

Ingénieur diplôme de l'école nationale supérieure de Bretagne sud (ENSIBS), spécialité : Sécurité des systèmes d'information

RNCP35799 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Sigle	Titre ingénieur — Titre ingénieur
Code(s) NSF	326r, 326n, 326
Formacode(s)	24231, 31006, 31008
Code(s) ROME	M1802, M1810, M1801, M1805, M1806
Type d'enregistrement	Enregistrement de droit
Date d'échéance	31/08/2026

Certificateur(s)

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE · SIRET : 11004401300040

UNIVERSITE DE BRETAGNE SUD (UBS) - ENSIBS LORIENT · SIRET : 19561718800485

Partenaires habilités

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

Organisme	SIRET	Habilitation
CFAI DIAFOR	39048242000028	Former et organiser l'évaluation
INST TECHNI INGENIEURS INDUSTRIE BRETAGN	43878554500023	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

Les entreprises, institutions et services de l'État ont un besoin croissant de professionnels capables de comprendre la menace et les modes opératoires des attaquants dans une approche système, de construire la sécurité des infrastructures dans une approche globale (technique, organisationnelle et humaine), afin de mieux se protéger et gérer les crises cyber. Le gouvernement, via l'Agence Nationale de la Sécurité des Système d'Information (ANSSI) et les différentes Lois de Programmation Militaire (LPM), fait de la formation en sécurité des systèmes d'informations (et en particulier en Cyberdéfense) une priorité de la France.

Pour répondre à ce besoin, l'un des objectifs est de certifier des ingénieurs capables de comprendre les métiers de l'entité qu'ils protègent afin d'adapter au mieux leurs recommandations de sécurité et leur mise en œuvre.

ACTIVITÉS VISÉES

Selon les fonctions occupées, l'ingénieur diplômé de l'ENSIBS est amené à réaliser les activités suivantes

- Analyste réponse aux incidents de sécurité

L'analyste réponse aux incidents de sécurité intervient généralement au sein d'un CERT (Computer Emergency Response Team) ou CSIRT (Computer Security Incident Response Team).

En cas de soupçons sur une activité malveillante ou d'attaque au sein du système d'information, l'analyste réponse aux incidents de sécurité analyse les symptômes et réalise les analyses techniques sur le système d'information.

Il identifie le mode opératoire de l'attaquant et qualifie l'étendue de la compromission. Il fournit des recommandations de remédiation pour assurer l'assainissement et le durcissement des systèmes attaqués.

- **Analyste de la menace cybersécurité**

L'analyste de la menace cybersécurité étudie l'évolution des motivations et des modes opératoires des attaquants afin de permettre à l'organisation d'ajuster sa stratégie de cybersécurité.

A un niveau plus opérationnel et technique, il fournit aux CERT/CSIRT et aux SOC des renseignements fiables et contextualisés leur permettant d'adapter et d'améliorer leurs moyens de prévention, de détection et de réponse à incident.

- **Responsable du soc**

Le responsable du SOC (Security Operation Center) planifie et organise les opérations quotidiennes du SOC afin d'évaluer le niveau de vulnérabilité et de détecter des activités suspectes ou malveillantes. Il met en place le service de détection des incidents de sécurité. Il valide la bonne exécution des processus de supervision et de gestion des événements de sécurité et assure un reporting complet et précis des indicateurs clés. Il définit et pilote le plan d'amélioration des services du SOC.

- **Responsable du csirt**

Le responsable du CSIRT (Computer Security Incident Response Team) ou du CERT (Computer Emergency Response Team) est responsable d'une équipe de réponse aux incidents de sécurité ciblant les systèmes d'information de l'organisation. Il s'assure de la bonne exécution des investigations et de la coordination des parties prenantes lors d'un incident de sécurité. Il contribue à la préparation de l'organisation pour garantir une réponse efficace. Lors d'incidents à fort impact, le responsable du CSIRT est amené à interagir avec l'équipe de gestion de crise.

