

Expert en cybersécurité (MS)

RNCP40640 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326
Formacode(s)	31045, 31038, 31025
Code(s) ROME	M1802, M1801, M1806
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	23/05/2025
Date d'échéance	23/05/2030

Certificateur(s)

UNIVERSITE DE TECHNOLOGIE DE TROYES (UTT) · SIRET : 19101060200032

Résumé de la certification

OBJECTIFS ET CONTEXTE

L'expert en cybersécurité (MS) est un professionnel clé dans la protection des systèmes informatiques contre les actes malveillants. Son rôle principal est d'identifier, corriger et prévenir les vulnérabilités et failles susceptibles d'être exploitées par des cybercriminels. Il conçoit, développe et maintient des stratégies de cybersécurité pour garantir l'efficacité et l'intégrité des systèmes informatiques au sein des entreprises. Son champ d'intervention couvre la sécurité des applications, la gestion des droits d'accès, la sécurisation des réseaux, la protection des données, la continuité des opérations et l'élaboration de plans de reprise après incident.

La certification "Expert en Cybersécurité (MS)" vise l'accès aux métiers de la cybersécurité en développant des compétences en analyse des systèmes compromis, en sécurité des dispositifs informatiques, et en gestion des cyber-menaces. La certification couvre les aspects techniques, fonctionnels et juridiques de la sécurité des systèmes d'information (SSI), permettant aux candidats de sécuriser les SI, d'effectuer des audits de sécurité, et de mener des analyses forensiques.

ACTIVITÉS VISÉES

- Traiter les incidents de cybersécurité :

Diagnostic de l'incident de cybersécurité et de son ampleur

Analyse de l'incident de cybersécurité

Remédiation à l'incident de cybersécurité

Participation à l'élaboration de la PSSI

- Analyser la menace cyber pesant sur une organisation :

Détection des incidents et des menaces

Analyse et catégorisation des codes malveillants

Remédiation aux menaces

Veille permanente sur les menaces émergentes

- Auditer la sécurité technique d'une organisation :

Préparation de l'audit de sécurité

Réalisation des tests d'intrusion sur les systèmes, les réseaux, les applications web ou mobiles

- Réaliser une analyse technico-légale (forensique) :

Préparation et collecte des données forensiques

Analyse et rédaction du rapport des preuves numériques

COMPÉTENCES ATTESTÉES

Coordonner la collecte de l'ensemble des informations relatives aux incidents informatiques (journaux d'évènements systèmes et réseau, diagrammes de topologie réseau, images systèmes) en utilisant des outils open-source (autopsy, foremost, scalpel, volatility, plaso, log2timeline, etc.) souvent présents sur la distribution Kali Linux afin d'avoir une première idée sur l'ampleur de la crise.

Trier les éléments liés à l'incident, en définissant des catégories et en les classant, afin d'organiser des éléments de preuves analysables.

Analyser les preuves numériques collectées, en appliquant la méthodologie forensique, à l'aide de la collecte de données brutes ou altérées, en identifiant la nature de l'incident et en reconstituant le déroulement de l'attaque, afin de lancer une action interne ou une procédure judiciaire.

Contextualiser l'incident, en établissant une corrélation

entre signe d'incident et l'analyse de traces informatiques (informations collectées) à l'aide d'outils de modélisation et/ou de visualisation, afin d'établir des scénarii potentiels d'incident.

Élaborer un plan de remédiation, en appliquant les actions de résolution de l'incident dans le respect de la politique de sécurité des systèmes d'information (PSSI), et en définissant des recommandations aux collaborateurs, afin de répondre à la crise cyber.

Organiser la sensibilisation des collaborateurs aux bonnes pratiques en matière de cybersécurité, en expliquant les vulnérabilités, en présentant les derniers correctifs de sécurité et en mettant en place des cas pratiques portant sur les plans de réponse aux incidents, en prenant les dispositions permettant l'appropriation des informations par tous les publics, y compris en situation de handicap, afin de minimiser les risques et les dommages en cas d'attaques cybernétiques.

Enrichir la politique de sécurité (PSSI) et les documents associés, en coordination avec le RSSI et/ou DSI, en utilisant les méthodologies d'analyse de risques (Méhari, EBIOS) ainsi que la norme ISO 27001, en spécifiant les exigences relatives aux systèmes de management de la sécurité des informations (SMSI) etc., afin d'améliorer la sécurité et la résilience du SI.

