2025/2026

Colint School

PROGRAMME PÉDAGOGIQUE

Préparation à la certification
TP - Expert en informatique et systèmes d'information

RNCP 40573 de niveau 7, publié par le Ministère du Travail, le 25/03/2025

Sommaire

Façonnez l'avenir du numérique

Colint vous forme et vous évalue afin de vous préparer à la certification : **Préparation à la certification TP - Expert en informatique et systèmes d'information RNCP40573 de niveau 7,** Délivré par 3W Academy - certification professionnelle enregistrée au RNCP par décision de France Compétences le 25/03/23
La date d'enregistrement est le 30/04/2025.

Méthode pédagogique et d’accompagnement Colint

L’intelligence Collective, au service de votre réussite.

La méthode pédagogique de la Colint School se distingue par une approche centrée sur l’apprenant et l’intelligence collective. Nous proposons un changement de paradigme par rapport aux méthodes d'enseignement traditionnelles, en plaçant l’apprenant au cœur du processus d’apprentissage.

La méthode projet
Les étudiants travaillent sur des projets concrets, en lien avec les problématiques actuelles du marché. Cette approche leur permet de développer des compétences pratiques et d’acquérir une expérience professionnelle significative.

L’Intelligence collective
L‘intelligence collective est au cœur de notre pédagogie. Les apprenants sont encouragés à partager leurs connaissances, à échanger leurs idées et à apprendre les uns des autres.

Le coaching pédagogique
Nos coachs pédagogiques accompagnent individuellement et collectivement les apprenants tout au long de leur parcours. Ils les aident à développer leurs compétences, à surmonter les difficultés et à atteindre leurs objectifs.

Modalités pédagogiques - Présentiel
Les étudiants doivent être présents sur le site de Colint School, pour les inciter à travailler en groupe et favoriser l’intelligence collective.

Ressources à votre disposition

Matériel

- Salles
- Ordinateurs
- Logiciels
- Plateforme e-learning (Qwasar)

Référents

- Responsable handicap : Sophie DUCROS
- Référent pédagogique : Kwame YAMGNANE
- Référent administratif : Stéphane SARR
- Référent mobilité géographique : Stéphane SARR

Accompagnement personnalisé

Principaux formateurs

- Iléana BUSELLI-GARS (coach savoir-être) : Bachelor Concepteur et Développeur d'Applications, Chef de Projet SI
- Olivier JACQUES (coach d'anglais) : Master en commerce international, Responsable des Opérations Export
- Antoine MILLE (coach programmation) : Titre d'Expert en ingénierie logicielle d'Epitech, Head of SG market / Solutions web project
- Kwame YAMGNANE (responsable du mastère) : Ingénieur Epita, co-fondateur de l'école 42

Recrutement

Modalités d'accès à la formation

Prérequis :

- Être titulaire d'un diplôme ou titre de niveau 6 (équiv. Bac + 3/4) en spécialité informatique ou justifiant d'une expérience professionnelle équivalente.
- Être titulaire d'un diplôme ou titre de niveau 7 (équiv. Bac +5) en spécialité scientifique ou justifiant d'une expérience professionnelle équivalente.

Délais d'accès :

- Envoi d'un e-mail de candidature, au format libre, avec une réponse sous 3 jours ouvrés.
- Test de culture générale & logique et Entretien de motivation, avec une réponse sous 5 jours.
- Ouverture du dossier d'inscription, dans un délai maximum de 30 jours.
- Intégration de la Colint School

Objectifs et contexte de la certification

La certification professionnelle Expert en informatique et systèmes d'information s'inscrit dans le secteur du numérique, en croissance continue depuis 15 ans, et soumis à des tendances structurelles fortes : Le Cloud qui modifie structurellement les métiers liés au développement, aux infrastructures et augmente les besoins d'expert en cybersécurité ; L'exploitation des données massives des entreprises par les modèles d'intelligence artificielle qui révolutionne la prise de décisions dans les entreprises et ouvre des opportunités importantes pour toutes les organisations ; L'intégration des technologies d'IA générative au cœur des processus des entreprises, transformant en profondeur leurs organisations ; Le « numérique responsable », devenu un levier essentiel pour les entreprises, et qui concerne en particulier l'éco conception des applications, la durabilité et la consommation d'énergie et l'éthique lié à l'exploitation des données et à l'IA.