- **Gestion des incidents et des crises de sécurité**

Le gestionnaire de crise de cybersécurité intervient souvent au sein d'un CSIRT (Computer Security Incident Response Team) ou d'un CERT (Computer Emergency Response Team) externe ou interne pour grandes organisations, ou bien dans une équipe dédiée à la gestion de crise travaillant étroitement avec le CSIRT. Il analyse l'ampleur de la crise, met en place les actions nécessaires à sa résolution et coordonne les équipes pour qu'elles appliquent ses recommandations. Il conseille les directions métiers afin de résoudre les crises de cybersécurité. Il organise la capacité de l'organisation à affronter de nouvelles menaces en matière de cybersécurité.

- **Consultant en cybersécurité**

Il propose, à partir d'un diagnostic, des solutions, méthodes, outils, etc. qui répondent aux enjeux posés.

Il mobilise pour ce faire des éléments issus de son expertise et de son expérience ainsi que des outils développés en interne.

Il anticipe les évolutions du contexte de cybersécurité, apporte un retour d'expérience et une vision des pratiques du marché.

Il peut contribuer à la définition de la stratégie de cybersécurité de l'organisation et à la mise en œuvre des solutions de cybersécurité. Il apporte son expertise aussi bien sur des sujets méthodologiques que techniques.

- **Auditeur de sécurité technique**

L'auditeur de sécurité technique réalise des évaluations techniques de la sécurité d'environnements informatiques. Il identifie les vulnérabilités et propose des actions de remédiation. Il peut réaliser différents types d'audits en fonction de son périmètre d'activité (tests d'intrusion, audit de code, revue de configuration, etc.).

COMPÉTENCES ATTESTÉES

L'ingénieur diplômé en Sécurité des Systèmes d'Information (cyberdéfense) de l'ENSIBS a :

les compétences professionnelles du socle commun ingénieur ENSIBS :

- gérer et piloter des projets dans la durée en exploitant les pratiques managériales respectueuses ;
- évaluer la dimension économique dans l'ensemble de ses missions ;
- intégrer l'éthique et le développement durable dans l'ensemble de ses missions ;
- discerner le bon niveau de communication selon l'interlocuteur ;
- manager les projets, en : animant les équipes, gérant les compétences ;
- travailler en anglais en milieu professionnel ;
- travailler dans un contexte international ;
- mettre en œuvre, organiser et optimiser les activités de management opérationnel des systèmes complexes.

les compétences professionnelles du spécialiste en Sécurité des Systèmes d'Information (cyberdéfense) :- auditer les systèmes d'informations ;

- assurer la résilience des services ;

- manager le risque cyber ;
- détecter et corrélérer les incidents de sécurité ;
- réagir aux incidents de sécurité ;
- opérationnaliser la sécurité des systèmes d'information.

Blocs de compétences

RNCP35799BC01 — Mettre en œuvre le management opérationnel pour la sécurité des systèmes d'information, en contexte pluridisciplinaire et multiculturel

LISTE DE COMPÉTENCES

- Identifier les codes et les besoins de son écosystème professionnel et les prendre en compte pour la mise en place de solutions techniques ou organisationnelles (pour résoudre des problèmes techniques ou organisationnels)
- Appliquer et promouvoir la culture sécurité par des pratiques managériales respectueuses pour garantir la sécurité des biens et des personnes
- Coordonner, fédérer et faire collaborer les équipes ainsi que les parties prenantes, gérer les compétences, former les collaborateurs pour un management efficient, dans un contexte pluridisciplinaire et multiculturel
- Communiquer en mobilisant le bon registre de communication selon l'interlocuteur pour atteindre ses objectifs
- Être capable d'être critique, de remettre en cause ses décisions et d'anticiper pour assurer l'agilité de l'organisation
- Adapter sa pratique pour répondre aux enjeux et besoins de la société, en intégrant le développement durable et l'éthique dans ses actions

MODALITÉS D'ÉVALUATION

Modalités d'évaluation et de certification : Travaux individuels et en groupes, mises en situation, comprenant une production écrite ou orale et validant les points ci-dessous.

