

Expert en sécurité des développements informatiques

RNCP37173 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326n, 326t
Formacode(s)	31006, 31067, 72054
Code(s) ROME	M1802, M1805
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	14/12/2022
Date d'échéance	14/12/2025

Certificateur(s)

AIROBJECT · SIRET : 53970902200039

Partenaires habilités

2 organismes habilités, d'après la liste publiée par France compétences : 2 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
ACADENICE	91520875500024	Former et organiser l'évaluation
AIROBJECT	53970902200039	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

Dans un contexte où la cybercriminalité croît, les cyberattaques de grande ampleur se multiplient aussi bien contre les services publics que les entreprises privées, partout dans le monde et dans tous les secteurs. La sécurité est au cœur des cybers-enjeux d'aujourd'hui et de demain, mais reste malgré tout en général un sujet de fin de projet informatique. Pourtant, une fois l'application développée, il est beaucoup plus complexe de la sécuriser, pour des raisons techniques et budgétaires.

La certification répond aux besoins des entreprises qui recherchent des experts informatiques ayant des compétences en développements informatique et réseaux, afin de sécuriser l'ensemble des plateformes applicatives des entreprises (logiciel, web, mobile) à travers un profil capable de définir la politique de sécurité, ayant un rôle de prévention au sein des organisations afin de garantir la sécurité d'une application de sa conception, son déploiement jusqu'à sa maintenance.

ACTIVITÉS VISÉES

Bloc 1 : Auditer la sécurité des applications d'un système d'information

L'expert en sécurité des développements informatiques doit garantir la conformité de l'application d'une entreprise avec un ensemble spécifique de critères de sécurité. Pour cela il procède à une analyse des risques reposant sur une méthodologie d'audit et d'analyse de risque reconnue. Il identifie les risques pour en dégager les causes potentielles et analyse ces résultats. Il en déduit un plan d'action permettant de renforcer la sécurité. Ces différentes actions doivent permettre à l'entreprise d'être en mesure de valider une accréditation d'une certification reconnue.

Bloc 2 : Élaborer une politique de sécurisation des applications

Sur l'appui de son expérience, des procédures internes et des résultats d'audit potentiels, l'expert en sécurité des développements informatiques définit la politique de sécurité des développements informatiques de l'entreprise. Il

effectue une veille permanente technique et réglementaire pour se tenir informer des failles pouvant être exploitées par des cybercriminels, au regard des technologies et composants utilisés par l'entreprise. Il coordonne le plan de formation des équipes. Il évangélise et anime des ateliers de formations pour sensibiliser notamment les équipes de développements aux meilleures pratiques.

Bloc 3 : Concevoir et développer une application sécurisée

L'expert en sécurité des développements informatiques s'assure que les hypothèses de sécurité relatives à l'environnement de son architecture applicative sont clairement énoncées et prises en compte dans sa conception. Il veille à ce que les exigences de sécurisation applicables aux différents constituants de son architecture ou aux outils permettant de la produire soient effectivement mises en œuvre. Il participe à la conception de l'architecture et de l'implémentation de l'application à développer en s'assurant que les différentes briques disposent du niveau de sécurité adapté aux contextes du projet sur les aspects techniques et métiers.

L'expert en sécurité des développements informatiques analyse et prend en charge les volets sécurité (objectifs, niveau de criticité et attentes en termes de résilience), en liaison avec les équipes de développement et de sécurité, des projets informatiques et programmes dans l'infrastructure. Il planifie, coordonne, en relation avec les autres secteurs concernés (systèmes, réseaux, système de gestion base de données, etc.), les besoins d'intégration exprimés. Il contribue à la qualification technique et à l'intégration des développements informatiques dans l'environnement de production, afin de s'assurer que seuls les utilisateurs autorisés pourront y accéder. Il développe des composants sécurisés, ainsi que des scripts de simulation pour les tests.

Bloc 4 : Piloter un projet d'application sécurisée

L'expert en sécurité des développements informatiques intervient dès la conception d'un projet. Ses compétences lui permettent de comprendre les problématiques à traiter dans un contexte de sécurité. Au-delà de ces compétences techniques, il sait analyser les besoins des utilisateurs et anticiper les nouveaux usages. Il réalise les spécifications des applications et produit les documents techniques à destination des équipes de développement et de production, en veillant à ce qu'elles résistent aux attaques à tous les niveaux : interface, design, code source et ce que dès sa conception. Pour cela, il mobilise des méthodes de gestion de projet agile et des méthodes d'analyse en besoin de sécurité.