Activités visées

L'Expert en informatique et systèmes d'information recouvre des activités clés :

- Déploiement d'une veille technologique et réglementaire et exploitation des résultats.
- Élaboration d'une stratégie informatique adaptée aux besoins identifiés.
- Formulation de solutions architecturales adaptées.
- Identification des besoins du client dans le cadre d'un projet informatique.
- Élaboration du cahier des charges techniques d'un projet informatique.
- Gestion opérationnelle du projet informatique validé.
- Pilotage et management des équipes du projet.
- Conception d'une application informatique.
- Développement d'une application informatique et de son environnement.
- Élaboration d'une stratégie de cybersécurité.

Selon la fonction spécifique exercée/ le projet concerné, le métier d'Expert en informatique et systèmes d'information peut également recouvrir des activités plus spécialisées :

- Liées au management de la cybersécurité : Élaboration d'une stratégie de cybersécurité ; Identification de vulnérabilités potentielles et suivi de l'activité.
- Liées à l'implémentation de modèles de Big Data et d'intelligence artificielle : Analyse et exploitation des données massives pour optimiser la prise de décision ; Optimisation de l'exploitation des données et conception de solutions IA.

Objectifs pédagogiques du cursus

- Analyser les besoins métiers pour concevoir des solutions informatiques adaptées.
- Concevoir et piloter des architectures techniques et logicielles robustes et évolutives.
- Gérer des projets informatiques complexes, en intégrant les dimensions qualité, sécurité, coût et délai.
- Superviser la mise en œuvre de systèmes d'information, en assurant leur cohérence avec les objectifs stratégiques de l'entreprise.
- Assurer la veille technologique et réglementaire, notamment en matière de cybersécurité, RGPD, IA, etc.
- Encadrer des équipes techniques et collaborer avec les directions métiers.
- Conduire des audits et des diagnostics sur les systèmes existants pour proposer des améliorations.

Points forts de l'année

- Approche projet fil rouge : chaque compétence est mise en pratique dans des projets concrets.
- Focus sur innovation et éco-conception : intégration des enjeux Green IT et IA responsable.
- Préparation à la certification RNCP 40573 avec livrables conformes au référentiel.

Projets Clefs

- Cartographie et analyse des risques SI (méthodes EBIOS, ISO 27005).
- Conception et développement d'une application sécurisée avec CI/CD.
- Optimisation via Big Data et IA : pipeline de données + modèle prédictif.
- Présentation du Projet de fin d'études (PFE).

Conférence

- Tech Show, du 18 & 19 Novembre 2026, à Paris.
- Semaine de préparation intensive au passage du titre.

Après la formation

Débouchés

- Ingénieur études & développement
- Ingénieur logiciel
- Ingénieur informatique/ systèmes d'information (SI)
- Responsable de projet IT
- Consultant business intelligence (BI) / informatique (IT)
- Expert en informatique décisionnelle
- Lead Dev
- Architecte big data
- Data engineer/ Data analyst
- Expert en sécurité informatique
- Consultant en cybersécurité

Etude d'employabilité en Bourgogne Franche-Comté

Selon l'Observatoire de l'emploi BFC, une Enquête Besoins en Main-d'Œuvre 2025, ainsi que le site EMFOR BFC :

Contexte régional de l'emploi dans le numérique

- 11 450 salariés travaillent dans le secteur du numérique en Bourgogne-Franche-Comté.
- Ce secteur est en croissance, notamment dans les bassins d'emploi de Dijon, Besançon, Montbéliard et Chalon-sur-Saône.
- Les métiers liés à l'informatique, à la cybersécurité, à la data et à la gestion des systèmes d'information sont identifiés comme métiers porteurs.