Définir des actions d'amélioration continue des pratiques, en coopérant avec des experts à l'aide des outils de réponse à incident spécifiques (CERT, plateforme de partage, virus total) dans le but de partager les failles, les vulnérabilités, les indices de compromission, et d'éviter que d'autres structures ne soient affectées par les mêmes menaces.

Assurer la supervision des infrastructures et des événements de sécurité, en exploitant un système de gestion de l'information et des événements de sécurité (SIEM), en utilisant ces informations pour retracer la chronologie d'une cyberattaque, afin de mettre en évidence les signaux faibles qui d'ordinaire passent inaperçus et d'éviter que ces mêmes attaques ne se reproduisent dans le futur.

Détecter en temps réel les incidents de sécurité et les menaces, en identifiant leurs sources et en configurant l'architecture réseau et les systèmes de sécurité, afin de prévenir l'accès non autorisé et de bloquer les tentatives d'intrusion dans le système informatique de l'organisation.

Analyser le code malveillant en employant des techniques d'analyse statique et dynamique, en examinant le comportement du code et en identifiant les signatures et les vecteurs d'attaque potentiels, afin de qualifier et de catégoriser précisément les menaces.

Exploiter l'intelligence artificielle générative, en développant et en déployant des algorithmes d'IA, en simulant des attaques et en analysant des patterns de menaces émergentes, afin d'améliorer continuellement la prévention, la détection et la réaction face aux cyberattaques.

Développer un correctif de sécurité en utilisant la distribution Kali Linux, en programmant avec le langage Python, en créant des scripts Bash sous Linux, et en écrivant des exécutables en C++, afin de fournir aux équipes les outils nécessaires pour répondre efficacement aux incidents de sécurité.

Attribuer l'incident de sécurité en établissant une grille d'analyse d'intrusion, en utilisant des méthodes adéquates telles que la Kill Chain, le Diamond Model et la matrice MITRE ATT&CK, afin de modéliser avec précision les intrusions ciblées.

Anticiper les futures évolutions des menaces en mettant en place un système de veille recensant le renseignement en source ouverte (OSINT), les flux de données commerciaux et communautaires, les médias sociaux (SOCMINT), le renseignement d'origine humaine et la capacité d'analyse et de corrélation (HUMINT), les informations provenant du Deep et Dark web, afin de limiter l'exposition de l'entreprise sur les réseaux sociaux, ou sur les moteurs de recherche, limitant ainsi la surface d'attaque que pourrait exploiter un "hacker".

Analyser le périmètre d'intervention pour les tests d'intrusion, en définissant les modalités et les outils spécifiques à utiliser, notamment nmap, metasploit et armitage de la distribution Kali Linux, afin de réaliser des tests cadrés et

précis qui permettent d'identifier les vulnérabilités potentielles dans les systèmes de l'organisation.

Animer une réunion de cadrage de la phase d'audit de sécurité, en réunissant les représentants des fonctions de gestion de l'information, de la technologie, et de la conformité, en les sensibilisant sur les objectifs de l'audit, les approches méthodologiques, la planification et les responsabilités partagées, et en identifiant les besoins d'adaptation du dispositif pour les personnes en situation de handicap, pour assurer une exécution cohérente et complète de l'audit de sécurité.

Réaliser des tests d'intrusion sur les systèmes, les réseaux, les applications web ou mobiles, en utilisant les outils adéquats selon la méthodologie de tests d'intrusion, tout en assurant une veille technique sur les outils d'audit et les pratiques d'attaque et tests d'intrusion dans le respect du Code pénal spécifique à la cybercriminalité, afin d'identifier les services vulnérables et de détecter les éventuelles menaces ou intrusions.

Superviser l'application de l'ensemble des protocoles de test, en configurant des environnements de simulation sécurisés pour les tests et en validant l'application des scénarios de test selon les spécifications définies, tout en facilitant un échange régulier d'informations entre les membres de l'équipe technique pour assurer la transparence et l'efficacité durant les phases de test.

Élaborer un rapport détaillé des résultats des tests comprenant des captures d'écran des tests et systématiquement, comporter une note explicitant, pour chaque faille ou vulnérabilité découverte, la contre mesure à mettre en place, afin d'éradiquer ou de limiter le risque voire de proposer un plan de remédiation.

