénéficient les grandes entreprises[1]. Pourtant, les PME sont essentielles à l'économie européenne et leur capacité à adopter des technologies telles que l'intelligence artificielle (IA) et la cybersécurité est désormais un facteur décisif pour leur compétitivité, leur résilience et leur croissance à long terme.

Tech Time 2 Skill a été créé pour aider à combler cette disparité.

Lancé par un consortium d'organismes de formation et de réseaux de PME en France, en Belgique et en Espagne, le projet vise à rendre les compétences numériques avancées accessibles à celles et ceux qui en ont le plus besoin, à savoir les dirigeants de PME, les employés et les demandeurs d'emploi à la recherche de nouvelles opportunités. L'objectif est simple : doter les personnes des compétences pratiques nécessaires pour comprendre, utiliser et intégrer l'IA et la cybersécurité dans des situations réelles sur le lieu de travail, quel que soit leur secteur d'activité ou leur niveau de connaissances techniques préalable.

Pour y parvenir, les partenaires ont développé une offre complète de programmes de formations, allant de courtes sessions de sensibilisation pour les décideurs à des cours intensifs pour les employés, en passant par des bootcamps de longue durée pour celles et ceux qui souhaitent entrer sur le marché du travail en tant que professionnels du numérique.
Ces programmes sont disponibles en plusieurs langues et sont volontairement conçus pour être modulaires, concrets et pertinents pour le travail quotidien, en réponse directe aux témoignages recueillis par les partenaires lors d'entretiens, d'enquêtes et de consultations menés auprès des PME.

L'une des principales forces de Tech Time 2 Skill réside dans son modèle de collaboration. Le consortium rassemble :

- Des organismes de formation spécialisés (BeCode, Simplon.co, Factoría F5), connus pour leur approche inclusive et pratique ainsi que pour leur vaste expérience dans le domaine de la formation numérique.
- Des organismes de soutien aux PME (PIMEC, Agoria, Agence du Numérique), qui aident à identifier les besoins, à atteindre les entreprises et à garantir que la formation réponde aux réalités économiques locales.
- Un expert du secteur, Microsoft, qui apporte des conseils techniques et des informations sur l'évolution du paysage de l'IA et de la cybersécurité.

[1] Selon les chiffres de la Commission européenne, 93 % des entreprises européennes sont des micro-entreprises (moins de 10 salariés).

Ensemble, ils ont conçu des programmes de formation basés sur des cas d'utilisation réels plutôt que sur la théorie académique. L'accent est toujours mis sur ce que les PME peuvent faire aujourd'hui, avec les outils dont elles disposent déjà, et sur la manière dont elles peuvent rapidement tirer parti des nouvelles pratiques, qu'il s'agisse d'améliorer leurs processus internes, de protéger leurs données sensibles ou d'expérimenter de nouvelles solutions d'IA.

Au cours du projet, des milliers de participants à travers l'Europe ont assisté à des ateliers, suivi des cours intensifs ou participé à des bootcamps qui ont changé leur carrière. Ces apprenants rejoindront une communauté croissante de professionnels capables de mener une transformation numérique responsable au sein de leurs organisations.

Plus largement, Tech Time 2 Skill contribue à une ambition plus vaste : renforcer l'autonomie numérique de l'Europe en dotant sa main-d'œuvre des compétences nécessaires pour innover de manière sûre et éthique. En investissant dans les personnes, et pas seulement dans les technologies, le projet soutient une vision de la transformation numérique qui soit inclusive, durable et bénéfique pour tous.

MODULES DE FORMATION

IA POUR LES DÉCIDEURS
FORMATION D'UNE JOURNÉE

Objectifs : fournir aux dirigeants une solide compréhension du potentiel et des opportunités commerciales de l'IA, leur permettant ainsi de prendre des décisions éclairées en matière d'adoption et de stratégie.

Public cible : dirigeants, décideurs et responsables de petites et moyennes entreprises de tous les secteurs.