L'expert en sécurité des développements informatiques traduit les exigences techniques en plans réalisables pour développer et mettre en œuvre les solutions proposées. Il encadre l'équipe projet afin d'atteindre les objectifs fixés et contrôler que les programmes développés sont sécurisés. Il apporte l'outillage DevSecOps qui automatise les tâches du développeur.

Il optimise la sécurité d'une application au niveau du codage, ce qui la rend moins vulnérable aux menaces, en opérant un contrôle plus étendu sur le résultat d'entrées inattendues. Il s'assure que ses équipes testent la sécurité des applications logicielles lors du processus de développement, afin de vérifier que l'application et sa mise à jour ne présentent aucune vulnérabilité. Il encadre et anime les audits et revues de code au sein de l'équipe puis automatise plusieurs types de tests. Par sa maîtrise des techniques d'audits de sécurité, il réalise également des pentest (test de pénétration) afin d'essayer d'accéder à l'application. Ils administrent les analyses de sécurité non authentifiées et authentifiées (en tant qu'utilisateurs connectés) afin de détecter les vulnérabilités de sécurité susceptibles d'apparaître pour ces deux types d'analyse.

Bloc 5 : Déployer et maintenir la sécurisation des applications d'un SI

L'expert en sécurité des développements informatiques déploie l'infrastructure sécurisée nécessaire au développement, au test, au déploiement dans l'environnement de production des applications afin de garantir la sécurité de l'application de bout en bout. Il construit les pipelines CI/CD pour des déploiements automatisés grâce à l'utilisation de la technologie de gestion de la configuration. Il est ainsi garant de la continuité de l'application et en porte la responsabilité.

Les applications d'aujourd'hui sont souvent disponibles sur divers réseaux et connectées au Cloud, ce qui augmente leur vulnérabilité aux menaces et aux violations de sécurité. Il est garant de la sécurité au niveau du réseau, mais également au sein des applications elles-mêmes à travers la mise en place de pare-feu d'applications Web. Il accompagne les équipes Ops sur la sécurisation des applications et leur déploiement, y compris dans des environnements Cloud. Il supervise également la maintenance une fois le produit mis en route et testé en contrôlant le fait que l'application intègre toujours la dimension sécurité face aux menaces et vulnérabilités communes. Il veille et assure la mise à jour automatisée des applications et de ses composants face aux failles reconnues.

Il s'assure que les utilisateurs ont uniquement accès aux données qu'ils sont autorisés à afficher dans leurs applications Cloud, où les données sensibles sont plus vulnérables. En cas d'incident de sécurité dans une application, il s'appuie sur des outils d'analyse (journalisation) pour identifier les utilisateurs ayant eu accès aux données concernées et comprendre comment ils ont pu y parvenir.

COMPÉTENCES ATTESTÉES

Définir un plan d'audit adapté en termes de moyens, ressources, organisation et contraintes réglementaires, par l'application d'une méthodologie d'audit, afin de déterminer précisément les failles et non conformités des applications d'un système d'information.

Conduire une analyse de sécurité de l'information et des données des applications d'un système d'information, en s'appuyant sur un plan d'audit, afin d'identifier les risques et menaces et d'en dégager les causes.

Analyser les écarts au regard des procédures définies au plan d'audit en rédigeant un rapport d'audit, afin de déterminer le

plan d'action permettant de renforcer la sécurité des applications et du SI.

Établir un plan d'action comportant les mesures de sécurité techniques et organisationnelles correctives et préventives, afin de corriger les non conformités et remédier aux failles de sécurité des applications et de leurs interactions avec le système d'information.

Préparer l'entreprise à la certification en sécurité de l'information, par une démarche d'accréditation à partir d'une norme de certification, afin de rassurer les clients et les partenaires.

Définir une politique de sécurité des applications du système d'information adaptée à l'activité de l'entreprise, à l'aide des différents acteurs et

procédures existantes, afin de répondre à ses enjeux.

Mettre en place un référentiel

"développeur sécurité" à destination des développeurs, en définissant des protocoles de développement et de tests issus du Security by Design, afin d'élaborer des bonnes pratiques par l'utilisation des outils (framework, composants...) les plus pertinents.