Présenter les résultats de l'audit lors d'une session de restitution aux décideurs et aux équipes techniques, en utilisant des outils de visualisations de données pour illustrer les vulnérabilités et les impacts potentiels, et en proposant des recommandations claires pour les actions de remédiation, afin de faciliter la prise de décision et la planification des suivis nécessaires.

Identifier le périmètre et l'environnement technique, en accédant si nécessaire au système d'exploitation ou au matériel pour avoir une vision précise de la volumétrie des données, et en définissant les exigences techniques et opérationnelles de la démarche avec les responsables IT et de projet concernés, afin d'évaluer la quantité de données à acquérir, conformément à la PSSI.

Définir la stratégie de préservation des données, en considérant la volumétrie des données à analyser, le temps dont on dispose, le matériel de copie dont on dispose, et d'autres contraintes externes, et en s'assurant de la conformité aux normes légales auprès des équipes juridiques, afin de rédiger le document de traçabilité des actions effectuées.

Réaliser la collecte de données de manière technico-légale, en utilisant des outils dédiés pour l'extraction des données sur des supports comme les clés USB ou pour la création de copies technico-légales avec des outils open source (tels que dd, dcfldd) et commerciaux (comme FTK Imager), disponibles sur la distribution Kali Linux, et en assurant le respect des politiques internes, de l'éthique et des cadres légaux en lien avec les équipes de sécurité informatique, afin de préserver les preuves numériques dans un contexte d'investigation légale.

Analyser les artefacts numériques identifiés, tels que disques durs, mémoires, traces réseau, journaux d'événements, emails, navigateurs, et smartphones, en employant des techniques et des logiciels d'analyse forensique avancés, afin de tracer et documenter les preuves numériques pour les besoins d'enquêtes et de conformité légale.

Rédiger un rapport d'analyse forensique, en mettant en avant les implications légales, les recommandations de sécurité et les conclusions techniques essentielles, et en adaptant le discours aux publics techniques et institutionnels (forces de l'ordre, magistrat, équipe de réponse à incidents), et en prenant les dispositions permettant l'accès des informations à tous, y compris en cas de handicap, afin de fournir une communication claire et complète des résultats d'investigation aux parties prenantes concernées.

Blocs de compétences

RNCP40640BC01 — Traiter les incidents de cybersécurité

LISTE DE COMPÉTENCES

Coordonner la collecte de l'ensemble des informations relatives aux incidents informatiques (journaux d'événements systèmes et réseau, diagrammes de topologie réseau, images systèmes) en utilisant des outils open-source (autopsy, foremost, scalpel, volatility, plaso, log2timeline, etc.) souvent présents sur la distribution Kali Linux afin d'avoir une première idée sur l'ampleur de la crise.

Trier les éléments liés à l'incident, en définissant des catégories et en les classant, afin d'organiser des éléments de preuves analysables.

Analyser les preuves numériques collectées, en appliquant la méthodologie forensique, à l'aide de la collecte de données brutes ou altérées, en identifiant la nature de l'incident et en reconstituant le déroulement de l'attaque, afin

lancer une action interne ou une procédure judiciaire.

Contextualiser l'incident, en établissant une corrélation entre signe d'incident et l'analyse de traces informatiques (informations collectées) à l'aide d'outils de modélisation et/ou de visualisation, afin d'établir des scénarii potentiels d'incident.

Elaborer un plan de remédiation, en appliquant les actions de résolution de l'incident dans le respect de la politique de sécurité des systèmes d'information (PSSI), et en définissant des recommandations aux collaborateurs, afin de répondre à la crise cyber.

Organiser la sensibilisation des collaborateurs aux bonnes pratiques en matière de cybersécurité, en expliquant les vulnérabilités, en présentant les derniers correctifs de sécurité et en mettant en place des cas pratiques portant sur les plans de réponse aux incidents, en prenant les dispositions permettant l'appropriation des informations par tous les publics, y compris en situation de handicap, afin de minimiser les risques et les dommages en cas d'attaques cybernétiques.

Enrichir la politique de sécurité (PSSI) et les documents associés, en coordination avec le RSSI et/ou DSI, en utilisant les méthodologies d'analyse de risques (Méhari, EBIOS) ainsi que la norme ISO 27001, en spécifiant les exigences relatives aux systèmes de management de la sécurité des informations (SMSI) etc., afin d'améliorer la sécurité et la résilience du SI.

