REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
1. Gestion stratégique d'un système d'information et innovation A1. Pilotage de projet SI A2. Audit d'un système d'information A3. Management d'équipe A4. Intégration de pratiques inclusives et durables	C1.1 : Piloter des projets interdisciplinaires en intégrant de nouvelles technologies et innovations afin de répondre aux enjeux stratégiques de l'entreprise, améliorer l'efficacité opérationnelle et renforcer la sécurité des systèmes d'information C1.2 : Collaborer avec les équipes métier pour recueillir leurs besoins et défis spécifiques, et traduire ces besoins en solutions techniques viables qui soutiennent les objectifs stratégiques de l'entreprise C1.3 : Définir le budget du projet et établir le plan stratégique en respectant les contraintes budgétaires et les échéances afin d'assurer la réalisation des objectifs fixés, maximiser le retour sur investissement et garantir la soutenabilité financière du projet C1.4 : Optimiser la gestion du cycle de vie IT et piloter l'adoption des systèmes pour garantir une infrastructure technologique performante et évolutive C2.1 : Évaluer les systèmes pour optimiser la performance et la sécurité C2.2 : Aligner les systèmes d'information avec les tendances sectorielles et les objectifs stratégiques afin de stimuler l'innovation, favoriser la compétitivité de l'entreprise sur le	**Cas pratique** : Le/la candidat(e) doit produire **un rapport d'expérience professionnelle** de 40 pages maximum, et le restituer lors d'une soutenance devant le jury. **Durée** : Présentation orale individuelle de 20 minutes, suivie de 20 minutes de questions-réponses avec le jury. Ce document comprend : • L'élaboration d'un plan de projet pour l'implémentation d'une innovation stratégique au sein du système d'information, incluant la définition des objectifs, des ressources nécessaires, et des étapes clés (C1) • La réalisation d'un audit pour identifier les forces, faiblesses, et	- Les choix de technologies et d'innovations sont alignés sur les objectifs du projet. (C1.1) - Des méthodologies agiles sont appliquées pour le développement de solutions (C1.1) - Le/la candidat(e) organise et conduit des sessions de recueil d'informations, utilisant des méthodes telles que des interviews, des questionnaires, ou des ateliers collaboratifs. (C1.2) - Les besoins métier sont traduits en solutions techniques soutenant les objectifs stratégiques. (C1.2) - Le budget et les échéances du projet sont clairement définis. (C1.3) - Le plan stratégique est aligné avec les contraintes budgétaires. (C1.3) - Le cycle de vie des applications et des infrastructures IT est géré. (C1.4) - Une mise à jour régulière et remplacement stratégique pour réduire les vulnérabilités sont réalisés. (C1.4) - Le nouveau système est testé avant d'être déployé. (C1.4) - La formation des utilisateurs est planifiée ou réalisée. (C1.4) - Un suivi post-déploiement est intégré. (C1.4) - Une mesure et une analyse de performance des systèmes d'information via des indicateurs clés de performance (KPIs) est réalisée.