Évaluer les dernières vulnérabilités connues et les opportunités technologiques, en organisant une veille axée juridique, réglementaire et technique, afin de répondre aux enjeux de sécurité de l'entreprise.

Analyser les compétences des équipes en matière de sécurité des applications, au moyen de questionnaires et d'entretiens, afin de concevoir et mettre en place un plan de formation.

Sensibiliser et former les équipes, à un niveau approprié, aux meilleures pratiques de sécurité, risque et conformité à travers un plan de formation, afin d'améliorer leur niveau de compréhension des problématiques de sécurité informatique.

Utiliser le référentiel général d'amélioration de l'accessibilité (RGAA), afin d'adapter la formation interne de la sécurité aux personnes handicapées.

Modéliser une architecture applicative et technique sécurisée, en s'appuyant sur une analyse des besoins et des spécificités du SI, afin de répondre aux exigences de sécurité durant tout le cycle de vie de l'application.

Structurer les choix technologiques et méthodologiques, en sélectionnant les solutions adaptées, afin de qualifier leur intégrations dans l'environnement de production et minimiser surface d'attaque à laquelle l'application va être exposée.

Définir l'automatisation des tests, par la mise en oeuvre des processus et outils adaptés aux tests techniques et fonctionnels automatisés, afin de garantir l'intégrité au niveau applicatif et des données.

Rédiger les spécifications techniques des attentes en matière d'architecture de solutions de sécurité, en vue de la rédaction du cahier des charges, afin de permettre la réalisation de l'application par les équipes de développement.

Coder des composants web, logiciel ou mobile conformes aux spécifications fonctionnelles et techniques, de sécurité et de performance, afin de tester leur robustesse à travers des outils de tests.

Intégrer des composants technologiques externes, en appliquant des règles de conception des fonctionnalités définies, afin de mettre en oeuvre une architecture applicative sécurisée.

Concevoir un projet de développement sécurisé, par l'application d'une méthode de gestion de projet agile, afin de gérer les besoins de sécurité lors du développement d'une application, afin de minimiser les attaques et garantir la sécurité des programmes.

Planifier les différentes activités à réaliser à travers des outils collaboratifs nécessaires à la collaboration et au partage d'informations, afin d'assurer la bonne diffusion des informations liées à la sécurité auprès de l'ensemble des équipes de développement.

Coordonner et motiver les équipes pour implémenter de manière appropriée les fonctionnalités spécifiées, afin de contrôler que les règles de codage préalablement définies sont appliquées dans le cycle de vie du projet de manière pertinente.

Mettre à disposition des outils et des infrastructures de développement pour optimiser et industrialiser les travaux des équipes de développement, afin d'atteindre les objectifs du projet.

Accompagner une personne en situation de handicap afin de faciliter son intégration dans l'équipe et dans son

environnement de travail.

Mener une analyse statique (analyse de code et de dépendance) et dynamique (pentest) des développements réalisés à travers des outils sélectionnés et automatisés, afin de tester la sécurité de l'application.

Analyser les ambiguïtés non détectées lors des tests et corriger les failles détectées, afin de remédier aux attaques avant le déploiement de l'application.

Déployer une architecture technique sécurisée, en appliquant les méthodes et outils définis par la politique de sécurité de l'entreprise, afin de garantir le niveau de sécurité et fonctionnement opérationnel des applications.

Superviser la sécurité des applications en mettant

œuvre des solutions techniques de protection automatisées, afin de protéger les données sensibles de l'application.

Déployer des solutions de monitoring pour être alerté de l'apparition des anomalies de sécurité dans le système, afin d'établir une surveillance la plus complète des événements et limiter l'impact d'un incident de sécurité.

Assurer la continuité d'activité des applications en concevant un plan de reprise d'activité, en s'appuyant sur la norme ISO, afin d'automatiser le traitement des incidents.

Suivre l'obsolescence et maintenir à jour les composants et de stacks logiciels devenus vulnérables, en installant les patches correctifs, afin de corriger les menaces et failles de sécurité et maintenir l'intégrité des applications.

Définir un plan de remédiation permettant de réagir aux incidents de sécurité, en s'appuyant sur des mesures de contournements et des solutions techniques précédemment identifiées, afin de pallier à de nouveaux incidents de sécurité et en réduire les impacts.

Mener une investigation technico légale, en s'appuyant sur les outils adéquats afin d'identifier la cause des incidents de sécurité et d'y apporter des solutions.