Définir des actions d'amélioration continue des pratiques, en coopérant avec des experts à l'aide des outils de réponse à incident spécifiques (CERT, plateforme de partage, virus total) dans le but de partager les failles, les vulnérabilités, les indices de compromission, et d'éviter que d'autres structures ne soient affectées par les mêmes menaces.

MODALITÉS D'ÉVALUATION

Cas d'études : sont fournis aux candidats des journaux d'événements à l'aide desquels ils doivent réunir les traces informatiques liées à l'incident. Le candidat doit trier les journaux d'événements pour identifier les traces pertinentes. Il est attendu des candidats la rédaction d'un plan de remédiation. Ils doivent proposer des solutions de sécurité en analysant les solutions existantes sur le marché.

RNCP40640BC02 — Analyser la menace cyber pesant sur une organisation

LISTE DE COMPÉTENCES

Assurer la supervision des infrastructures et des événements de sécurité, en exploitant un système de gestion de l'information et des événements de sécurité (SIEM), en utilisant ces informations pour retracer la chronologie d'une cyberattaque, afin de mettre en évidence les signaux faibles qui d'ordinaire passent inaperçus et d'éviter que ces mêmes attaques ne se reproduisent dans le futur.

Détecter en temps réel les incidents de sécurité et les menaces, en identifiant leurs sources et en configurant l'architecture réseau et les systèmes de sécurité, afin de prévenir l'accès non autorisé et de bloquer les tentatives d'intrusion dans le système informatique de l'organisation.

Analyser le code malveillant en employant des techniques d'analyse statique et dynamique, en examinant le comportement du code et en identifiant les signatures et les vecteurs d'attaque potentiels, afin de qualifier et de catégoriser précisément les menaces.

Exploiter l'intelligence artificielle générative, en développant et en déployant des algorithmes d'IA, en simulant des attaques et en analysant des patterns de menaces émergentes, afin d'améliorer continuellement la prévention, la détection et la réaction face aux cyberattaques.

Développer un correctif de sécurité en utilisant la distribution Kali Linux, en programmant avec le langage Python, en créant des scripts Bash sous Linux, et en écrivant des exécutables en C++, afin de fournir aux équipes les outils nécessaires pour répondre efficacement aux incidents de sécurité.

Attribuer l'incident de sécurité en établissant une grille d'analyse d'intrusion, en utilisant des méthodes adéquates telles que la Kill Chain, le Diamond Model et la matrice MITRE ATT&CK, afin de modéliser avec précision les intrusions ciblées.

Anticiper les futures évolutions des menaces en mettant en place un système de veille recensant le renseignement en source ouverte (OSINT), les flux de données commerciaux et communautaires, les médias sociaux (SOCMINT), le renseignement d'origine humaine et la capacité d'analyse et de corrélation (HUMINT), les informations provenant du Deep et Dark web, afin de limiter l'exposition de l'entreprise sur les réseaux sociaux, ou sur les moteurs de recherche, limitant ainsi la surface d'attaque que pourrait exploiter un "hacker".

MODALITÉS D'ÉVALUATION

Cas pratique : D'après des journaux d'événements donnés, les candidats doivent détecter les incidents et les

menaces afin de les bloquer. Il est attendu que les codes malveillants soient analysés et qualifiés. Les candidats doivent proposer des correctifs.

Test écrit: Evaluation des connaissances visant à évaluer la bonne assimilation des termes et des définitions.

Cas pratique : D'après un article de blog à modéliser grâce à la matrice MITRE ATT&CK, en Cyber Kill, Chain et en Intrusion, Diamond Model, le candidat doit rédiger un rapport d'investigation. L'évaluation est orale par les pairs.

Cas pratique : Les candidats doivent programmer un outil de veille (scraper) sur les menaces identifiées.

RNCP40640BC03 — Auditer la sécurité technique d'une organisation

LISTE DE COMPÉTENCES

Analyser le périmètre d'intervention pour les tests d'intrusion, en définissant les modalités et les outils spécifiques à utiliser, notamment nmap, metasploit et armitage de la distribution Kali Linux, afin de réaliser des tests cadrés et précis qui permettent d'identifier les vulnérabilités potentielles dans les systèmes de l'organisation.

