

Expert en cybersécurité

RNCP42868 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326
Formacode(s)	31038, 31045, 42881, 13235, 24231
Code(s) ROME	M1802, M1805
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	30/09/2026
Date d'échéance	30/09/2029

Certificateur(s)

ESGCV · SIRET : 75253547600325

HETIC · SIRET : 49336137200011

PSTB-PARIS SCHOOL OF TECHNOLOGY & BUSINESS EN ABREGE P.S.T.B · SIRET : 81209558600044

Partenaires habilités

4 organismes habilités, d'après la liste publiée par France compétences : 4 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
ESGCV -75253547600143	75253547600143	Former et organiser l'évaluation
GALILEO VAE	90077772300033	Former et organiser l'évaluation
INSTITUT DE MANAGEMENT ECOLE SUP GESTI	39039183700031	Former et organiser l'évaluation
STUDI	91114836900018	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

Dans un contexte de transformation numérique généralisée et de multiplication des menaces cyber, les organisations font face à des risques croissants portant sur la sécurité de leurs systèmes d'information, de leurs données et de leur patrimoine immatériel. L'évolution des technologies, des usages numériques, du cadre réglementaire et des modes d'attaque impose un renforcement des compétences expertes en cybersécurité.

Le métier d'expert en cybersécurité couvre aujourd'hui des responsabilités élargies, allant de l'analyse stratégique des risques à la conception et au pilotage des politiques de sécurité de l'information, en passant par la gestion des incidents et des crises cyber, la gouvernance de la sécurité, la conformité réglementaire et l'accompagnement des transformations organisationnelles et technologiques des systèmes d'information.

La certification a pour objectif d'apporter les compétences nécessaires à l'exercice autonome du métier d'Expert en cybersécurité et de ses activités professionnelles complexes. Elle repose sur un socle de compétences transversales en gouvernance, déploiement et pilotage de la cybersécurité, complété par des blocs de spécialisation permettant d'approfondir des domaines à forte valeur stratégique et/ou à des demandes en forte évolution. Elle vise ainsi à répondre aux besoins actuels et futurs des organisations en matière de résilience numérique, de sécurité des systèmes d'information et de maîtrise des risques cyber.

ACTIVITÉS VISÉES

La certification vise les activités suivantes :

Activités communes :

Définition du dispositif de pilotage de la politique de sécurité de l'information

Pilotage d'un système de veille scientifique, géopolitique, technologique, réglementaire, sectorielle

Réalisation d'audit périodique de cybersécurité auprès d'une/plusieurs organisations

Définition des axes et des objectifs stratégiques en matière de cybersécurité

Planification du déploiement de la politique de sécurité à l'échelle d'une organisation

Déploiement de la politique de sécurité de l'information

Evaluation de la nature et de la criticité des risques

Organisation des structures de pilotage stratégique et techniques des plans de traitement des risques en matière de sécurité au sein de l'organisation

Gestion de incidents liés à la sécurité de l'information

Diffusion d'une culture SSI à destination des utilisateurs et décideurs

Conception stratégique et pilotage d'un projet de transformation et/ou d'innovation SI/cybersécurité

Définition et structuration d'une réponse au développement d'un projet de transformation et/ ou d'innovation cybersécurité

Pilotage du déploiement du projet de transformation/ d'innovation de cybersécurité

Sélection et identification de partenaires (prestataires, fournisseurs, experts)

Accompagnement au changement et à l'appropriation des bonnes pratiques en matière de cybersécurité

Management des hommes et des équipes dans un contexte de pilotage de chantiers cyber

Identification des besoins en compétences nécessaires au déploiement de projet IT / Cyber

Supervision de la réalisation des objectifs individuels et collectifs d'une équipe IT et/ou cyber

Activités de spécialisation :

Déploiement de solutions d'intelligence artificielle en cybersécurité (Spécialisation A- cybersécurité et intelligence artificielle)

Conception et intégration d'une solution IA en cybersécurité

Sécurisation des modèles IA de cybersécurité

Encadrement de l'usage réglementaire et éthique des traitements IA

Déploiement sécurisé de systèmes embarqués et autonomes (Spécialisation B- IoT, drones, robotique)