Indicateurs d'employabilité pertinents pour le RNCP 40573

- Demande forte en compétences techniques : architecture des systèmes, cybersécurité, cloud computing, gestion de projet IT.
- Tensions de recrutement dans les métiers de développeur, ingénieur systèmes et réseaux, chef de projet informatique, data analyst.
- Mobilité interrégionale : les diplômés peuvent facilement accéder à des postes dans les régions voisines (Auvergne-Rhône-Alpes, Île-de-France) où la demande est encore plus forte.
- Alternance et insertion : les parcours en alternance sont particulièrement valorisés par les entreprises locales, qui cherchent à fidéliser les talents.

Indicateurs de performance

- Les taux de réussite et d'abandon seront calculés avec les 1ères promotions, à partir de septembre 2027.
- Le taux de satisfaction global est de 78,80%.
- Pour plus d'informations, consultez les statistiques https://travail-emploi.gouv.fr/.

Année d'obtention de la certification	Nombre de certifiés	Nombre de certifiés à la suite d'un parcours vae	Taux d'insertion global à 6 mois (en %)	Taux d'insertion dans le métier visé à 6 mois (en %)	Taux d'insertion dans le métier visé à 2 ans (en %)
2023	64	0	92	89	-
2022	26	0	100	88	100

Contenu Pédagogique - Technique - 1ère année (420h)

Module	Durée (h)	Bloc de compétences	Outils et Technologies
Veille technologique, innovation (BC01) *English Project*	35h	**C1.** Concevoir et structurer une veille technologique et règlementaire, en ciblant les nouvelles technologies qui limitent l'impact environnemental des projets et favorisent la sécurité informatique, et en évaluant les sources d'information selon les normes appropriées, afin de répondre aux évolutions du marché et à l'obsolescence du système d'information (SI). **C2.** Synthétiser les données issues de la veille en validant leur fiabilité, l'impact sur l'environnement, les gains et les risques possibles pour en faire une restitution disponible et compréhensible aux acteurs du projet. **C3.** Recommander des solutions innovantes en s'appuyant sur les résultats de la veille afin de conseiller les parties prenantes.	Flipboard, Google Alerts Gartner CNIL / EUR-Lex GitHub Trending ThoughtWorks Tech Radar Miro, Notion Perplexity AI / ChatGPT Cloud Carbon Footprint
Stratégie SI (BC01) & Cadrage SMSI (mineure)	80h	**C4.** Schématiser une cartographie du SI en utilisant une méthode d'analyse de risques pour anticiper les besoins du projet. **C5.** Élaborer la stratégie informatique à partir de la cartographie validée afin de proposer des axes d'évolution. **C6.** Présenter les préconisations du projet SI et de ses spécifications correspondantes aux parties prenantes du projet. **C28**. En réponse à une demande interne ou externe, cartographier les risques de sécurité d'un SI affectant la confidentialité, l'intégrité ou la disponibilité des actifs afin de mettre en évidence les vulnérabilités et les risques. **C29** : Élaborer une stratégie de cybersécurité. Il définit la politique de sécurité (PSSI) et les règles de gouvernance.	Draw.io, LucidChart, Miro Archimate / TOGAF tools Ebios Risk Manager (ANSSI) Norme ISO/IEC 27001:2022
Cahier des charges & cadrage projet (BC02 + mineure)	40h	**C10.** Analyser la problématique du client dans une transformation digitale, en évaluant les enjeux, défis et besoins, afin de formaliser une étude d'opportunité pour la mise en œuvre du projet. **C11.** Évaluer et organiser les fonctionnalités requises en les classant selon leur importance et leur impact, afin de prioriser les implémentations. **C12.** Constituer des solutions techniques en coordonnant les processus du cahier des charges fonctionnel afin de construire un cahier des charges technique conforme RGPD et intégrant l'accessibilité PSH. **C13.** Décrire chaque fonctionnalité attendue dans le cahier des charges technique en utilisant une modélisation des processus métier et en tenant compte des contraintes et de l'existant.	Miro / Notion / Trello / Jira / Github / Confluence Lucidchart / Draw.io Figma RGPD Compliance Tools Wave / Axe DevTools / Lighthouse Airtable Discord