Animer une réunion de cadrage de la phase d'audit de sécurité, en réunissant les représentants des fonctions de gestion de l'information, de la technologie, et de la conformité, en les sensibilisant sur les objectifs de l'audit, les approches méthodologiques, la planification et les responsabilités partagées, et en identifiant les besoins d'adaptation du dispositif pour les personnes en situation de handicap, pour assurer une exécution cohérente et complète de l'audit de sécurité.

Réaliser des tests d'intrusion sur les systèmes, les réseaux, les applications web ou mobiles, en utilisant les outils adéquats selon la méthodologie de tests d'intrusion, tout en assurant une veille technique sur les outils d'audit et les pratiques d'attaque et tests d'intrusion dans le respect du Code pénal spécifique à la cybercriminalité, afin d'identifier les services vulnérables et de détecter les éventuelles menaces ou intrusions.

Superviser l'application de l'ensemble des protocoles de test, en configurant des environnements de simulation sécurisés pour les tests et en validant l'application des scénarios de test selon les spécifications définies, tout en facilitant un échange régulier d'informations entre les membres de l'équipe technique pour assurer la transparence et l'efficacité durant les phases de test.

Élaborer un rapport détaillé des résultats des tests comprenant des captures d'écran des tests et systématiquement, comporter une note explicitant, pour chaque faille ou vulnérabilité découverte, la contre mesure à mettre en place, afin d'éradiquer ou de limiter le risque voire de proposer un plan de remédiation.

Présenter les résultats de l'audit lors d'une session de restitution aux décideurs et aux équipes techniques, en utilisant des outils de visualisations de données pour illustrer les vulnérabilités et les impacts potentiels, et en proposant des recommandations claires pour les actions de remédiation, afin de faciliter la prise de décision et la planification des suivis nécessaires.

MODALITÉS D'ÉVALUATION

Cas d'étude : d'après un cas d'étude donnée par le formateur, les candidats doivent réaliser une étude de vulnérabilité visant à définir le périmètre des tests d'intrusion.

Cas pratique : le candidat doit identifier l'ensemble des vulnérabilités dans un serveur. Sont attendus un rapport des résultats et une proposition de correctifs à mettre en place.

RNCP40640BC04 — Réaliser une analyse technico-légale (forensique)

LISTE DE COMPÉTENCES

Identifier le périmètre et l'environnement technique, en accédant si nécessaire au système d'exploitation ou au matériel pour avoir une vision précise de la volumétrie des données, et en définissant les exigences techniques et opérationnelles de la démarche avec les responsables IT et de projet concernés, afin d'évaluer la quantité de données à acquérir, conformément à la PSSI.

Définir la stratégie de préservation des données, en considérant la volumétrie des données à analyser, le temps dont on dispose, le matériel de copie dont on dispose, et d'autres contraintes externes, et en s'assurant de la conformité aux normes légales auprès des équipes juridiques, afin de rédiger le document de traçabilité des actions effectuées.

Réaliser la collecte de données de manière technico-légale, en utilisant des outils dédiés pour l'extraction des données sur des supports comme les clés USB ou pour la création de copies technico-légales avec des outils open source (tels que dd, dcfldd) et commerciaux (comme FTK Imager), disponibles sur la distribution Kali Linux, et en assurant le respect des politiques internes, de l'éthique et des cadres légaux en lien avec les équipes de sécurité informatique, afin de préserver les preuves numériques dans un contexte d'investigation légale.

Analyser les artefacts numériques identifiés, tels que disques durs, mémoires, traces réseau, journaux d'événements, emails, navigateurs, et smartphones, en employant des techniques et des logiciels d'analyse forensique avancés, afin de tracer et documenter les preuves numériques pour les besoins d'enquêtes et de conformité légale.

Rédiger un rapport d'analyse forensique, en mettant en avant les implications légales, les recommandations de sécurité et les conclusions techniques essentielles, et en adaptant le discours aux publics techniques et institutionnels (forces de l'ordre, magistrat, équipe de réponse à incidents), et en prenant les dispositions permettant l'accès des informations à tous, y compris en cas de handicap, afin de fournir une communication claire et complète des résultats d'investigation aux parties prenantes concernées.