Prérequis : aucun requis : ce cours est conçu pour être accessible à tous les professionnels, quelle que soit leur formation technique.

Objectifs pédagogiques :

- Introduction à l'IA et à son importance stratégique pour les PME
- Exploration des modèles génératifs de l'IA : cas d'utilisation et limites pour les PME
- Applications de l'IA prédictive et de la vision par ordinateur dans tous les départements
- Stratégies pour une intégration efficace de l'IA et une maximisation de l'impact

commercial
- Élaboration d'une vision stratégique pour les solutions d'IA dans votre PME

CYBERSÉCURITÉ POUR LES DÉCIDEURS
FORMATION D'UNE JOURNÉE

Objectifs : identifier les obligations en matière de cybersécurité et les principales menaces pour une entreprise, comprendre comment y répondre et acquérir les meilleures pratiques et stratégies en matière de cybersécurité pour les PME.

Public cible : dirigeants, décideurs et responsables de petites et moyennes entreprises de tous les secteurs.

Prérequis : aucun : conçu pour les professionnels de tous niveaux d'expertise technique.

Objectifs pédagogiques :
- Comprendre les principaux risques et obligations en matière de cybersécurité pour les PME.
- Stratégies de réponse efficaces aux cybermenaces identifiées.
- Meilleures pratiques et stratégies pour une cybersécurité robuste.
- Planification de la continuité des activités dans un contexte de cybersécurité.
- Intégration de la cybersécurité dans la stratégie globale de l'entreprise.

LES FONDAMENTAUX DE L'IA POUR LES PME
FORMATION DE 5 JOURS

Objectifs : permettre aux participants de comprendre les principes fondamentaux de l'IA, d'explorer ses applications pratiques et de concevoir des cas d'utilisation et des feuilles de route stratégiques pour leur organisation.

Public cible : jusqu'à 15 employés de petites et moyennes entreprises (PME) sans prérequis techniques.

Prérequis : aucun : conçu pour les professionnels de tous niveaux d'expertise technique.

Objectifs pédagogiques :
- Introduction aux principes fondamentaux de l'IA et aux applications pour les PME
- Identification de cas d'utilisation de l'IA à forte valeur ajoutée pour votre entreprise
- Compétences pratiques avec les LLM, la conception de prompts et la personnalisation des RAG
- Génération de contenu multimédia avec Gen AI
- Automatisation des flux de travail

- Conception de votre feuille de route IA et des prochaines étapes pour son adoption

AMBASSADEUR DE LA CYBERSÉCURITÉ
FORMATION DE 5 JOURS

Objectifs : Devenir un ambassadeur de la cybersécurité pour votre entreprise, vous permettant de mettre en œuvre les meilleures pratiques, de diffuser une culture de la sécurité dans toute l'organisation, de sélectionner les meilleures solutions de sécurité et de communiquer efficacement avec des experts sur vos besoins en matière de cybersécurité.

Public cible : Tout employé d'une PME ou d'une start-up souhaitant promouvoir des initiatives en matière de sécurité.

Prérequis : Au moins 2 ans d'études supérieures et 2 ans d'expérience professionnelle.

Objectifs pédagogiques :

- Acquérir des bases solides sur les principes de la cybersécurité et les menaces actuelles.
- Apprendre les meilleures pratiques en matière de classification des données, de cryptage et de sécurité de l'information.
- Maîtriser la sécurité des appareils mobiles et des environnements de travail distribués.
- Comprendre les stratégies de défense des réseaux et d'atténuation des menaces liées aux e-mails.
- Élaborer des plans d'intervention et des stratégies de continuité pour votre organisation.

Tout au long de la formation, les participants mettront à jour le plan directeur de cybersécurité de leur PME et concevront des activités de sensibilisation pour leurs collègues, garantissant ainsi une application pratique immédiate.

BOOTCAMPS PROFESSIONNELS

Des programmes de formation intensive sont proposés aux demandeurs d'emploi qui souhaitent se spécialiser dans le développement de l'IA ou les opérations de cybersécurité. Les PME et les professionnels spécialisés sont également visés par ce programme, soit par le biais d'un recrutement direct, soit par l'intermédiaire de leurs prestataires de services. Ces programmes complets combinent une formation rigoureuse et des applications pratiques.