Conception d'une architecture de cybersécurité embarquée

Sécurisation des communications du système embarqué et/ou autonome

Pilotage du projet de cybersécurité embarquée

Définition d'un dispositif stratégique de renseignement cyber (spécialisation C- renseignement, cti, osint)

Collecte et qualification de données de renseignement cyber

Analyse et modélisation des scénarios de menace cyber

Restitution stratégique du renseignement cyber

Gouvernance de la lutte contre les menaces informationnelles numériques (spécialisation D- cybersécurité et lutte informationnelle d'influence (I2i)

Détection, analyse et neutralisation des campagnes de manipulation de l'information dans un contexte numérique conflictuel.

Sécurisation des environnements d'influence

Pilotage d'un dispositif de lutte informationnelle

COMPÉTENCES ATTESTÉES

Élaborer un dispositif de veille scientifique, technologique et réglementaire afin d'anticiper les évolutions stratégiques en cybersécurité.

Piloter la réalisation et/ou réaliser un audit de gouvernance et physique du SI de l'organisation afin de réaliser un état des lieux exhaustif des risques et de la maturité des systèmes SI.

Mettre en œuvre une méthode d'analyse de risques de cybersécurité en concertation avec les métiers afin de prioriser les scénarios de risques et de proposer des mesures de sécurité adaptées.

Élaborer la politique de sécurité de l'information d'une/plusieurs organisations afin d'assurer un dispositif conforme, performant et responsable.

Planifier les plans d'actions sécurité permettant le déploiement de la politique de sécurité de l'information en déterminant les objectifs, les mesures de sécurité et le calendrier de suivi de manière à suivre les risques et renforcer

la sécurité du SI.

Développer un dispositif d'évaluation continue des risques en cybersécurité pour anticiper les impacts potentiels et renforcer la résilience opérationnelle.

Mettre en place une gouvernance opérationnelle de la cybersécurité afin d'assurer un suivi régulier et une amélioration continue des mesures de sécurité

Déployer des mesures de sécurité organisationnelles (politiques d'accès, procédures, sensibilisation) et techniques (firewall avancés, VPN, cryptographie renforcée...), afin de garantir la conformité réglementaire et une sécurité opérationnelle renforcée.

Piloter la gestion opérationnelle des incidents de cybersécurité en mobilisant des techniques avancées (forensic, SIEM, analyses logs approfondies...), afin d'identifier rapidement leur origine, mesurer leur impact et assurer une réponse adaptée et efficace.

Former et sensibiliser les collaborateurs afin de diminuer les risques de cybersécurité liée aux comportements humains.

Élaborer le cadrage stratégique d'un projet de transformation ou d'innovation SI/Cyber afin de proposer des solutions durables et sécurisées.

Rédiger une proposition de réponse à un projet de développement en cybersécurité afin de maximiser les chances de succès de la proposition dans un contexte de marché.

Définir l'organisation et les étapes d'un projet de transformation et/ou d'innovation afin de prioriser les différents chantiers SI

Identifier et sélectionner des partenaires (prestataires, fournisseurs, experts...) afin de garantir la réussite du projet de transformation ou d'innovation SI/cyber.

Piloter l'accompagnement au changement suite au déploiement d'un projet SI/Cybersécurité afin de favoriser l'adoption durable des bonnes pratiques de cybersécurité.

Evaluer l'adéquation entre les compétences des collaborateurs d'une DSI et/ou d'une équipe projet cyber et le besoin en compétences de manière à déployer un plan de développement de compétences, de formation, et/ou de recrutement adaptés aux enjeux stratégiques de l'entreprise.

Accompagner les collaborateurs dans la définition et la réalisation de leurs objectifs individuels et collectifs afin de garantir performance et conditions de travail équitables.

Mettre en œuvre un management de délégation aux membres d'une équipe projet cybersécurité ou d'une direction IT afin d'assurer une répartition optimale du travail et l'atteinte efficace des objectifs fixés.

Spécialisation A : cybersécurité et intelligence artificielle

Piloter la conception d'un système d'intelligence artificielle destiné à détecter des comportements suspects ou malveillants afin d'améliorer la détection et la prévention des menaces.