MODALITÉS D'ÉVALUATION

Cas d'études :

des cas d'études sont proposés aux étudiants. Ces cas sont fournis sous forme de scénarii comportant des copies de disques durs, des copies de smartphones. Il est demandé à l'étudiant de réaliser une analyse technico-légale des supports fournis à l'aide d'outils dédiés. Il est demandé une restitution écrite relatant le scénario, son analyse ainsi que la présentation synthétique des résultats.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

L'expert en cybersécurité (MS) exerce sa mission dans divers secteurs d'activités, les plus représentés sont les suivants : grands groupes industriels, secteur bancaire, entreprises publiques, administrations, PME/TPE.

Il trouve des opportunités d'emploi dans une vaste gamme d'entreprises, d'organisations et d'administrations, toutes confrontées aux défis de la sécurité informatique. Ce professionnel est susceptible d'être engagé par des Entreprises de Service Numériques (ESN) ou des prestataires spécialisés en cybersécurité, qui le déploient ensuite comme consultants au sein de diverses organisations.

TYPE D'EMPLOIS ACCESSIBLES

- Expert en Cybersécurité
- Ingénieur sécurité informatique
- Expert sécurité informatique
- Responsable sécurité des SI
- Architecte de sécurité des systèmes d'information
- Expert en sécurité des SI
- Expert sécurité, méthode et qualité informatique
- Expert en tests d'intrusion – sécurité des SI
- Auditeur en sécurité des SI
- Post auditeur en sécurité des SI
- Responsable sécurité informatique
- Ingénieur sécurité web

RÈGLEMENTATIONS D'ACTIVITÉ

Le métier d'Expert en Cybersécurité (MS) n'est pas réglementé. Cependant, dans l'exercice de ses activités, il est impératif de se conformer aux lois, obligations et normes en vigueur visant la sécurisation des systèmes d'information et la protection des données. Cela inclut des cadres juridiques nationaux et internationaux relatifs à la protection des données, à la sécurité des réseaux et des systèmes d'information.

L'application des principes régissant la sécurité numérique et la conformité repose sur des cadres réglementaires et des standards établis par les autorités compétentes.

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)	Élevée (4/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 3 à 5 sur 5.
Facteurs principaux	Lien formation-emploi, Manque de main-d'œuvre disponible
Salaire médian (mensuel)	2 704 €

Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (35 % des actifs en emploi)
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique · tension 4/5 (Élevée) M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom · tension 3/5 (Modérée) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	14 307
Jugés difficiles à recruter	46 %
Emplois saisonniers	2 %
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

Titre d'ingénieur diplômé conférant le grade de master (formations évaluées par la Commission des titres d'ingénieur, liste publiée au journal officiel)

Diplôme d'une école de management, privée ou consulaire, conférant le grade de master (formations évaluées par la CEFDG, liste publiée au bulletin officiel du MESR)

;
Diplôme de 3e cycle habilité par les autorités administratives (Diplôme national de master, DEA, DESS...) ou diplôme professionnel de niveau Bac+5 ;

Diplôme ou attestation de validation d'un niveau équivalent M1 pour des candidats ayant au moins trois années d'expérience professionnelle en lien avec la formation visée ;

Titre inscrit au Répertoire national des certifications professionnelles (RNCP) niveau 7

Diplôme étranger équivalent aux diplômes français exigés ci-dessus.

Conditions d'accès dérogatoires :

a) Dans la limite de 40 % maximum de l'effectif de la promotion suivant la formation Mastère Spécialisé concernée, sont recevables, après une procédure de Validation des acquis personnels et professionnels (VAPP), les candidatures de personnes, justifiant a minima de 5 années d'expérience professionnelle pour lesquelles les activités exercées ont un lien avéré avec les compétences professionnelles visées par la formation.

b) Par dérogation pour 30 % maximum du nombre d'apprenants suivant la formation Mastère Spécialisé concernée, sont recevables les candidatures de titulaires d'un des diplômes suivants :

- Diplôme ou attestation de validation d'un niveau équivalent M1 sans expérience professionnelle ou ayant moins de trois ans d'expérience professionnelle en lien avec la formation visée.
- Diplôme de licence (L3) ou grade de Licence ou titre inscrit au RNCP niveau 6 justifiant d'une expérience professionnelle de 3 ans minimum, en lien avec la formation visée

Le pourcentage total des dérogations prévues au a) et au b) ci-dessus ne doit pas excéder 40%.