		C14. Rédiger une note de cadrage définissant la démarche, les objectifs, les délais, le budget, les ressources et les exigences de qualité.	
Planification, pilotage & gouvernance (BC02 + mineure)	40h	**C15.** Planifier le projet en décomposant les phases et en allouant les ressources nécessaires. **C16.** Coordonner les méthodes de gestion de projet adaptées au contexte. **C17.** Développer et intégrer des stratégies de mitigation des risques. **C18.** Coordonner la communication entre parties prenantes. **C19.** Gérer l'engagement des parties prenantes. **C20.** Organiser la capitalisation et le partage des compétences.	Trello / Jira / Github / Miro / Notion Discord Airtable
Architecture & Urbanisation (BC01 + mineure)	30h	**C7.** Comparer les différents types d'architectures en identifiant leurs caractéristiques et leurs cas d'usage afin de schématiser leurs interactions. **C8.** Analyser les composants de ces architectures en indiquant leurs fonctions et dépendances afin d'évaluer leur performance et de proposer des améliorations. **C9.** Comprendre les avantages et inconvénients de chaque type d'architecture afin de recommander des solutions adaptées répondant aux contraintes de sécurité, de performance, de scalabilité et d'éco-conception.	AWS Well-Architected Tool Azure Architecture Center Dynatrace / New Relic Cloud Carbon Footprint
Réseaux & systèmes approfondi (Majeure)	120h	**C28**. En réponse à une demande interne ou externe, cartographier les risques de sécurité d'un SI affectant la confidentialité, l'intégrité ou la disponibilité des actifs afin de mettre en évidence les vulnérabilités et les risques. **C29**. Élaborer une stratégie de cybersécurité en respectant les normes et accords de niveaux de services, et en intégrant les critères d'accessibilité pour les personnes en situation de handicap (PSH), les exigences du RGPD, ainsi que les obligations légales en cas de cyberattaque, afin de sécuriser les systèmes de manière optimale et de garantir la souveraineté numérique. **C30**. Évaluer l'efficacité des mesures de protection mises en place en effectuant des tests d'intrusion ("pentest"), pour identifier les vulnérabilités potentielles. **C31**. Structurer et mener une analyse approfondie d'un système d'information après une intrusion ou une attaque informatique, en utilisant des techniques de "forensic" pour examiner les preuves, identifier les vulnérabilités exploitées, et déterminer l'impact d'un potentiel incident. **C32**. Identifier et alimenter des indicateurs d'activité pertinents pour soutenir le processus décisionnel, en fournissant des analyses détaillées et des rapports réguliers sur les performances et les tendances.	DNS, NTP, Kerberos, LDAP, delegations
Pentesting	40h	CTF progressifs (TryHackMe, HackTheBox) et labs supervises	TryHackMe, HackTheBox

Crypto	55h	Les 93 controles de l'Annexe A (ISO 27001:2022) : organisation, personnes, physique, technologique Controle des acces logiques : IAM, MFA, principe du moindre privilege Cryptographie : gestion des cles, PKI, chiffrement des donnees au repos et en transit Securite physique : controle d'acces aux locaux, protection du materiel Securite des systemes et reseaux : durcissement, patch management, journalisation Relations fournisseurs et sous-traitants : clause securite, audit, SLA Lien avec la Major : comment les resultats de pentest alimentent les controles	

Contenu Pédagogique - Soft skills - 1ère année (58h)