Intégrer un système d'intelligence artificielle dans un dispositif de sécurité afin de garantir la robustesse, la supervision et la conformité des traitements automatisés.

Renforcer la résilience du système d'intelligence artificielle contre des attaques ciblées (data poisoning, adversarial input, inversion)

afin de garantir la continuité et la fiabilité des traitements automatisés.

Superviser la conformité réglementaire et éthique de l'usage de l'intelligence artificielle dans un dispositif de cybersécurité afin de garantir la transparence et la légitimité des décisions automatisées.

Spécialisation B : IoT, drones, robotique

Concevoir une architecture sécurisée pour systèmes embarqués ou autonomes (IoT, drones, robots) afin de prévenir les intrusions.

Renforcer la résilience du système embarqué ou autonome afin de garantir la fiabilité et la résilience du dispositif.

Piloter un projet de cybersécurité appliqué à un système autonome ou embarqué

afin d'assurer la conformité et la robustesse du dispositif.

Spécialisation C : renseignement, cti, osint

Concevoir un dispositif de renseignement cyber afin d'alimenter la stratégie de détection des menaces.

Superviser la conformité éthique, juridique et normative d'un dispositif de renseignement cyber afin de garantir la légitimité et la conformité des pratiques.

Modéliser les menaces cyber à partir de données de renseignement afin d'anticiper les comportements hostiles et adapter les mesures de sécurité.

Structurer des rapports de renseignement stratégiques à destination de la direction générale afin de faciliter l'arbitrage en période de crise ou pour orienter les choix de sécurité.

Spécialisation D : cybersécurité et lutte informationnelle d'influence (I2i)

Analyser une opération d'influence numérique afin d'éclairer les décisions stratégiques de réponse informationnelle.
Renforcer la sécurité informationnelle des environnements numériques exposés à des opérations d'influence afin de limiter la propagation de la désinformation.
Piloter un dispositif de lutte informationnelle afin d'anticiper les attaques informationnelles et d'organiser la réponse de manière cohérente et réactive.

Blocs de compétences

RNCP42868BC01 — Définir le dispositif de pilotage de la politique de sécurité de l'information

LISTE DE COMPÉTENCES

Élaborer un dispositif de veille scientifique, technologique et réglementaire en mobilisant des sources fiables et les cadres éthiques applicables, tout en intégrant les innovations issues de la transition numérique, afin d'anticiper les évolutions stratégiques en cybersécurité.

Piloter la réalisation et/ou réaliser un audit de gouvernance et physique du SI de l'organisation et/ou des partenaires en : définissant les objectifs visés par l'audit, conduisant des interviews auprès des audités (administrateurs système, développeurs, commanditaire, collaborateurs ...), réalisant des analyses techniques sur des points de contrôles précisés, et en supervisant des tests d'intrusion approfondis afin de réaliser un état des lieux exhaustif des risques et de la maturité des systèmes SI.

Mettre en œuvre une méthode d'analyse de risques de cybersécurité en concertation avec les métiers en s'appuyant sur une cartographie des actifs et des menaces afin de prioriser les scénarios de risques et de proposer des mesures de sécurité adaptées.

Élaborer la politique de sécurité de l'information d'une/plusieurs organisations en définissant le SMSI et les objectifs de sécurité, en intégrant la sobriété numérique et les enjeux de transition numérique, afin d'assurer un dispositif conforme, performant et responsable.

Planifier les plans d'actions sécurité permettant le déploiement de la politique de sécurité de l'information en déterminant les objectifs, les mesures de sécurité et le calendrier de suivi de manière à suivre les risques et renforcer la sécurité du SI.

MODALITÉS D'ÉVALUATION

Mémoire professionnel

Mise en situation professionnelle

portant sur la mise en place d'une politique de sécurité

RNCP42868BC02 — Déployer la politique de sécurité de l'information

LISTE DE COMPÉTENCES

Développer un dispositif d'évaluation continue des risques en cybersécurité en réalisant régulièrement des simulations d'incidents pour anticiper les impacts potentiels et renforcer la résilience opérationnelle.