	marché, et soutenir une prise de décision éclairée C2.3 : Mettre en œuvre des plans d'action et évaluer la résilience face aux cybermenaces C2.4 : Documenter les résultats et assurer le suivi des améliorations afin de garantir la traçabilité des actions entreprises C2.5 : Renforcer la culture de sécurité et instaurer un processus d'audit continu afin de minimiser les risques de cyberattaques et de violations de données	opportunités d'amélioration du système d'information existant. La proposition de mesures correctives alignées avec les objectifs stratégiques de l'organisation (C2) • Le développement d'un plan de management visant à mobiliser et à coordonner l'équipe projet, avec un accent sur la communication, la motivation et la gestion des conflits. Ce plan devra inclure à minima le détail d'un aménagement de poste réel ou fictif pour un collaborateur en situation de handicap (C3) • La proposition d'initiatives visant à intégrer des pratiques inclusives et durables dans la gestion du système d'information, avec une analyse de leur impact sur la performance et la responsabilité sociale de l'entreprise (C4)	Les données sont utilisées pour orienter les décisions stratégiques et opérationnelles relatives aux systèmes d'information. (C1.4) - Le/la candidat(e) met en place une gestion proactive du changement lors de l'introduction de nouveaux systèmes ou de mises à jour majeures, en réduisant au minimum les interruptions des opérations commerciales pour stimuler l'adoption par les utilisateurs. (C1.4) - Le/la candidat(e) examine l'architecture, évalue l'efficacité et les configurations des systèmes d'information existants. Il/elle identifie les lacunes en termes de performance et des risques de sécurité. (C2.1) - Les procédures actuelles de gestion des données sont évaluées pour s'assurer qu'elles respectent les meilleures pratiques et les exigences légales. (C2.1) - Des améliorations basées sur les dernières innovations technologiques pour renforcer la sécurité et l'efficacité sont proposées. (C2.1) - Le/la candidat(e) effectue une veille sur les tendances et évolutions du secteur. Il/elle recommande des mises à jour stratégiques des systèmes d'information. (C2.2) - Il/elle maintient une collaboration étroite est avec les départements IT et métiers pour comprendre les flux de travail et les exigences spécifiques. Il/elle intègre les solutions d'audit dans les opérations quotidiennes sans perturber les activités. (C2.2) - Des plans d'action détaillés sont élaborés pour remédier aux déficiences identifiées. Les interventions sont priorisées en fonction de leur impact sur l'entreprise. (C2.3) - La résilience des systèmes est évaluée à travers des tests de pénétration et des simulations d'attaque. (C2.3)
	C3 : Constituer et manager des équipes pour atteindre les objectifs fixés, tout en intégrant des collaborateurs en situation de handicap afin de garantir l'inclusion au sein des équipes		
	C4.1 : Promouvoir l'accessibilité et le développement durable dans la conception des systèmes pour contribuer à l'économie circulaire C4.2 : Engager les parties prenantes et évaluer l'impact pour une amélioration continue		

			- Le/la candidat(e) développe des rapports d'audit clairs et détaillés qui documentent les constatations et recommandent des actions correctives. (C2.4) - Le suivi de la mise en œuvre des recommandations d'audit est assuré : les améliorations sont effectivement réalisées et produisent les résultats attendus. (C2.4) - Un processus d'audit continu est instauré pour anticiper les défis de sécurité et de conformité. (C2.5) - Une formation du personnel sur les nouvelles procédures de sécurité découlant des audits est assurée. (C2.5) - Le/la candidat(e) communique avec les équipes et fixe des objectifs. (C3) - Il/elle organise et en coordonne les membres de l'équipe entre eux tout en créant de la cohésion d'équipe. (C3) - Il/elle adapte ses modes de management au travail hybride, entre présentiel et télétravail. (C3) - Le/la candidat(e) - Prépare l'arrivée du collaborateur en situation de handicap en amont (en analysant les stéréotypes liés au handicap, en s'éduquant sur les différents types de handicaps, en sensibilisant les équipes) - Nomme un référent au sein de l'équipe pour faciliter l'inclusion du collaborateur en situation de handicap - Réalise des aménagements de poste ou de temps de travail en fonction des besoins du collaborateur en situation de handicap (en collaboration avec le service ressources humaines) - adapte son mode de management et de communication au collaborateur et à son handicap (C3) - Des standards d'accessibilité, garantissant l'utilisation sans barrière par tous les utilisateurs, y compris ceux en