BOOTCAMP POUR DÉVELOPPEURS IA

Durée : 9 mois

- Maîtriser le cycle des données : de la collecte à l'analyse.
- Intégrer les modèles IA existants dans les applications destinées aux utilisateurs finaux.
- Acquérir des compétences en gestion de projet pour les applications IA.

OPÉRATEUR DE SOLUTIONS DE CYBERSÉCURITÉ

Durée : 6 mois

- Intégrer et administrer des solutions de cybersécurité.
- Sécuriser les composants de l'infrastructure réseau.
- Optimiser les niveaux de sécurité de l'infrastructure.

INDICATEURS DE RÉUSSITE

TOTAL

98 FORMATIONS

1 471 PARTICIPANTS

47% FEMMES *(692)*

Au cours de l'initiative Tech Time 2 Skill, le consortium a déployé avec succès une offre de formation ambitieuse et diversifiée destinée aux demandeurs d'emploi, aux employés de PME et aux chefs d'entreprise à travers l'Europe. Au total, 98 éditions des différents programmes ont été organisées, permettant à 1 471 participants de renforcer leurs compétences en intelligence artificielle et en cybersécurité, deux domaines qui deviennent essentiels pour la compétitivité et la résilience.

L'une des principales réussites du projet réside dans son engagement en faveur de l'inclusion : 47 % des participants étaient des femmes, ce qui témoigne d'une nette amélioration de la parité homme-femme dans la formation aux compétences numériques avancées.

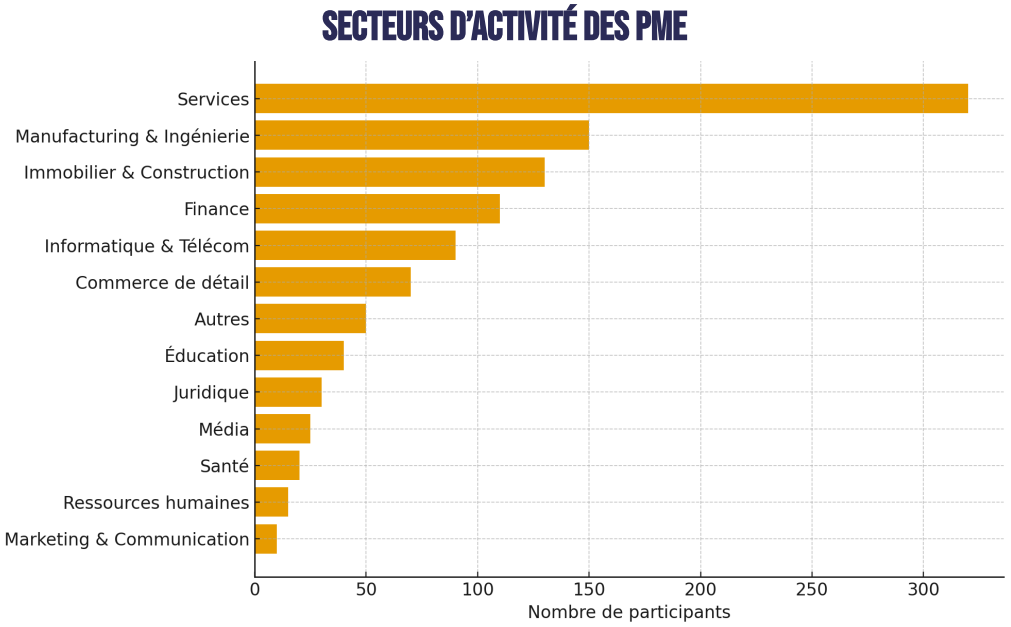
Les bootcamps destinés aux demandeurs d'emploi, d'une durée de 400 à 1 250 heures, ont joué un rôle central dans l'accélération de l'accès à des carrières numériques très demandées. Au cours de 9 éditions, le programme a formé 194 participants, dont 43 % de femmes, leur permettant d'acquérir une expertise approfondie et immédiatement exploitable dans les domaines de l'IA et de la cybersécurité.