Mettre en place une gouvernance opérationnelle de la cybersécurité par un pilotage stratégique formalisé (tableaux de bord, indicateurs de suivi, reporting ...) afin d'assurer un suivi régulier et une amélioration continue des mesures de sécurité

Déployer des mesures de sécurité organisationnelles (politiques d'accès, procédures, sensibilisation) et techniques (firewall avancés, VPN, cryptographie renforcée...), en s'appuyant notamment sur les référentiels tels que ISO 27002 par exemple et le guide ANSSI..., afin de garantir la conformité réglementaire et une sécurité opérationnelle renforcée.

Piloter la gestion opérationnelle des incidents de cybersécurité en mobilisant des techniques avancées (forensic, SIEM, analyses logs approfondies...), afin d'identifier rapidement leur origine, mesurer leur impact et assurer une réponse adaptée et efficace.

Former et sensibiliser les collaborateurs au travers de : la rédaction d'une charte informatique, la réalisation de campagne d'information (communication, sensibilisation et formation), l'animation de campagne de live-hacking, et en partageant les risques en matière de cybersécurité et les impacts RSE associés, afin de diminuer les risques de cybersécurité liée aux comportements humains.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle

portant sur le déploiement d'une politique de sécurité

RNCP42868BC03 — Concevoir et piloter un projet de transformation et/ou d'innovation SI/cybersécurité

LISTE DE COMPÉTENCES

Élaborer le cadrage stratégique d'un projet de transformation ou d'innovation SI/Cyber en mobilisant les données techniques, économiques et environnementales, et en intégrant les enjeux de transition numérique, afin de proposer des solutions durables et sécurisées.

Rédiger une proposition de réponse à un projet de développement en cybersécurité, en structurant les aspects techniques, méthodologiques et financiers, et en valorisant les avantages concurrentiels de l'offre, afin de maximiser les chances de succès de la proposition dans un contexte de marché.

Définir l'organisation et les étapes d'un projet de transformation et/ou d'innovation, les principaux livrables, les besoins en ressources humaines, matérielles et financières, ainsi que les contraintes spécifiées par la maîtrise d'ouvrage afin de prioriser les différents chantiers SI

Identifier et sélectionner des partenaires (prestataires, fournisseurs, experts...) en tenant compte de critères techniques, organisationnels, économiques et normatifs précis (PASSI, ISO 27001...), afin de garantir la réussite du projet de transformation ou d'innovation SI/cyber.

Piloter l'accompagnement au changement suite au déploiement d'un projet SI/Cybersécurité en mobilisant des outils (charte de sécurité, procédure...) et méthodes de conduite du changement adaptés à la singularité des personnes (handicap, intergénérationnel...) et du projet de cybersécurité de manière à permettre l'acculturation des collaborateurs et la gestion des résistances.

MODALITÉS D'ÉVALUATION

Mise en situation professionnel dans le cadre d'une problématique rencontrée par une entreprise réelle ou fictive portant sur un projet (transformation numérique, sécurisation d'infrastructure, audit externalisé...)

RNCP42868BC04 — Manager des hommes et des équipes dans un contexte de pilotage de chantiers cyber

LISTE DE COMPÉTENCES

Évaluer l'adéquation entre les compétences des collaborateurs d'une DSI et/ou d'une équipe projet cyber et le besoin en compétences nécessaires au soutien des besoins fonctionnels et stratégiques IT de manière à déployer un plan de développement de compétences, de formation, et/ou de recrutement adaptés aux enjeux stratégiques de l'entreprise.

Accompagner les collaborateurs dans la définition et la réalisation de leurs objectifs individuels et collectifs, en veillant à l'équilibre des charges et à l'adaptation des suivis aux besoins spécifiques, tout en tenant compte des enjeux de santé afin de garantir performance et conditions de travail équitables.