			situation de handicap, sont appliqués dans la conception des systèmes (C4.1) - Des approches de développement durable visant à réduire la consommation d'énergie et l'utilisation des ressources dans les infrastructures IT sont adoptées. (C4.1) - Le recyclage et la réutilisation des équipements informatiques sont favorisés. (C4.1) - Le/la candidat(e) s'assure que les solutions sont bien alignées avec les valeurs de l'entreprise en impliquant les parties prenantes dans la définition des besoins inclusifs et écologiques. (C4.2) - Il/elle identifie les opportunités d'amélioration continue en évaluant régulièrement l'impact environnemental et social des systèmes d'information (C4.2) - Des formations sont dispensées aux équipes IT et aux utilisateurs finaux sur l'importance de l'accessibilité et de l'écologie dans le domaine des systèmes d'information. (C4.2)

2. **Développement et mise en œuvre des technologies avancées et des services de sécurité** A5. Développement et déploiement de plateforme applicative A6. Application de la data science A7. Intégration de l'IA A8. Renforcement de la sécurité	C5.1 : Sélectionner et appliquer les technologies et méthodologies pertinentes afin d'optimiser les processus opérationnels, accroître l'efficience et l'efficacité des projets C5.2 : Améliorer l'expérience utilisateur et la prise de décision par l'analyse et l'IA afin de personnaliser les services, augmenter la satisfaction client, identifier de nouvelles opportunités de marché et optimiser les processus décisionnels, pour une meilleure performance opérationnelle et un avantage concurrentiel durable pour l'entreprise C5.3 : Garantir la sécurité et la performance de la plateforme afin de assurer une expérience utilisateur fiable et fluide, minimiser les risques de cyberattaques et de pannes, et soutenir la continuité des activités en maintenant des niveaux élevés de disponibilité et de réactivité des systèmes d'information. C5.4 : Assurer l'alignement avec les besoins métier et une amélioration continue afin de s'assurer que la plateforme répond précisément aux besoins des équipes C6.1 : Développer et intégrer des analyses de données avancées afin de dévoiler des insights stratégiques, optimiser la prise de décision fondée sur des données probantes, améliorer les performances opérationnelles, et identifier de nouvelles opportunités de croissance et d'innovation, contribuant ainsi à la transformation numérique et à la compétitivité de l'organisation. C6.2 : Assurer la conformité, la communication et l'évaluation continue afin de garantir que les pratiques et procédures de l'entreprise	Le rapport d'expérience professionnelle comprend un projet de développement d'une application web/mobile sécurisée, avec rapport technique détaillant les choix de conception, les mesures de sécurité intégrées et les tests de validation, incluant : • La conception et la mise en œuvre d'une plateforme applicative, incluant la sélection des technologies, le développement de fonctionnalités spécifiques, et le déploiement efficace de la solution. (C5) • Une mise en place de techniques de data science pour analyser et exploiter les données de manière à améliorer les performances et l'efficacité d'une solution informatique. (C6) • L'intégration de solutions d'intelligence artificielle pour automatiser les processus, améliorer l'expérience utilisateur et renforcer les capacités analytiques d'une	- Le/la candidat(e) choisit des outils de développement alignés avec les objectifs du projet. (C5.1) - Des frameworks et des outils de développement adaptés aux objectifs du projet et aux exigences fonctionnelles sont sélectionnés. (C5.1) - Les méthodologies agiles sont appliquées pour accélérer le développement et le déploiement de solutions. (C5.1) - Le/la candidat(e) intègre des fonctionnalités d'analyse de données. (C5.2) - Des insights sont fournis pour améliorer la prise de décision des utilisateurs. (C5.2) - L'IA est utilisée pour personnaliser l'expérience utilisateur et automatiser les processus. (C5.2) - Le/la candidat(e) adopte des