Évaluer la performance des mesures de sécurité en place, à travers la définition, la mise en œuvre et le pilotage des indicateurs clés de sécurité,

afin d'assurer l'amélioration continue des dispositifs de sécurité et mettre à jour les procédures.

Blocs de compétences

RNCP37173BC01 — Auditer la sécurité des applications d'un système d'information

LISTE DE COMPÉTENCES

Définir un plan d'audit adapté en termes de moyens, ressources, organisation et contraintes réglementaires, par l'application d'une méthodologie d'audit, afin de déterminer précisément les failles et non conformités des applications d'un système d'information.

Conduire une analyse de sécurité de l'information et des données des applications d'un système d'information, en s'appuyant sur un plan d'audit, afin d'identifier les risques et menaces et d'en dégager les causes.

Analyser les écarts au regard des procédures définies au plan d'audit en rédigeant un rapport d'audit, afin de déterminer le

plan d'action permettant de renforcer la sécurité des applications et du SI.

Établir un plan d'action comportant les mesures de sécurité techniques et organisationnelles correctives et préventives, afin de corriger les non conformités et remédier aux failles de sécurité des applications et de leurs interactions avec le système d'information.

Préparer l'entreprise à la certification en sécurité de l'information, par une démarche d'accréditation à partir d'une norme de certification, afin de rassurer les clients et les partenaires.

MODALITÉS D'ÉVALUATION

Etude de cas portant sur une organisation qui souhaite se préparer à la certification CSPN de l'ANSSI en s'appuyant sur une méthodologie d'analyse de risque afin de qualifier les enjeux, les menaces des applications du SI.

RNCP37173BC02 — Mettre en place une politique de sécurisation des applications

LISTE DE COMPÉTENCES

Définir une politique de sécurité des applications du système d'information adaptée à l'activité de l'entreprise, à l'aide des différents acteurs et

procédures existantes, afin de répondre à ses enjeux.

Mettre en place un référentiel

“développeur sécurité” à destination des développeurs, en définissant des protocoles de développement et de tests

issus du Security by Design, afin d'élaborer des bonnes pratiques par l'utilisation des outils (framework, composants...) les plus pertinents.

Evaluer les dernières vulnérabilités connues et les opportunités technologiques, en organisant une veille axée juridique, réglementaire et technique, afin de répondre aux enjeux de sécurité de l'entreprise.

Analyser les compétences des équipes en matière de sécurité des applications, au moyen de questionnaires et d'entretiens, afin de concevoir et mettre en place un plan de formation.

Sensibiliser et former les équipes, à un niveau approprié, aux meilleures pratiques de sécurité, risque et conformité à travers un plan de formation, afin d'améliorer leur niveau de compréhension des problématiques de sécurité informatique.

Utiliser le référentiel général d'amélioration de l'accessibilité (RGAA), afin d'adapter le formation interne de la sécurité aux personnes handicapées.

MODALITÉS D'ÉVALUATION

Etude de cas portant sur une entreprise qui souhaite former ses développeurs à travers des ateliers de développements sécurisés et notamment sur le Security by Design. Le candidat dispose des résultats d'une enquête pour connaître le niveau de chacun des collaborateurs, la cartographie des applications du SI et les résultats des audits de sécurité et des actions mises en place par l'entreprise.

RNCP37173BC03 — Concevoir et développer une application sécurisée

LISTE DE COMPÉTENCES

Modéliser une architecture applicative et technique sécurisée, en s'appuyant sur une analyse des besoins et des spécificités du SI, afin de répondre aux exigences de sécurité durant tout le cycle de vie de l'application.

Structurer les choix technologiques et méthodologiques, en sélectionnant les solutions adaptées, afin de qualifier leur intégrations dans l'environnement de production et minimiser surface d'attaque à laquelle l'application va être exposée.

Définir l'automatisation des tests, par la mise en oeuvre des processus et outils adaptés aux tests techniques et fonctionnels automatisés, afin de garantir l'intégrité au niveau applicatif et des données.

Rédiger les spécifications techniques des attentes en matière d'architecture de solutions de sécurité, en vue de la rédaction du cahier des charges, afin de permettre la réalisation de l'application par les équipes de développement.

Coder des composants web, logiciel ou mobile conformes aux spécifications fonctionnelles et techniques, de sécurité et de performance, afin de tester leur robustesse à travers des outils de tests.