Pour les employés des PME, le projet a proposé 32 éditions de cours intensifs de 5 jours, qui ont permis de former 473 professionnels. Il est à noter que ces programmes ont atteint un taux de participation féminine de 51 %, une étape importante qui reflète l'intérêt et l'engagement croissants des femmes pour les parcours de perfectionnement

technique. Ces cours de 35 heures ont permis aux participants de comprendre rapidement les applications pratiques, de développer des cas d'utilisation concrets et de soutenir directement la transformation numérique de leur entreprise.

L'initiative a également touché un large public de décideurs, un groupe essentiel pour favoriser l'adoption stratégique des technologies numériques au sein des PME. Au cours de 57 sessions d'une journée, le projet a formé 804 dirigeants et cadres, dont 46 % étaient des femmes. Ces sessions de sensibilisation ont contribué à démystifier l'IA et la cybersécurité, à clarifier les risques et les opportunités commerciaux, et à donner aux dirigeants les moyens d'élaborer des feuilles de route concrètes adaptées aux besoins de leur organisation.

Dans l'ensemble, ces résultats illustrent l'impact significatif de Tech Time 2 Skill. Au-delà des chiffres, ils soulignent un intérêt croissant à travers l'Europe pour des formations numériques pratiques, accessibles et axées sur les entreprises, ainsi qu'une forte dynamique en faveur d'une main-d'œuvre numérique plus inclusive.



TÉMOIGNAGES

Bouchaib : de la criminalistique à l'IA

Basé à Nancy, en France, Bouchaib est passé avec succès de sa carrière en criminalistique à l'intelligence artificielle grâce au programme TT2S et à un programme d'alternance au CHRU de Nancy. Passionné par la santé et l'éthique, il contribue à des projets tels que la robotique automatisée et un outil OCR sur mesure pour l'hôpital. Son parcours montre comment des parcours diversifiés, associés à une formation adaptée, peuvent conduire à des innovations significatives dans le domaine de l'IA.

« J'ai eu beaucoup de mal à trouver du travail après avoir suivi un cursus universitaire traditionnel. Cette expérience pratique en alternance facilite donc ma réorientation professionnelle et me rassure. »

Noémie : aborder l'IA de manière responsable

Forte d'une formation en génie informatique et d'une carrière consacrée à la responsabilité numérique et à la RSE, Noémie a suivi une formation de cinq jours sur l'IA afin de mieux comprendre les enjeux éthiques et environnementaux liés aux technologies émergentes. Cette expérience lui a permis d'acquérir une connaissance pratique du potentiel et des limites de l'IA, en particulier dans le domaine du contenu génératif. Aujourd'hui, elle intègre ces connaissances dans ses activités de coaching et de formation, en encourageant une utilisation raisonnée, éthique et pratique de l'IA.

« J'étais très préoccupée par le développement rapide de l'IA. Cette démocratisation me semblait trop rapide et insuffisamment réglementée. J'ai donc préféré aborder ces questions le plus tôt possible afin de mieux comprendre les défis et de les maîtriser. »

Myriam : à la pointe de la formation continue pour les PME européennes

Myriam est une formatrice expérimentée spécialisée dans l'intelligence artificielle et la cybersécurité, qui possède une solide expérience dans la conception et la mise en œuvre de formations destinées aux PME, aux entrepreneurs et aux équipes d'entreprise. Elle a animé des formations de formats très variés, allant de sessions de sensibilisation d'une demi-journée à des programmes intensifs de deux jours, offrant des expériences d'apprentissage hautement adaptables et adaptées aux besoins et au niveau de maturité de publics divers.
Elle préconise fortement la formation en présentiel, en particulier pour les sujets complexes ou en évolution rapide. Pour elle, les sessions en face à face permettent des questions spontanées, une interaction plus approfondie et un ajustement en temps réel du contenu, des éléments qui sont plus difficiles à réaliser dans le cadre de l'apprentissage en ligne et qui améliorent considérablement l'impact de l'expérience d'apprentissage tant pour les formateurs que pour les participants.