Mettre en œuvre un management de délégation aux membres d'une équipe projet cybersécurité ou d'une direction IT, en tenant compte de leurs compétences individuelles, des enjeux du projet et des impératifs opérationnels, afin d'assurer une répartition optimale du travail et l'atteinte efficace des objectifs fixés.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle portant sur un cas de management d'une entreprise réelle ou fictive

RNCP42868BC05 — Déployer des solutions d'intelligence artificielle en cybersécurité (spécialisation A)

LISTE DE COMPÉTENCES

Piloter la conception d'un système d'intelligence artificielle destiné à détecter des comportements suspects ou malveillants en exploitant les données issues du SI (logs, flux réseau, alertes) tout en intégrant des objectifs de performance énergétique et de transition numérique responsable afin d'améliorer la détection et la prévention des menaces.

Intégrer un système d'intelligence artificielle dans un dispositif de sécurité en appliquant des pratiques de MLOps sécurisées (déploiement contrôlé, supervision, journalisation, traçabilité), afin de garantir la robustesse, la supervision et la conformité des traitements automatisés.

Renforcer la résilience du système d'intelligence artificielle contre des attaques ciblées (data poisoning, adversarial input, inversion) en réalisant une analyse de vulnérabilité et en mettant en œuvre des mécanismes de protection adaptés afin de garantir la continuité et la fiabilité des traitements automatisés.

Superviser la conformité réglementaire et éthique de l'usage de l'intelligence artificielle dans un dispositif de cybersécurité, en appliquant les exigences réglementaires (RGPD, IA Act) et les principes d'éthique algorithmique afin de garantir la transparence et la légitimité des décisions automatisées.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle portant sur la mise en œuvre d'une solution IA dans un environnement de cybersécurité

RNCP42868BC06 — Déployer des systèmes embarqués et autonomes sécurisés (spécialisation B)

LISTE DE COMPÉTENCES

Concevoir une architecture sécurisée pour systèmes embarqués ou autonomes (IoT, drones, robots), en intégrant les contraintes techniques et les principes d'écoconception numérique, afin de prévenir les intrusions.

Renforcer la résilience du système embarqué ou autonome en identifiant ses vulnérabilités par des tests ciblés, et en déployant des mécanismes adaptés de sécurité (chiffrement, authentification, contrôle d'intégrité...) afin de garantir la fiabilité et la résilience du dispositif.

Piloter un projet de cybersécurité appliqué à un système autonome ou embarqué en intégrant les contraintes légales, normatives et techniques afin d'assurer la conformité et la robustesse du dispositif.

MODALITÉS D'ÉVALUATION

Mise en situation portant sur la conception d'une architecture embarquée sécurisée

RNCP42868BC07 — Définir un dispositif stratégique de renseignement cyber (spécialisation C)

LISTE DE COMPÉTENCES

Concevoir un dispositif de renseignement cyber, en structurant un système de collecte des données issues de sources ouvertes, techniques ou comportementales (OSINT, CTI, SIGINT, logs, réseaux sociaux...), en mobilisant des outils de veille automatisée et des méthodes d'analyse contextuelle* (origine, fiabilité, temporalité, diffusion), afin d'alimenter la stratégie de détection des menaces.

Superviser la conformité éthique, juridique et normative d'un dispositif de renseignement cyber, en identifiant les risques liés aux traitements mis en œuvre, en intégrant les exigences réglementaires, et en mettant en place les mesures de régulation adaptées, afin de garantir la légitimité et la conformité des pratiques.

Modéliser les menaces cyber à partir de données de renseignement, en mobilisant des cadres d'analyse reconnus et des méthodes de corrélation et de qualification, afin d'anticiper les comportements hostiles et adapter les mesures de sécurité.

Structurer des rapports de renseignement stratégiques à destination de la direction générale, en traduisant des données techniques complexes en scénarios d'aide à la décision lisibles, contextualisés et priorisés, afin de faciliter l'arbitrage en période de crise ou pour orienter les choix de sécurité.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle portant sur la mise en place d'un dispositif de renseignement cyber

RNCP42868BC08 — Mettre en place un système de gouvernance de lutte contre les menaces informationnelles numériques (spécialisation D)

LISTE DE COMPÉTENCES

Analyser une opération d'influence numérique en identifiant les acteurs, les contenus manipulés, les canaux et les leviers cognitifs mobilisés, à partir d'une veille ciblée, d'outils d'OSINT et d'intelligence artificielle, afin d'éclairer les décisions stratégiques de réponse informationnelle.