Module	Durée (h)	Bloc de compétences	Outils et Technologies
Anglais	8h	• Communiquer par écrit et oralement en utilisant le vocabulaire approprié	
Culture générale et droit du numérique	10h	• Synthétiser des données fournies par le client • Intégrer des contraintes budgétaires, techniques ou environnementales	
Savoir être	20h	• Communiquer par écrit et oralement en utilisant le vocabulaire approprié • Synthétiser des données fournies par le client • Intégrer des contraintes budgétaires, techniques ou environnementales • S'assurer du bon déroulement du projet • Collaborer à la gestion d'un projet informatique et à l'organisation de l'environnement de développement.	
Analyse, la posture et la résolution de problèmes	20h	• Développer une posture professionnelle adaptée aux interlocuteurs (DSI, clients, équipes) • Pratiquer l'écoute active pour comprendre les enjeux au-delà du besoin exprimé • Résoudre des problèmes complexes en utilisant des méthodes structurées • Travailler efficacement dans des environnements pluridisciplinaires • Gérer son stress et maintenir une attitude professionnelle en situation de pression • Faire preuve d'adaptabilité lorsqu'un contexte, une contrainte ou une priorité change • Prendre des décisions éclairées dans l'incertitude	
Total	294		

Contenu Pédagogique - Technique - 2ème année (420h)

Module	Durée (h)	Bloc de compétences	Outils et Technologies
SecOps & Pentest (Majeure)	140h	**C28**. En réponse à une demande interne ou externe, cartographier les risques de sécurité d'un SI affectant la confidentialité, l'intégrité ou la disponibilité des actifs afin de mettre en évidence les vulnérabilités et les risques. **C29**. Élaborer une stratégie de cybersécurité en respectant les normes et accords de niveaux de services, et en intégrant les critères d'accessibilité pour les personnes en situation de handicap (PSH), les exigences du RGPD, ainsi que les obligations légales en cas de cyberattaque, afin de sécuriser les systèmes de manière optimale et de garantir la souveraineté numérique. **C30**. Évaluer l'efficacité des mesures de protection mises en place en effectuant des tests d'intrusion ("pentest"), pour identifier les vulnérabilités potentielles. **C31**. Structurer et mener une analyse approfondie d'un système d'information après une intrusion ou une attaque informatique, en utilisant des techniques de "forensic" pour examiner les preuves, identifier les vulnérabilités exploitées, et déterminer l'impact d'un potentiel incident. **C32**. Identifier et alimenter des indicateurs d'activité pertinents pour soutenir le processus décisionnel, en fournissant des analyses détaillées et des rapports réguliers sur les performances et les tendances.	ThreatDragon, Snyk, GitGuardian CrowdStrike, Darktrace, Tenable.io Microsoft Sentinel, SIEM Nmap, Metasploit, Burp Suite, Wireshark
Conception technique & architecture applicative (BC03)	70h	**C21.** Concevoir une architecture applicative en produisant des maquettes représentatives et sécurisées. **C22.** Schématiser les processus métier en tenant compte des contraintes et vulnérabilités. **C23.** Recommander un environnement informatique cohérent et éco-responsable. **C24.** Justifier l'utilisation de patterns logiciels pour assurer modularité, réutilisabilité et maintenabilité.	Draw.io, Lucidchart Miro Figma, Canva AWS / Azure / GCP / Clever Cloud Architecture Diagrams tools MongoDB / PostgreSQL SonarQube
Développement sécurisé (BC03)	100h	**C25.** Développer des applications métiers en appliquant des pratiques de sécurité rigoureuses. **C26.** Rédiger et exécuter des scénarios de tests pour détecter et corriger les erreurs. **C27.** Concevoir un suivi qualité automatisé incluant un cycle complet CI/CD.	OWASP ZAP SonarQube GitHub Advanced Security Postman Apache Airflow Talend Open Studio HuggingFace / OpenAI APIs KeepA.io / CNIL Outils RGPD

PFE & Préparation à l'examen	110h		

Contenu Pédagogique - Soft skills - 2ème année (109h)