« Je privilégie les ateliers pratiques et les scénarios réels. Les participants travaillent sur des cas concrets, qu'il s'agisse de scénarios de cyberattaques ou d'expériences avec des outils d'IA. Cela rend la formation dynamique et permet à chacun de s'impliquer, quel que soit son niveau. »

DÉFIS RENCONTRÉS

L'un des défis les plus importants rencontrés tout au long du programme Tech Time 2 Skill a été le fort déséquilibre entre l'intérêt pour l'intelligence artificielle (IA) et celui pour la cybersécurité. Avec l'essor rapide de l'IA générative à partir de la fin 2022, l'IA a

dominé l'attention du public et a été largement perçue comme une source d'innovation et d'opportunités futures. La cybersécurité, en revanche, a eu du mal à susciter l'intérêt. De nombreuses PME continuent de la considérer comme un domaine hautement technique réservé aux spécialistes, et une approche réactive plutôt que préventive prévaut souvent. En conséquence, la participation aux activités liées à l'IA a été systématiquement plus élevée, tandis que les pratiques de sécurité quotidiennes sont restées sous-utilisées. Pour combler cet écart, les partenaires ont adopté une stratégie qui a permis d'intégrer les deux thèmes dans les mêmes expériences de formation. En tirant parti de l'enthousiasme naturel pour l'IA, il a été possible de maintenir l'engagement et d'introduire progressivement les concepts de cybersécurité d'une manière plus accessible. Au fil du temps, les partenaires ont observé un changement tangible : au fur et à mesure que les participants progressaient dans les sessions, leur conscience de l'importance de la cybersécurité s'est accrue, ce qui montre que l'intérêt peut être cultivé lorsque l'exposition est constante et que l'expérience d'apprentissage est concrète et accessible.

Un autre défi majeur découlait de la diversité des contextes des PME et des profils des participants. Les personnes qui assistaient aux sessions de formation provenaient de secteurs, de fonctions et de niveaux de maturité numérique très différents : des dirigeants aux responsables des ressources humaines, en passant par les équipes marketing, les responsables financiers, les chefs de projet et le personnel plus technique. Leurs besoins n'étaient pas les mêmes, et les exemples qui trouvaient un écho dans le secteur manufacturier ne s'appliquaient pas nécessairement aux secteurs de la santé, du commerce de détail ou des services. Même au sein d'une même entreprise, les pratiques numériques variaient considérablement. Cette diversité rendait difficile la conception d'une approche de formation unique pouvant convenir à tous, en particulier pour les activités pratiques telles que le prototypage de l'IA. L'équipe du projet a donc structuré son contenu de manière à ce que les concepts fondamentaux restent accessibles à tous, tandis que des scénarios spécifiques à chaque secteur et des applications adaptées aux différents rôles ont permis d'ancrer l'apprentissage dans la réalité quotidienne.

Les contraintes de temps ont également joué un rôle majeur : les employés des PME ne peuvent souvent pas se libérer pendant plusieurs jours consécutifs, ce qui rend difficile la participation à des formats intensifs. La participation dépendait souvent de la capacité des employés à trouver de petits créneaux dans leur emploi du temps, souvent à la dernière minute. Cette réalité a poussé l'équipe à opter pour des formats plus courts et plus flexibles, parfois dispensés en ligne par segments de 2 à 3 heures, tout en conservant un espace pour la découverte pratique. Trouver le juste équilibre entre la nécessité de la concision et l'importance de l'expérimentation pratique a été un défi constant en matière de conception, mais essentiel pour transformer la prise de conscience en capacité réelle.