pratiques de codage sécurisé. (C5.3) - Les systèmes de gestion des identités et des accès protègent les données et les applications contre les menaces. (C5.3) - Des tests de performance et de sécurité sont réalisés pour identifier et corriger les vulnérabilités avant le déploiement. (C5.3) - Le/la candidat(e) collabore étroitement avec les équipes métier. (C5.4) - La performance de la plateforme post-déploiement est surveillée pour garantir sa performance continue et intervenir rapidement en cas de besoin. (C5.4) - Les nouvelles technologies sont régulièrement évaluées. La plateforme applicative est mise à jour, optimisée et améliorée afin de maintenir son avantage concurrentiel. (C5.4) - Le/la candidat(e) identifie les opportunités offertes par la data science. (C6.1)

	respectent les normes réglementaires et les standards	solution informatique. (C7) • Le développement et implémentation de stratégies avancées de sécurité pour protéger une plateforme logicielle contre les menaces numériques et garantir la confidentialité et l'intégrité des données. (C8)	- Des projets d'analyse de données sont conçus pour extraire des insights pertinents. (C6.1) - Les techniques avancées de machine learning et d'intelligence artificielle sont appliquées pour créer des modèles prédictifs. (C6.1) - Le/la candidat(e) collabore avec les équipes IT et métier pour intégrer les résultats d'analyse dans les systèmes et processus existants. (C6.1) - Le/la candidat(e) garantit la conformité des projets de data science avec les réglementations sur la protection des données. (C6.2) - Les résultats des analyses sont communiqués aux parties prenantes pour faciliter l'adoption des recommandations basées sur les données. (C6.2) - Les outils et techniques de data science sont continuellement évalués pour rester à la pointe de la technologie et améliorer les capacités analytiques de l'entreprise. (C6.2)
	C7.1 : Optimiser les processus et développer des solutions d'IA personnalisées afin d'automatiser et rationaliser les opérations, réduire les coûts et les délais, améliorer la précision et l'efficacité, et fournir des services et des produits plus adaptés C7.2 : Renforcer la sécurité des plateformes logicielles avec l'IA, afin d'assurer la sécurité des données, protéger la confidentialité des informations des utilisateurs, prévenir les accès non autorisés et les fuites de données, et garantir la conformité avec les réglementations en matière de protection des données, contribuant ainsi à la confiance et à la fidélité des clients ainsi qu'à la réputation de l'entreprise sur le marché. C7.3 : Collaborer avec les équipes métier pour recueillir leurs besoins et adapter les solutions d'IA pour répondre à ces besoins. C7.4 : Former les utilisateurs finaux à l'utilisation des nouveaux outils et systèmes basés sur l'IA pour maximiser leur adoption et leur utilité		- Le/la candidat(e) identifie les processus métier susceptibles d'être optimisés par l'IA Il/elle définit les objectifs spécifiques de performance et d'efficacité. (C7.1) - Des outils et plateformes d'IA adaptés aux besoins spécifiques de l'entreprise sont sélectionnés et configurés. (C7.1) - Des modèles d'IA personnalisés sont développés pour traiter, analyser et interpréter de grandes quantités de données. (C7.1) - Le/la candidat(e) intègre une transparence des solutions d'IA dans l'infrastructure TI existante. Il/elle minimise les perturbations des opérations en cours. (C7.1) Le/la candidat(e) évalue l'impact de l'IA sur la sécurité des données. (C7.2) - Les mesures de protection sont renforcées en conséquence. (C7.2)
	C8 : Renforcer la sécurité des applications, des bases de données et des infrastructures utilisées pour le développement et l'analyse de données, ainsi que la protection contre les menaces et la conformité avec les normes		