Intégrer des composants technologiques externes, en appliquant des règles de conception des fonctionnalités définies, afin de mettre en oeuvre une architecture applicative sécurisée.

MODALITÉS D'ÉVALUATION

Etude de cas portant sur la conception d'une nouvelle fonctionnalité sécurisée (web et mobile) au sein d'une application SAAS d'un éditeur de logiciel. Il est mis à disposition du candidat un cahier des charges et un environnement où il peut programmer sur l'application et réaliser les tests.

RNCP37173BC04 — Piloter un projet d'application sécurisée

LISTE DE COMPÉTENCES

Concevoir un projet de développement sécurisé, par l'application d'une méthode de gestion de projet agile, afin de gérer les besoins de sécurité lors du développement d'une application, afin de minimiser les attaques et garantir la sécurité des programmes.

Planifier les différentes activités à réaliser à travers des outils collaboratifs nécessaires à la collaboration et au partage d'informations, afin d'assurer la bonne diffusion des informations liées à la sécurité auprès de l'ensemble des équipes de développement.

Coordonner et motiver les équipes pour implémenter de manière appropriée les fonctionnalités spécifiées, afin de contrôler que les règles de codage préalablement définies sont appliquées dans le cycle de vie du projet de manière pertinente.

Mettre à disposition des outils et des infrastructures de développement pour optimiser et industrialiser les travaux des équipes de développement, afin d'atteindre les objectifs du projet.

Accompagner une personne en situation de handicap afin de faciliter son intégration dans l'équipe et dans son environnement de travail.

Mener une analyse statique (analyse de code et de dépendance) et dynamique (pentest) des développements réalisés à travers des outils sélectionnés et automatisés, afin de

tester la sécurité de l'application.

Analyser les ambiguïtés non détectées lors des tests et corriger les failles détectées, afin de remédier aux attaques avant le déploiement de l'application.

MODALITÉS D'ÉVALUATION

Etude de cas portant sur les tests lors de la finalisation d'un projet d'évolution d'application (nouvelles fonctionnalités) avant son déploiement, sur la base de programmes informatiques développés.

RNCP37173BC05 — Déployer et maintenir la sécurisation des applications d'un SI

LISTE DE COMPÉTENCES

Déployer une architecture technique sécurisée, en appliquant les méthodes et outils définis par la politique de sécurité de l'entreprise, afin de garantir le niveau de sécurité et fonctionnement opérationnel des applications.

Superviser la sécurité des applications en mettant

œuvre des solutions techniques de protection automatisées, afin de protéger les données sensibles de l'application.

Déployer des solutions de monitoring pour être alerté de l'apparition des anomalies de sécurité dans le système, afin d'établir une surveillance la plus complète des événements et limiter l'impact d'un incident de sécurité.

Assurer la continuité d'activité des applications en concevant un plan de reprise d'activité,

en s'appuyant sur la norme ISO, afin d'automatiser le traitement des incidents.

Suivre l'obsolescence et maintenir à jour les composants et de stacks logiciels devenus

vulnérables, en installant les patches correctifs, afin de corriger les menaces et failles de sécurité et maintenir l'intégrité des applications.

Définir un plan de remédiation permettant de réagir aux incidents de sécurité, en s'appuyant sur des mesures de contournements et des solutions techniques précédemment identifiées, afin de pallier à de nouveaux incidents de sécurité et en réduire les impacts.

Mener une investigation technico légale, en s'appuyant sur les outils adéquats afin d'identifier la cause des incidents de sécurité et d'y apporter des solutions.

Évaluer la performance des mesures de sécurité en place, à travers la définition, la mise en œuvre et le pilotage des indicateurs clés de sécurité,

afin d'assurer l'amélioration continue des dispositifs de sécurité et mettre à jour les procédures.

MODALITÉS D'ÉVALUATION

Etude de cas portant sur l'analyse d'un incident sur une application en production dans le cloud, remontée par une équipe Ops.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Les entreprises employeurs sont principalement celles qui développent des logiciels ou des applications SAAS. L'expert en sécurité des développements informatiques peut être employé dans des entreprises de toutes tailles : entreprises et institutions publiques et privées dotées de systèmes d'informations (éditeur de logiciel, cabinet de conseil en informatique, ESN) dans tous les secteurs, ou entreprises de services numériques et organismes spécialisés en cybersécurité.