L'évolution technologique a présenté une autre difficulté. Les outils, modèles, interfaces et meilleures pratiques en matière d'IA évoluent à une vitesse extraordinaire, rendant certains exemples obsolètes quelques mois seulement après

leur introduction. Les risques liés à la cybersécurité et les techniques d'attaque ont également évolué rapidement. Les partenaires ont réagi en actualisant régulièrement le contenu et en se concentrant sur les principes et les méthodes transférables plutôt que sur les compétences spécifiques à un outil, aidant ainsi les apprenants à retenir des approches qui resteraient pertinentes malgré les changements technologiques.

De plus, les conditions techniques de base n'étaient pas toujours réunies. Certaines PME ne disposaient pas d'une connectivité fiable, d'équipements adaptés, voire des compétences numériques de base nécessaires pour suivre les sessions en ligne. Dans ces cas, le simple fait de participer à une vidéoconférence ou d'utiliser des outils collaboratifs pouvait devenir un obstacle, illustrant les disparités en matière de préparation numérique entre les régions et les secteurs.

Malgré ces obstacles, le projet a permis aux participants de mieux comprendre l'importance de la cybersécurité. Au fil des sessions, il est apparu clairement que l'exposition et une communication claire et pratique peuvent faire évoluer les mentalités, passant d'une approche réactive à une approche proactive. Cela revêt une grande importance : la cybersécurité n'est pas seulement une question technique, mais une responsabilité partagée par l'ensemble de l'organisation. Les PME, qui ne disposent souvent pas d'équipes informatiques dédiées ni d'infrastructures de sécurité avancées, sont particulièrement vulnérables. Une seule erreur humaine, comme cliquer sur un lien de phishing ou utiliser un mot de passe faible, peut entraîner des violations, des perturbations opérationnelles ou des pertes financières difficiles à absorber. La mise en place de pratiques de sécurité quotidiennes nécessite donc un changement culturel, dans lequel les employés à tous les niveaux comprennent leur rôle en tant que première ligne de défense.

Cette perspective plus large s'applique également à l'IA. Si l'enthousiasme pour l'IA est fort, il est essentiel de l'adopter de manière responsable. L'IA offre aux PME des avantages concrets, allant de l'automatisation des tâches à l'amélioration des opérations et à la réduction des coûts, mais elle a également des implications environnementales, éthiques et sociales. Derrière les outils d'IA se cachent des infrastructures énergivores et des conditions de travail mondiales qui restent souvent invisibles. L'utilisation de l'IA peut entraîner des risques tels que des biais, des problèmes de confidentialité des données ou une dépendance excessive à des systèmes opaques, et les PME peuvent ne pas disposer des structures internes nécessaires pour gérer ces défis. C'est pourquoi le projet a mis l'accent non seulement sur la manière d'utiliser les outils d'IA, mais aussi sur les raisons et les coûts de leur utilisation, encourageant ainsi une approche plus éclairée et réfléchie.

L'ensemble de ces défis ont façonné l'évolution de Tech Time 2 Skill. Ils ont souligné la nécessité d'une formation flexible, inclusive, réaliste, régulièrement mise à jour et fondée sur des pratiques numériques responsables. Ils ont également mis en évidence une vérité essentielle : une transformation numérique significative nécessite non seulement des compétences et des outils, mais aussi une prise de conscience, une culture et une responsabilité collective.

RECOMMANDATIONS

L'expérience acquise tout au long du projet Tech Time 2 Skill met en évidence une série de recommandations concrètes visant à renforcer la préparation numérique de l'Europe. Si les PME sont confrontées à des défis communs, les solutions doivent être adaptées aux différents acteurs : employés, dirigeants de PME, autorités publiques et organisme de formation. Les recommandations suivantes synthétisent les enseignements tirés du projet et décrivent les mesures concrètes à prendre pour soutenir une transformation numérique responsable et durable.