Module	Durée (h)	Bloc de compétences	Outils et Technologies
Anglais	10h	• Communiquer par écrit et oralement en utilisant le vocabulaire approprié	
Culture générale et droit du numérique	19h	• Synthétiser des données fournies par le client • Intégrer des contraintes budgétaires, techniques ou environnementales	
Savoir être	30h	• Communiquer par écrit et oralement en utilisant le vocabulaire approprié • S'assurer du bon déroulement du projet • Collaborer à la gestion d'un projet informatique et à l'organisation de l'environnement de développement.	
Leadership, influence et gestion des interactions complexes	50h	• Développer un leadership positif pour fédérer les équipes autour des objectifs du projet • Gérer les conflits et tensions en adoptant une posture constructive • Influencer et convaincre grâce à une argumentation structurée et objective • Animer des réunions ou ateliers avec aisance, clarté et neutralité • Engager les parties prenantes en clarifiant attentes, enjeux et responsabilités • Identifier et anticiper les risques humains dans le projet (résistance, incompréhension, démotivation) • Favoriser la coopération et encourager le partage de connaissances au sein des équipes • Synthétiser des données fournies par le client • Intégrer des contraintes budgétaires, techniques ou environnementales	
Total	546		

Modalités d'évaluation

La certification RNCP 40573 repose sur une évaluation structurée autour de blocs de compétences, chacun donnant lieu à des épreuves spécifiques. Les modalités incluent des mises en situation professionnelles, des études de cas, des projets techniques, ainsi que des oraux de présentation. Les candidats doivent produire des livrables écrits tels que :

- A. Dossier de cartographie et Analyse de risques
    - Cartographies du SI : Schémas infrastructure et applicatif mettant en évidence la segmentation réseau et les zones de confiance.
    - Inventaire des actifs primordiaux : Identification des processus métiers critiques et des données sensibles de l'organisation.
    - Tableau d'analyse DIC : Évaluation des besoins de sécurité sur trois piliers : Disponibilité, Intégrité et Confidentialité.
    - Matrice des risques : Analyse des menaces (Ransomware, espionnage, fuite de données) et identification des vulnérabilités prioritaires.
- B. Dossier de conception d’architecture sécurisée
    - Tableau comparatif : Analyse comparative entre une architecture traditionnelle et une approche moderne
    - Schéma d'architecture cible : Modélisation incluant les dispositifs de défense
    - Justification des composants : Argumentaire sur la réduction de la surface d'attaque et la performance des briques de sécurité choisies
- C. Note de stratégie SI & Gouvernance SMSI
    - Roadmap à 3 ans : Planification des projets techniques et organisationnels de sécurisation et de mise en conformité (NIS2 / RGPD).
    - Synthèse de la PSSI : Définition des règles d'or de la Politique de Sécurité des Systèmes d'Information applicables à l'entreprise.
    - Plan de Traitement des Risques (PTR) : Arbitrages stratégiques (réduction, transfert à l'assurance, ou acceptation des risques résiduels).
- D. Présentation
    - Support de restitution: Pitch structuré pour convaincre un Board ou une Direction Générale d'investir dans la cyber-résilience.

Accessibilité

Les locaux sont accessibles aux personnes à mobilité réduite.

L’ensemble de nos cursus de formation et d’évaluation préparant à la certification peuvent être adaptés aux besoins de compensation de l’handicap.

Contacter notre référent handicap à l’adresse suivante : handicap@colint.school.

Planning de la formation

Le cursus de formation a une durée totale de 1 an et 8 mois.

Remarque : La durée peut être personnalisée en fonction du positionnement du candidat ou d’un besoin de compensation du handicap.

Le mois type de l’étudiant, lors du contrat d’alternance, est réparti comme suit : 3 semaines en entreprise et 1 semaine en formation.

54 rue d’Autun
71100 Chalon sur Saône
08 05 29 81 56
contact@colint.school
https://colint.school

En cas de handicap, contacter handicap@colint.school