- Les parties prenantes de l'organisation sont identifiées de même que leurs interactions
- les méthodes et outils utilisés sont pertinents au regard des objectifs et leur choix est justifié
- la solution est dimensionnée au contexte, sa mise en œuvre intègre le facteur humain et prévoit des rétroactions
- la production orale ou écrite, en français ou en anglais est d'un niveau professionnel, du bon registre de langage et compréhensible par le récepteur ; elle comprend une synthèse réflexive
- L'élève connaît les points clés de sa personnalité et ceux du groupe
- Il sait exprimer ses attentes et les faire partager à l'équipe
- Il sait écouter et tenir compte des attentes des collaborateurs et interlocuteurs
- Il fait preuve de leadership et d'anticipation

RNCP35799BC02 — Conduire des projets complexes en matière de cybersécurité, de manière agile

LISTE DE COMPÉTENCES

- Piloter des projets : de l'analyse du besoin à sa recette, en passant par la rédaction du cahier des charges, l'allocation des ressources, la planification, et le retour d'expérience, contribuant ainsi à la réalisation de la stratégie de l'entreprise.
- Intégrer systématiquement la dimension économique dans l'ensemble de ses missions
- Assurer la communication, à tous les niveaux de l'organisation, y compris institutionnelle, en français et en anglais pour être compris sans ambiguïté.
- Identifier la démarche entrepreneurial

MODALITÉS D'ÉVALUATION

Modalités d'évaluation et de certification :

Mises en situation et réalisation de projets en groupe avec production effective, restitutions écrites et orales où sont évalués les items ci-dessous.

- Les caractéristiques du projet sont identifiées, analysées et reformulées dans un document cadre : enjeux, objectifs, périmètre, acteurs, livrables, validation des livrables (coût, délai, qualité), risque.
- Des indicateurs sont mis en place pour le suivi du projet ; ils sont analysés régulièrement et le rendu fait état des actions correctrices menées.
- Les livrables sont comparés aux attendus et sont conformes
- Un plan de communication entre les acteurs du projet est établi, suivi, évalué
- La production écrite, orale, est conforme aux attendus

L'élève a participé au moins à une manifestation ou un challenge sur l'entrepreneuriat

RNCP35799BC03 — Réaliser des audits de sécurité des systèmes d'informations

LISTE DE COMPÉTENCES

- Intégrer des champs disciplinaires variés comme réponse aux besoins de la société (géostratégie et la gouvernance) pour auditer des systèmes d'informations
- Intégrer les dimensions juridiques, éthiques et la conformité pour auditer des systèmes d'informations
- Prendre en compte les systèmes complexes numériques des entreprises (internet des objets, cloud...) pour auditer des systèmes d'informations
- Concevoir des solutions techniques innovantes pour auditer des systèmes d'informations
- Trouver, évaluer et exploiter des informations pertinentes pour auditer des systèmes d'informations
- Auditer des systèmes d'informations à l'aide des méthodes et outils de l'ingénieur (identification, modélisation, analyse, synthèse...)
- Auditer des systèmes d'informations à l'aide d'une large culture IT
- Communiquer et négocier, à l'oral et à l'écrit y compris en anglais et dans un contexte international
- Adapter sa communication en fonction du contexte socio-culturel et du niveau de compétences techniques de ses interlocuteurs

MODALITÉS D'ÉVALUATION

Modalités d'évaluation et de certification :

La validation des acquis d'apprentissage et compétences est établie par une combinaison des modalités suivantes :

- mises en situations, analyse d'articles, études de cas, examens sur table et questionnaires de vérification du savoir, travaux de groupe ;
- évaluation des rapports séquences en entreprise : présentation des projets conduits en entreprise et évaluation par le maître d'apprentissage des savoir-faire et savoir être tout au long de la formation ;
- rédaction et soutenance d'un projet de fin d'études.