POUR LES EMPLOYÉS DES PME

1. Faciliter l'accès à la formation grâce à des formats flexibles et réalistes
Les employés des PME ont souvent du mal à se libérer pour suivre des sessions longues. La formation doit donc être proposée dans des formats très adaptables, mettant l'accent sur les échanges entre pairs :

- modules courts (1 à 3 heures)
- formation en ligne ou hybride
- journées intensives ou programmes répartis sur plusieurs semaines
- modules regroupés par défis pratiques plutôt que par thèmes techniques

2. Encourager la participation par des mesures incitatives
Les mécanismes qui motivent les employés à améliorer leurs compétences peuvent contribuer à éliminer les obstacles à la participation, comme les micro-certifications, les diplômes ou les certificats de participation.

3. Fournir des outils concrets et immédiatement applicables
Les employés tirent le meilleur parti des sessions qui comprennent :

- des cas d'utilisation réels dans les PME
- des exercices guidés étape par étape
- des modèles, des listes de contrôle et des guides de démarrage rapide qu'ils peuvent directement appliquer dans leur organisation

4. Intégrer la cybersécurité en tant que compétence transversale
La cybersécurité ne doit pas être considérée comme une spécialité distincte réservée aux experts. Les employés doivent être systématiquement initiés aux éléments suivants :

- pratiques numériques sécurisées
- détection quotidienne des risques
- habitudes en matière de protection des données
- et rôle qu'ils jouent en tant que première ligne de défense

POUR LES DIRIGEANTS ET LES GESTIONNAIRES DE PME

1. Adopter des programmes de formation combinant IA et cybersécurité.
L'IA attire l'attention et peut servir de point d'entrée pour sensibiliser à la cybersécurité. Des sessions combinées aident les managers à comprendre à la fois les opportunités et les risques de manière accessible et stratégique.

2. Élaborer des plans de transformation concrets.
Les programmes doivent aider les dirigeants à :

- identifier les cas d'utilisation pertinents pour leur organisation
- évaluer les risques
- hiérarchiser les actions
- et concevoir des feuilles de route réalistes adaptées à leurs contraintes

3. Impliquer les équipes grâce à des opportunités pratiques
Les décideurs doivent encourager les projets pilotes internes et l'expérimentation en équipe, en veillant à ce que les compétences acquises lors de la formation se traduisent par des mises en œuvre concrètes.

4. Considérer la cybersécurité comme une responsabilité stratégique
Les dirigeants doivent veiller à ce que la cybersécurité ne soit pas confinée aux équipes informatiques, mais intégrée à l'ensemble de l'organisation en tant que responsabilité partagée, influençant la gouvernance, la culture et les routines quotidiennes.

POUR LES AUTORITÉS PUBLIQUES ET LES INSTITUTIONS EUROPÉENNES

1. Investir dans des campagnes de sensibilisation à la cybersécurité à grande échelle
Des initiatives régionales, nationales ou européennes sont essentielles pour améliorer les connaissances de base, lutter contre la complaisance et atteindre les PME qui ne sont pas connectées aux réseaux de formation.

2. Créer des incitations financières et réglementaires pour la formation des PME
Les autorités peuvent jouer un rôle décisif en :

- offrant des avantages fiscaux aux entreprises qui investissent dans le renforcement des compétences numériques
- simplifiant l'accès aux subventions et aux aides financières
- donnant la priorité aux PME dans l'attribution des chèques-formation et des fonds nationaux

3. Soutenir des cadres d'apprentissage flexibles, modulaires et basés sur les compétences
Les programmes de financement devraient encourager explicitement :

- la conception de cours modulaires
- le renforcement des compétences sur des cycles courts
- et les infrastructures d'apprentissage hybrides adaptées aux contraintes des PME

4. Promouvoir des infrastructures responsables et alignées sur les normes européennes
Les politiques publiques devraient encourager l'adoption d'outils européens d'IA et de cybersécurité qui renforcent la souveraineté, la protection de la vie privée et la conformité avec les réglementations de l'UE.

POUR LES PRESTATAIRES DE FORMATION ET LES ORGANISMES DE FORMATION

1. Développer des parcours de formation modulaires
Les programmes de formation doivent être conçus comme des modules adaptables pouvant être combinés, réorganisés ou personnalisés afin de s'adapter aux différents profils des PME, aux secteurs d'activité et aux contraintes locales. La modularité garantit la pertinence du contenu malgré la diversité des profils des apprenants et les besoins variés des organisations.