			- Le/la candidat(e) engage un dialogue constructif avec les équipes métier pour identifier précisément leurs besoins et élabore des comptes-rendus des entretiens réalisés. (C7.3) - Il/elle conçoit ou modifie des solutions d'IA qui répondent spécifiquement aux exigences métier recueillies avec des démonstrations de fonctionnalités ou des études de cas montrant comment les ajustements des solutions d'IA ont mené à des améliorations mesurables. (C7.3) - Le/la candidat(e) développe et délivre des formations ciblées, facilitant la compréhension et l'utilisation efficace des nouveaux outils d'IA par les utilisateurs finaux et des évaluations post-formation indiquant une augmentation de la compétence. (C7.4) - Le/la candidat(e) évalue les risques de sécurité spécifiques aux applications développées et aux systèmes d'analyse de données. (C8) - Les données sensibles sont protégées par des techniques de cryptographie. (C8) - Des protocoles de sécurité sont mis en œuvre pour les échanges de données et les communications entre services. (C8) - Des audits et tests de sécurité réguliers sont réalisés pour identifier et corriger les vulnérabilités, tels que des audits et des tests de pénétration. (C8) - Les développeurs et analystes sont formés aux meilleures pratiques de sécurité dans leur travail quotidien. (C8)

3. **Mise en place et gestion des infrastructures numériques et de la cybersécurité** A9. Gestion de l'infrastructure IT A10. Élaboration et renforcement des mesures de cybersécurité A11. Application de l'IA à la sécurité	C9.1 : Optimiser et sécuriser l'infrastructure IT afin de garantir sa performance, sa fiabilité et sa résilience C9.2 : Surveiller, gérer et innover pour la haute disponibilité afin d'assurer un accès constant et fiable aux services et aux applications critiques, minimiser les temps d'arrêt et les perturbations des opérations, et améliorer l'expérience utilisateur, contribuant ainsi à la satisfaction et à la fidélité des clients tout en soutenant les objectifs stratégiques de l'entreprise dans un marché compétitif C10 : Élaborer et renforcer les mesures de cybersécurité à travers des approches innovantes et des technologies avancées pour protéger les actifs numériques contre les attaques internes et externes, tout en intégrant la conformité réglementaire C11 : Implémenter l'intelligence artificielle dans les stratégies de sécurité pour anticiper, détecter et neutraliser les cybermenaces de manière proactive, améliorant ainsi la résilience des systèmes informatiques	Le rapport d'expérience professionnelle comprend : • La présentation d'une stratégie de gestion pour l'infrastructure IT de l'organisation, incluant la planification, la mise en œuvre et la maintenance des systèmes et réseaux (C9) • Le développement d'un plan de sécurité comprenant l'évaluation des risques, l'élaboration de politiques de sécurité, et la mise en place de mesures de protection adaptées aux menaces actuelles (C10) • La conception d'un projet innovant appliquant l'IA dans le domaine de la cybersécurité, pour améliorer la détection des menaces, l'analyse des risques ou l'automatisation des réponses aux incidents. (C11)	**-** La performance et la fiabilité sont améliorées en configurant et en maintenant les serveurs, le stockage, et les réseaux. (C9.1) - L'efficacité opérationnelle est accrue par l'automatisation des processus d'infrastructure avec des outils de DevOp. (C9.1) - Les systèmes sont protégés contre les vulnérabilités dès leur conception. (C9.1) - L'infrastructure IT gagne en flexibilité et en évolutivité grâce à l'intégration de solutions cloud. (C9.1) - L'optimisation des ressources cloud permet la réduction des coûts. (C9.1) - Le/la candidat(e) assure une surveillance continue de l'infrastructure. Les incidents sont détectés et résolus rapidement, garantissant une haute disponibilité. (C9.2) - Les droits d'accès et habilitations sont gérés pour prévenir les accès non autorisés, et sécuriser les données et les applications. (C9.2) - L'intégration de technologies émergentes renforce l'innovation et la compétitivité. (C9.2) - La posture de sécurité est continuellement optimisée pour prévenir les attaques. (C10) - Des normes et des frameworks de sécurité reconnus pour structurer la protection des systèmes guident la protection des systèmes. (C10) - Des simulations d'attaque et des tests de pénétration évaluent la résilience des infrastructures face aux cybermenaces. (C10) - La sensibilisation à la sécurité est promue parmi le personnel. (C10) - Des systèmes de détection et de réponse aux incidents sont implémentés pour minimiser les impacts des attaques. (C10) - Des solutions de sécurité avancées, telles que le chiffrement des données et l'authentification multi-facteurs, augmentent la sécurité des données. (C10)