RNCP35799BC04 — Opérationnaliser la sécurité des systèmes d'informations

LISTE DE COMPÉTENCES

- Intégrer des champs disciplinaires variés comme réponse aux besoins de la société (géostratégie et la gouvernance) pour opérationnaliser la sécurité des systèmes d'informations
- Intégrer les dimensions juridiques, éthiques et la conformité pour opérationnaliser la sécurité des systèmes d'informations
- Prendre en compte les systèmes complexes numériques des entreprises (internet des objets, cloud...) pour opérationnaliser la sécurité des systèmes d'informations
- Concevoir des solutions techniques innovantes pour opérationnaliser la sécurité des systèmes d'informations
- Trouver, évaluer et exploiter des informations pertinentes pour opérationnaliser la sécurité des systèmes d'informations
- Opérationnaliser la sécurité des systèmes d'informations à l'aide des méthodes et outils de l'ingénieur (identification, modélisation, analyse, synthèse...)
- Opérationnaliser la sécurité des systèmes d'informations à l'aide d'une large culture IT
- Communiquer et négocier, à l'oral et à l'écrit y compris en anglais et dans un contexte international
- Adapter sa communication en fonction du contexte socio-culturel et du niveau de compétences techniques de ses interlocuteurs

MODALITÉS D'ÉVALUATION

Modalités d'évaluation et de certification :

La validation des acquis d'apprentissage et compétences est établie par une combinaison des modalités suivantes :

- mises en situations, analyse d'articles, études de cas, examens sur table et questionnaires de vérification du savoir, travaux de groupe ;
- évaluation des rapports séquences en entreprise : présentation des projets conduits en entreprise et évaluation par le maître d'apprentissage des savoir-faire et savoir être tout au long de la formation ;
- rédaction et soutenance d'un projet de fin d'études.

RNCP35799BC05 — Assurer la résilience des services numériques vitaux des entreprises

LISTE DE COMPÉTENCES

- Intégrer des champs disciplinaires variés comme réponse aux besoins de la société (géostratégie et la gouvernance) pour assurer la résilience des services vitaux des entreprises - Intégrer les dimensions juridiques, éthiques et la conformité pour assurer la résilience des services
 - Contribuer à la responsabilité sociétale de l'entreprise pour assurer la résilience des services vitaux des entreprises
 - Trouver, évaluer et exploiter des informations pertinentes pour assurer la résilience des services vitaux des entreprises
 - Assurer la résilience des services vitaux des entreprises à l'aide des méthodes et outils de l'ingénieur (identification, modélisation, analyse, synthèse...)
- et être capable de produire des documents et modes d'emplois en interagissant avec les interlocuteurs
- Communiquer et négocier, à l'oral et à l'écrit y compris en anglais et dans un contexte international
 - Adapter sa communication en fonction du contexte socio-culturel et du niveau de compétences techniques de ses interlocuteurs

MODALITÉS D'ÉVALUATION

Modalités d'évaluation et de certification :

La validation des acquis d'apprentissage et compétences est établie par une combinaison des modalités suivantes :

- mises en situations, analyse d'articles, études de cas, examens sur table et questionnaires de vérification du savoir, travaux de groupe ;
- évaluation des rapports séquences en entreprise : présentation des projets conduits en entreprise et évaluation par le maître d'apprentissage des savoir-faire et savoir être tout au long de la formation ;
- rédaction et soutenance d'un projet de fin d'études.