2. Assurer une mise à jour constante du contenu
Compte tenu de l'évolution rapide de l'IA et de la cybersécurité, les supports de formation doivent être mis à jour tous les 3 à 6 mois avec l'aide d'experts.
Il est important de noter que ce rythme rapide de changement rend les formats d'apprentissage en ligne beaucoup plus difficiles à maintenir, car la mise à jour des modules numériques, des vidéos ou des contenus interactifs nécessite du temps, des ressources techniques et des cycles de redéveloppement fréquents pour rester pertinents.

C'est pourquoi les parcours de formation en présentiel doivent être privilégiés et renforcés, car ils permettent aux formateurs :

- d'ajuster les exemples et les outils en temps réel
- d'intégrer immédiatement les dernières évolutions
- et de garantir que le contenu reste en phase avec un paysage technologique en constante évolution

3. Proposer à la fois des formats interentreprises et intra-entreprises
Une double approche maximise l'impact :

- les sessions interentreprises favorisent les échanges intersectoriels et permettent aux PME d'apprendre de leurs pairs confrontés à des défis similaires

- les sessions intra-entreprises permettent une adaptation plus poussée à la culture organisationnelle, aux cas d'utilisation spécifiques au secteur et aux priorités stratégiques

4. Renforcer les partenariats avec les réseaux de PME
Les organismes de formation doivent travailler en étroite collaboration avec les chambres de commerce, les associations de PME, les fédérations et les clusters. Ces réseaux sont essentiels pour atteindre efficacement les entreprises, comprendre les besoins locaux et garantir que les interventions de formation répondent aux conditions réelles du marché.

5. Intégrer la cybersécurité dans toutes les formations numériques
La cybersécurité ne doit pas être considérée comme un sujet spécialisé. Les pratiques sécurisées doivent être intégrées dans les modules consacrés à l'IA, aux données, au cloud et au lieu de travail numérique, afin que chaque apprenant, quel que soit son rôle ou son expertise, adopte la cybersécurité dans son comportement numérique quotidien.

6. Fournir des supports prêts à l'emploi
Pour maximiser l'impact, les prestataires doivent fournir aux PME :

- des modèles pratiques
- des listes de contrôle
- des exercices basés sur des scénarios
- et des cadres simples permettant d'appliquer immédiatement les leçons apprises

7. Renforcer la coopération européenne pour la qualité et l'impact
La transformation numérique est un défi européen commun, et les organismes de formation ont beaucoup à gagner d'une collaboration transfrontalière. Cela comprend :

- l'échange de bonnes pratiques, de méthodologies et de nouvelles connaissances pédagogiques
- le développement conjoint ou l'adaptation de contenus de formation afin de garantir leur conformité avec les normes européennes et les priorités technologiques
- la participation à des réseaux de formation européens afin de mettre en commun l'expertise et de réduire les doubles emplois
- e partage des informations sur l'évolution de la réglementation (par exemple, la loi sur l'IA, NIS2) et l'alignement de la formation en conséquence
- la création de communautés transnationales de formateurs afin de soutenir la collaboration et d'accélérer l'innovation

Une telle coopération améliore la qualité de la formation, favorise la cohérence à travers l'Europe et renforce la capacité du continent à constituer une main-d'œuvre numérique qualifiée et résiliente.

CONTACTS DES PARTENAIRES

</becode>

LOUIS DE VIRON

Responsable Technologie et Pédagogie
louis.deviron@becode.org

F5 factoria POWERED BY SIMPLON

OLGA CORRALES

Responsable des relations B2B et cheffe de projet
olga.corrales@factoriaf5.org

simplon

TIMOTHÉE LEENHARDT

Responsable du développement international et de l'innovation pédagogique
tleendardt@simplon.co

Cofinancé par
l'Union européenne