Renforcer la sécurité informationnelle des environnements numériques exposés à des opérations d'influence, en identifiant les vulnérabilités techniques, en mobilisant des outils d'IA pour la détection automatisée de contenus falsifiés, de comportements inauthentiques et de narratifs manipulateurs, afin de limiter la propagation de la désinformation.

Piloter un dispositif de lutte informationnelle en définissant les objectifs, les moyens d'analyse, les canaux d'intervention et les modalités de coordination interservices, afin d'anticiper les attaques informationnelles et d'organiser la réponse de manière cohérente et réactive.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle

portant sur la conception et mise en œuvre d'une réponse à une opération d'influence numérique

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

La cybersécurité concerne aujourd'hui l'ensemble des secteurs d'activités. Néanmoins, certains secteurs sont davantage la cible des cyberattaques. Parmi eux figurent les secteurs suivants, sans en être toutefois restrictif : Le secteur bancaire - L'administration publiques & les collectivités - L'informatique et les télécommunications - L'enseignement et la recherche - Le secteur énergétique - La santé - Le service aux entreprises - L'industrie Chimique / Parachimique / Agroalimentaire - Le transport et la logistique.

TYPE D'EMPLOIS ACCESSIBLES

L'expert en cybersécurité peut se spécialiser dans des domaines d'expertise . De ce fait, les intitulés de postes peuvent donc varier selon le domaine d'expertise dans lequel l'expert en cybersécurité évolue.

Appellations métiers généralistes : Expert en cybersécurité / Responsable de projet de sécurité / Consultant en cybersécurité / Directeur de la cybersécurité / Responsable de la sécurité des systèmes d'information (rssi)

Selon le domaine de spécialisation

:

Spécialisation IA et cyber : Expert IA appliquée à la cybersécurité / Responsable IA et conformité en cybersécurité

Spécialisation

IoT, drones, robotique : Expert cybersécurité embarquée / Ingénieur sécurité IoT /

Manager de projet cybersécurité industrielle

Spécialisation Renseignement,CTI,Osint : Cyber Threat Intelligence Analyst / Responsable veille et renseignement cyber

Spécialisation Cybersécurité et lutte informationnelle d'influence (L2I) : Responsable cybersécurité cognitive / Responsable sécurité informationnelle - influence

RÈGLEMENTATIONS D'ACTIVITÉ

A ce jour, la profession d'expert en cybersécurité n'est pas règlementée dans le sens où il n'est pas nécessaire que le candidat détienne un titre ou qualité particulière, ni ne dispose d'une habilitation ou d'une certification complémentaire.

En revanche, il y a un durcissement de la réglementation en matière de droit du numérique (RGPD, droit des contrats ou encore questions de propriété intellectuelle...). Les titulaires de la certification sont donc formés et évalués sur leur capacité à mobiliser des savoirs pluridisciplinaires, à maintenir leurs connaissances en matière de lois, de réglementations, de normes, référentiels, et recommandations délivrés par les organes compétents.

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 %

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

Les prérequis d'entrée en formation dépendent de la voie d'accès et du cadre de la formation.

En formation initiale (étudiants)

Entrée en 1ère année : Etre titulaire d'une certification de niveau 6 ou d'un diplôme équivalent (diplôme étranger...), ou avoir validé 180 crédits ECTS dans le domaine visé ou proche : l'ingénierie informatique, le développement, les sciences politiques, le droit pénal, l'intelligence économique, la défense et sécurité nationale, conseil & sciences de gestion, etc.

Entrée en 2ème année : Etre titulaire d'une certification de niveau 6 (bac +4), ou d'un diplôme équivalent (diplôme étranger...), ou avoir validé 240 crédits ECTS, dans le domaine visé ou proche : l'ingénierie informatique, le développement, les sciences politiques, le droit pénal, l'intelligence économique, la défense et sécurité nationale, conseil & sciences de gestion, etc.