RNCP35799BC06 — Manager le risque lié à des menaces numériques

LISTE DE COMPÉTENCES

- Intégrer des champs disciplinaires variés comme réponse aux besoins de la société (géostratégie et la gouvernance) pour manager le risque lié à des menaces
- Intégrer les dimensions juridiques, éthiques et la conformité pour manager le risque lié à des menaces numériques
- Contribuer à la responsabilité sociétale de l'entreprise pour manager le risque lié à des menaces numériques
- Trouver, évaluer et exploiter des informations pertinentes pour manager le risque lié à des menaces numériques
- Manager le risque lié à des menaces numériques à l'aide des méthodes et outils de l'ingénieur (identification, modélisation, analyse, synthèse...)
- Communiquer et négocier, à l'oral et à l'écrit y compris en anglais et dans un contexte international
- Adapter sa communication en fonction du contexte socio-culturel et du niveau de compétences techniques de ses interlocuteurs

MODALITÉS D'ÉVALUATION

Modalités d'évaluation et de certification : La validation des acquis d'apprentissage et compétences est établie par une combinaison des modalités suivantes :

- mises en situations, analyse d'articles, études de cas, examens sur table et questionnaires de vérification du savoir, travaux de groupe ;
- évaluation des rapports séquences en entreprise : présentation des projets conduits en entreprise et évaluation par le maître d'apprentissage des savoir-faire et savoir être tout au long de la formation ;
- rédaction et soutenance d'un projet de fin d'études.

RNCP35799BC07 — Détecter et corréler les incidents de sécurité numérique

LISTE DE COMPÉTENCES

- Trouver, évaluer et exploiter des informations pertinentes pour détecter et corréler les incidents de sécurité numérique
- Intégrer les dimensions juridiques, éthiques et la conformité pour détecter et corréler les incidents de sécurité numérique
- Détecter et corréler les incidents de sécurité numérique à l'aide des méthodes et outils de l'ingénieur (identification, modélisation, analyse, synthèse...)
- Prendre en compte les systèmes complexes numériques des entreprises (internet des objets, cloud...) pour détecter et corréler les incidents de sécurité numérique

- Concevoir des solutions techniques innovantes pour détecter et corrélérer les incidents de sécurité numérique
- Communiquer et négocier, à l'oral et à l'écrit y compris en anglais et dans un contexte international
- Adapter sa communication en fonction du contexte socio-culturel et du niveau de compétences techniques de ses interlocuteurs

MODALITÉS D'ÉVALUATION

Modalités d'évaluation et de certification :

La validation des acquis d'apprentissage et compétences est établie par une combinaison des modalités suivantes :

- mises en situations, analyse d'articles, études de cas, examens sur table et questionnaires de vérification du savoir, travaux de groupe ;
- évaluation des rapports séquences en entreprise : présentation des projets conduits en entreprise et évaluation par le maître d'apprentissage des savoir-faire et savoir être tout au long de la formation ;
- rédaction et soutenance d'un projet de fin d'études.

RNCP35799BC08 — Réagir aux incidents de sécurité numérique

LISTE DE COMPÉTENCES

- Trouver, évaluer et exploiter des informations pertinentes pour réagir aux incidents de sécurité numérique
- Intégrer les dimensions juridiques, éthiques et la conformité pour réagir aux incidents de sécurité numérique - Réagir aux incidents de sécurité numérique à l'aide des méthodes et outils de l'ingénieur (identification, modélisation, analyse, synthèse...)
- Prendre en compte les systèmes complexes numériques des entreprises (internet des objets, cloud...) pour réagir aux incidents de sécurité numérique
- Concevoir des solutions techniques innovantes pour réagir aux incidents de sécurité numérique
- Communiquer et négocier, à l'oral et à l'écrit y compris en anglais et dans un contexte international
- Adapter sa communication en fonction du contexte socio-culturel et du niveau de compétences techniques de ses interlocuteurs

MODALITÉS D'ÉVALUATION

Modalités d'évaluation et de certification :

La validation des acquis d'apprentissage et compétences est établie par une combinaison des modalités suivantes :