PRÉREQUIS À LA VALIDATION

Le jury de délivrance de la certification est composé de 4 membres, dont au moins deux membres professionnels et extérieurs au dispositif de formation. Le jury est présidé par le directeur à la formation et à la pédagogie ou son représentant ou le responsable de la certification selon le jury mis en place.

Pour garantir la transparence et l'objectivité du processus d'évaluation, la décision finale du jury sera prise à la majorité relative des voix exprimées par les membres présents.

En cas d'égalité des votes, le président du jury dispose d'une voix prépondérante.

COMPOSITION DU JURY — FORMATION INITIALE, FORMATION CONTINUE, APPRENTISSAGE, CONTRAT DE PROFESSIONNALISATION, VAE

Le jury de délivrance de la certification est composé de 4 membres, dont au moins deux membres professionnels et extérieurs au dispositif de formation. Le jury est présidé par le directeur à la formation et à la pédagogie ou son représentant ou le responsable de la certification selon le jury mis en place.

Pour garantir la transparence et l'objectivité du processus d'évaluation, la décision finale du jury sera prise à la majorité relative des voix exprimées par les membres présents.

En cas d'égalité des votes, le président du jury dispose d'une voix prépondérante.

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	9 000 €
Selon la branche	7 697 € – 9 800 €
Prise en charge	Branches concernées
9 000 €	Valeur par défaut · 182 branches
9 800 €	CNPE des sociétés financières, CPNE Casinos, CPNE Personnel navigant technique des exploitants d'hélicoptères, CPNE Transport aérien : personnel au sol, CPNE Travail Temporaire
8 696 €	CPNE FP Commerce de Détail de l'Horlogerie Bijouterie, CPNEFP Commerce succursaliste de la Chaussure, CPNEFP Commerce à distance, CPNEFP Grands Magasins/ Magasins Populaires, CPNEFP Import-Export
9 276 €	CPNEF de l'Exploitation cinématographique et de la Distribution de films
9 005 €	CPNE FP Branche des magasins du Bricolage
8 974 €	CPNE de la branche de la Distribution Directe
8 813 €	CPNEFP Professions de la Photographie
8 775 €	CPNEFP de la branche des entreprises du bureau et du numérique (commerces et services)
8 711 €	CPNEFP de la Branche des Caisses régionales de Crédit Agricole et autres organismes
8 600 €	CPNEFP de l'habillement, mercerie, chaussure et jouet
8 519 €	CPNE Industrie pétrolière
8 500 €	CPNEFP de la métallurgie
7 697 €	CPNEFP de la blanchisserie, laverie, location de linge, nettoyage à sec, pressing et teinturerie

Base légale

Date de décision	23/05/2025
Durée de l'enregistrement	5 ans
Date d'échéance de l'enregistrement	23/05/2030
Date de dernière délivrance possible	23/05/2034

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2022	36	0	100 %	93 %

2021	28	0	100 %	94 %
2020	24	0	100 %	100 %

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP36072

CORRESPONDANCES (PAR BLOCS)

RNCP36072

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/40640/>

Où se former

Formations référencées	6
Organismes	1
Régions couvertes	2
Prix indicatif	4 653 € – 10 500 €
Durée	70 – 1076 h

Offre de formation — MonCompteFormation (Caisse des Dépôts), licence ouverte.

Se former en apprentissage

Formations en apprentissage	2
Organismes gestionnaires (CFA)	1
Organismes formateurs	1
Régions couvertes	2
Départements couverts	2
Organismes certifiés Qualiopi	1
Sessions	de 09/2026 à 08/2028

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

Entrées et sorties de formation

Entrées en formation	8
Parcours menés à terme	4
Taux d'achèvement	50 %
Période	09/2025 – 09/2026

Entrées et sorties — Caisse des Dépôts (open data), tous organismes confondus.

Demande CPF — formations engagées

Dossiers CPF engagés	11
Montant total engagé	80 453 €
Coût moyen par dossier	7 314 €
Durée moyenne	531 h
Période	08/2025 – 08/2026
France compétences	48 %
Reste à charge titulaire	26 %
Entreprise	20 %
OPCO	6 %

Formations engagées via le CPF — Caisse des Dépôts (open data), tous organismes confondus.