En alternance (contrat apprentissage ou contrat de professionnalisation)

Pour un cursus en 3 ans : Etre titulaire d'une certification de niveau 5 ou d'un diplôme équivalent (diplôme étranger...), ou avoir validé 120 crédits ECTS dans le domaine visé ou proche : l'ingénierie informatique, le développement, les sciences politiques, le droit pénal, l'intelligence économique, la défense et sécurité nationale, conseil & sciences de gestion, etc.

Pour un cursus en 2 ans : Etre titulaire d'une certification de niveau 6 ou d'un diplôme équivalent (diplôme étranger...), ou avoir validé 180 crédits ECTS dans le domaine visé ou proche : l'ingénierie informatique, le développement, les sciences politiques, le droit pénal, l'intelligence économique, la défense et sécurité nationale, conseil & sciences de gestion, etc.

Pour un cursus en 1 an : Etre titulaire d'une certification de niveau 6 ou d'un diplôme équivalent (diplôme étranger...), ou avoir validé 240 crédits ECTS, dans le domaine visé ou proche : l'ingénierie informatique, le développement, les sciences politiques, le droit pénal, l'intelligence économique, la défense et sécurité nationale, conseil & sciences de gestion, etc.

En formation continue

- Entrée avec un niveau 6 : Etre titulaire d'une certification de niveau 6 ou d'un diplôme équivalent (diplôme étranger...), ou avoir validé 180 crédits ECTS dans le domaine visé ou proche : l'ingénierie informatique, le développement, les sciences politiques, le droit pénal, l'intelligence économique, la défense et sécurité nationale, conseil & sciences de gestion, etc.

- Ou Etre titulaire d'une certification de niveau 6 ou d'un diplôme équivalent (diplôme étranger...), ou avoir validé 180 crédits ECTS, dans un autre domaine de formation/métier de la certification visée et justifier d'une expérience professionnelle dans le secteur visé de 12 mois minimum (pour exemples (non limitatifs): cadre du secteur des Stratégies Informatiques (DSI), de la Sécurité Globale et des Stratégies Sécurité, anciens fonctionnaires du Ministère de la Défense ou de l'Intérieur en reconversion vers le secteur privé)

Dérogation spécifique : Si le candidat ne dispose pas de l'expérience professionnelle ou du diplôme requis, il devra présenter un dossier démontrant sa capacité à suivre la formation et à valider la certification professionnelle (VAP, attestation employeur ou autres preuves d'une expérience professionnelle, personnelle ou associative permettant l'acquisition de compétences connexes...).

Classe dédiée toute voie confondue : dans le cadre d'une classe dédiée - que ce soit en partenariat avec une entreprise, une collectivité locale ou territoriale, une branche professionnelle - les prérequis pourraient être en deçà de ceux prévus initialement. Et dans ce cas, la formation sera adaptée à ce public pour permettre d'assurer les mêmes chances de réussite.

PRÉREQUIS À LA VALIDATION

Avoir respecté les prérequis d'accès d'entrée en formation, et avoir suivi le cursus de formation préparant à la certification

Si le candidat ne dispose pas de l'expérience professionnelle ou du diplôme requis, il devra présenter un dossier démontrant sa capacité à suivre la formation et à valider la certification professionnelle (VAP, attestation employeur ou

autres preuves d'une expérience professionnelle, personnelle ou associative permettant l'acquisition de compétences connexes...).

COMPOSITION DU JURY — FORMATION INITIALE, FORMATION CONTINUE, APPRENTISSAGE, CONTRAT DE PROFESSIONNALISATION, VAE
Le jury est composé de 4 membre dont 50% de professionnels : Le directeur de l'organisme certificateur (ou son représentant) - Le responsable pédagogique (ou son représentant) - Deux professionnels externes exerçant dans le métier visé

Base légale

Date de décision	30/09/2026
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	30/09/2029
Date de dernière délivrance possible	30/09/2033

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2025	9	0	100 %	—
2024	10	0	83 %	—

Liens avec d'autres certifications

ANCIENNES VERSIONS
RNCP37649

CORRESPONDANCES (PAR BLOCS)
RNCP37649

Pour plus d'informations

LIEN VERS LE DESCRIPTIF
/

Fiche officielle (France Compétences)
<https://www.francecompetences.fr/recherche/rncp/42868/>