- mises en situations, analyse d'articles, études de cas, examens sur table et questionnaires de vérification du savoir, travaux de groupe ;
- évaluation des rapports séquences en entreprise : présentation des projets conduits en entreprise et évaluation par le maître d'apprentissage des savoir-faire et savoir être tout au long de la formation ;
- rédaction et soutenance d'un projet de fin d'études.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Sécurité des Systèmes d'Information(cyberdéfense) : Programmation, conseil et autres activités informatiques ; Fabrication de produits informatiques, électroniques et optiques ; Activités d'architecture et d'ingénierie ; activités de contrôle et analyses techniques ; Administration publique et défense ; sécurité sociale obligatoire ; Fabrication d'autres matériels de transport ; Réparation et installation de machines et d'équipements ; Production et distribution d'électricité, de gaz, de vapeur et d'air conditionné ; Transports aériens ; Télécommunications ; Services d'information ; Activités des services financiers, hors assurance et caisses de retraite ; Activités juridiques et comptables.

TYPE D'EMPLOIS ACCESSIBLES

Son large spectre de compétences techniques, scientifiques et managériales lui permet d'exercer les métiers suivants (Référentiel ANSSI 2018) :

- Analyste de la menace
- Responsable de la Sécurité des Systèmes d'Information (RSSI)
- Spécialiste en gestion de crise cyber
- Chef de projet sécurité
- Architecte sécurité
- Intégrateur de sécurité
- Expert réponse à incident
- Consultant sécurité « organisationnel »

- Consultant sécurité « technique »
- Évaluateur sécurité
- Analyste SOC

RÈGLEMENTATIONS D'ACTIVITÉ
Aucune référence juridique des règlementations d'activité

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	Manque de main-d'œuvre disponible, Lien formation-emploi
Salaire médian (mensuel)	2 781 €
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) M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique · tension 4/5 (Élevée) M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom · tension 5/5 (Très 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)	41 765
Jugés difficiles à recruter	50 %
Emplois saisonniers	2 %
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom 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

MODALITÉS D'ACCÈS
Formation continue, Apprentissage, Contrat de professionnalisation, Candidature individuelle, VAE

COMPOSITION DU JURY — FORMATION CONTINUE, APPRENTISSAGE, CONTRAT DE PROFESSIONNALISATION, CANDIDATURE INDIVIDUELLE
L'organisation des jurys est placée sous la responsabilité de son président désigné par le président de l'Université de Bretagne Sud.
Le jury est composé du directeur de l'école, des directeurs adjoints, des responsables de spécialités, d'au moins 1 professionnel du monde de l'entreprise. Il est complété de 2 à 3 enseignants responsables des certifications, mobilités et stages. Les directeurs de CFA sont invités au jury de diplôme pour les apprentis qui les concernent.

COMPOSITION DU JURY — VAE

Composition du jury VAE définie par le Code de l'éducation : article L613-3 modifié par la loi n°2015-366 du 31 mars 2015.

ACCESSIBLE EN OUTRE-MER

Polynésie française

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	9 160 €
Selon la branche	8 100 € – 9 200 €
Prise en charge	Branches concernées
9 160 €	Valeur par défaut · 198 branches
9 200 €	CPNE de l'exploitation des équipements thermiques et de génie climatique, CPNE de l'ingénierie, des services informatiques et du conseil, CPNE des Télécoms, CPNEFP dans les établissements d'enseignement privés sous contrat, CPNEFP de la Branche des Caisses régionales de Crédit Agricole et autres organismes
9 000 €	CPNE chimie, CPNEFP des industries électriques et gazières
8 668 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager, CPNEFP du Négoce de l'ameublement
8 924 €	CPNE des industries de santé (CPNEIS)
8 583 €	CPNEFP Commerce à distance
8 500 €	CPNEFP de la métallurgie
8 100 €	CPNE Banque

Base légale

Date d'échéance de l'enregistrement	31/08/2026
--	------------

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2018	27	0	92 %	100 %
2017	25	0	89 %	100 %
2016	28	0	1 %	1 %

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP16311

NOUVELLE(S) CERTIFICATION(S)

RNCP42905

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/35799/>

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
Sessions	de 09/2025 à 08/2029

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