			- Des algorithmes d'IA sont intégrés pour améliorer la détection des menaces et les réponses automatiques dans les systèmes de sécurité. (C11) - L'IA est utilisée pour analyser les données de sécurité en temps réel, permettant une identification rapide des comportements suspects ou des anomalies. (C11) - Des modèles prédictifs sont développés grâce à l'IA pour anticiper les attaques potentielles et renforcer les mesures de sécurité préventives. (C11) - La surveillance de la sécurité et la gestion des incidents sont automatisées avec des solutions basées sur l'IA, réduisant le temps de réponse aux incidents (C11) - Les systèmes d'IA restent efficaces contre les dernières menaces cybersécuritaires grâce à des données à jour. (C11)

4. **Production et Intégration Sécurisés d'Objets Connectés (IoT) avec Renforcement par l'IA** A12. Développement de solutions IoT A13. Application de l'IA pour l'analyse et la sécurité A14. Intégration de pratiques de sécurité avancées	C12 : Développer des solutions IoT innovantes pour améliorer l'efficacité opérationnelle et créer de nouvelles opportunités de service, en intégrant une fluidité dans les systèmes existants et en garantissant la sécurité des données	Le rapport d'expérience professionnelle comprend la présentation d'un projet d'innovation numérique répondant à un problème d'entreprise réel, incluant l'étude de faisabilité, le plan de mise en œuvre et l'évaluation des impacts technologiques et économiques, et incluant : • La conception et la mise en œuvre d'une solution IoT répondant à un besoin spécifique, avec description du processus de développement, des technologies utilisées, et de l'architecture système (C12) • L'intégration de l'IA pour l'analyse de données générées par les objets connectés et pour renforcer les mécanismes de sécurité. La présentation des modèles d'IA utilisés, de leur entraînement, et de leur efficacité dans des scénarios réels (C13) • L'implémentation de pratiques de sécurité avancées pour protéger les solutions IoT contre les menaces et les vulnérabilités. La	Le/la candidat(e) développe des solutions IoT innovantes. - Les dispositifs IoT innovants sur mesure développés par le/la candidat(e) répondent précisément aux exigences des utilisateurs et de l'entreprises. (C12) - Les capteurs et appareils sont programmés pour une collecte de données précise et fiable. (C12) - Des interfaces utilisateur intuitives facilitent la gestion et le contrôle des dispositifs IoT. (C12) - Des protocoles de communication sécurisés sont intégrés pour la transmission des données IoT. (C12 - La collaboration avec des équipes multidisciplinaires assure une intégration fluide des solutions IoT dans les environnements existants. (C12) - Des mesures de sécurité, mises en place dès la phase de conception, protègent les dispositifs et les données contre les cyberattaques. (C12)
	C13 : Utiliser l'intelligence artificielle pour analyser les données issues des dispositifs IoT et renforcer la sécurité des systèmes, permettant ainsi une meilleure prise de décision et une détection précoce des menaces		- L'IA est utilisée pour le traitement et l'analyse avancée des données collectées par les dispositifs IoT. L'IA optimise les processus et la prise de décision grâce à une analyse avancée des données IoT. (C13) - Des algorithmes d'IA sont implémentés pour la détection précoce des anomalies et des menaces de sécurité dans les réseaux IoT. La réactivité aux incidents est améliorée. (C13) - Des systèmes d'alerte intelligents basés sur l'IA informent en temps réel des risques et permettent une intervention rapide. (C13)
	C14 : Intégrer des pratiques de sécurité avancées dans la conception et le déploiement des solutions IoT, en utilisant l'IA pour anticiper, détecter et répondre de manière proactive aux vulnérabilités et aux attaques cybernétiques		Le/la candidat(e) intègre des pratiques de sécurité avancées dans les solutions IoT avec l'IA. - La cryptographie et la sécurité basées sur l'IA protègent contre les intrusions et fuites de données. (C14) - Le/la candidat(e) développe des protocoles de sécurité avancés pour la communication entre les dispositifs IoT. Il/elle s'appuye sur l'IA pour adapter dynamiquement les mesures de sécurité en fonction du niveau de risque détecté.

		description des stratégies de sécurité adoptées, des tests de pénétration réalisés, et des mesures de mitigation appliquées (C14)	- Des audits réguliers des systèmes IoT à l'aide d'outils d'IA identifient et corrigent proactivement les vulnérabilités. (C14)