TYPE D'EMPLOIS ACCESSIBLES

- Développeur sécurité
- DevSecOps
- Architecte sécurité
- Champion security
- Pentester
- Architecte cybersécurité
- Directeur cybersécurité
- Intégrateur de solutions de sécurité
- Développeur de solutions de sécurité
- Consultant sécurité
- Responsable SOC (security operation center)
- Analyste SOC
- Security Project Manager Officer (PMO)

- Program Manager IT program manager
- Architecte sécurité
- Architecte Sécurité Informatique
- Intégrateur de sécurité
- Chef de projet sécurité
- Product security officer
- Chief Product Security Officer

RÉGLEMENTATIONS D'ACTIVITÉ

L'expert en sécurité des développements informatiques ne dépend pas d'une réglementation spécifique. Cependant, afin d'assurer ses différentes activités, il doit nécessairement suivre les préconisations de plusieurs organismes reconnus comme des autorités de la cyber sécurité des systèmes d'informations. Parmi ceux-ci on retrouve :

- l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ;
- l'Open Web Application Security Project (OWASP) ;
- l'Internet Security Research Group (ISRG) ;

Marché du travail

Indicateurs au niveau des familles professionnelles (FAP) des métiers visés, agrégés au niveau national — France Travail / DARES (open data).

Tension de recrutement (DARES 2024)	Très élevée (5/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 4 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible, Lien formation-emploi
Salaire médian (mensuel)	2 942 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (41 % des actifs en emploi)
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique · tension 4/5 (Élevée) M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom · tension 5/5 (Très élevée) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	32 216
Jugés difficiles à recruter	51 %
Emplois saisonniers	1 %
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

Être titulaire d'un titre de niveau 6 ou justifier d'une expérience professionnelle significative dans le domaine Informatique

PRÉREQUIS À LA VALIDATION

L'obtention de la certification est conditionnée à la validation de l'ensemble des 5 blocs de compétences. Pour se présenter aux épreuves certificatives, les candidats devront au préalable avoir participé aux évaluations en cours de formation, avoir remis les travaux demandés, et avoir satisfait aux exigences en matière de participation aux évaluations.

Le jury est composé d'1 responsable pédagogique et de 2 professionnels externes qui ne connaissent ni professionnellement ni personnellement le candidat, et qui sont légitimes et compétents pour évaluer les compétences définies dans le référentiel. Ils doivent exercer depuis au moins 3 ans le métier visé. Le président du jury est un membre du jury professionnel extérieur ; il est désigné par le directeur de l'école.

Financement en alternance (NPEC)

Niveau de prise en charge d'un contrat d'apprentissage par les OPCO, fixé par France compétences par branche professionnelle (CPNE).

Prise en charge usuelle	8 696 €
Selon la branche	7 500 € – 9 157 €
Prise en charge	Branches concernées
8 696 €	Valeur par défaut · 198 branches
9 157 €	CPNE Casinos, CPNE autoroutes, CPNE des Télécoms, CPNEF de l'audiovisuel, CPNEF de la Publicité
9 005 €	CPNE FP Branche des magasins du Bricolage
9 000 €	CPNEFP des industries des tuiles et briques
8 813 €	CPNEFP Professions de la Photographie
8 775 €	CPNEFP de la branche des entreprises du bureau et du numérique (commerces et services)
8 600 €	CPNEFP de l'habillement, mercerie, chaussure et jouet
8 500 €	CPNEFP de la métallurgie
8 347 €	CPNEFP de la Branche des Caisses régionales de Crédit Agricole et autres organismes
7 697 €	CPNEFP de la blanchisserie, laverie, location de linge, nettoyage à sec, pressing et teinturerie
7 500 €	CPNE des industries de santé (CPNEIS)

Base légale

Date de décision	14/12/2022
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	14/12/2025
Date de dernière délivrance possible	14/12/2029

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://livecampus.fr/formation-expert-securite-developpement-informatique/>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/37173/>

Se former en apprentissage

Formations en apprentissage	1
Organismes gestionnaires (CFA)	1

Organismes formateurs	1
Régions couvertes	1
Départements couverts	1
Organismes certifiés Qualiopi	1
Formations à distance	1
Sessions	de 10/2024 à 10/2026

Catalogue des formations en apprentissage — réseau des Carif-Oref. Sans frais pour l'alternant : formation financée par l'OPCO de la branche (NPEC).