

Ingénieur de l'Ecole Nationale Supérieure de Bretagne Sud (ENSIBS), spécialité Informatique et Cybersécurité

RNCP37726 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Sigle	Titre ingénieur — Titre ingénieur
Code(s) NSF	326, 326m, 326t
Formacode(s)	31006, 31096, 31024, 31028, 32062
Code(s) ROME	M1806, M1802, M1805, M1803
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

La filière de la confiance numérique regroupe la sécurité numérique et la cybersécurité. Elle réunit plus de 2000 entreprises en France et compte près de 70.000 emplois. L'alliance pour la confiance numérique (ACN) regroupe les entreprises de l'informatique autour de la cybersécurité, qui correspond à la sécurisation « interne » des systèmes numériques. La cybersécurité se concentre sur deux types d'activités souvent associées dans la pratique, les services (conseil, conception, mise en place, exploitation, formation) et les logiciels et solutions, destinés aux marchés professionnels (État et secteur public, installations critiques, entreprises, PME) et grand public (ordinateurs, smartphones, maison, véhicules et objets connectés, etc). Selon un rapport réalisé en 2021, en collaboration entre l'APEC et le Pôle d'excellence cyber (PEC), 7 000 offres d'emploi cadre ont été publiées sur apec.fr dans le champ de la cybersécurité. 46 % des profils recherchés par les entreprises sont des spécialistes de la conception d'architectures sécurisées, du développement de solutions sécurisées et de l'administration des systèmes d'information. Il est noté que, non seulement ces profils sont difficiles à recruter, mais qu'à l'avenir, les besoins et les tensions vont s'accroître. Leur conclusion était : Former aux risques cyber reste une des priorités.

L'ingénieur diplômé de l'ENSIBS en informatique et cybersécurité développe des compétences générales en informatique, mais également dans le domaine de la cybersécurité. Il intervient dans la conception, le développement, la mise en production et la maintenance d'applications et systèmes logiciels sécurisés par conception. Il sait prendre en compte les contraintes fonctionnelles, d'architectures et de cybersécurité tout au long

du cycle de vie d'un système. Il évolue dans les domaines de l'information et la communication, de l'industrie et des administrations publiques, de l'aéronautique, de la défense, de l'énergie, des services financiers, des télécommunications et des transports. Il dispose de solides bases fondamentales (architecture des systèmes, programmation, analyses des données, sécurité et qualification), et maîtrise les nouvelles technologies numériques (intelligence artificielle, vérification formelle, analyse par preuve, architectures de service). L'ingénieur diplômé de l'ENSIBS en informatique et cybersécurité intervient dans le secteur des produits de cybersécurité (gouvernance cyber, gestion des identités et accès, sécurité des données, sécurité des applications, sécurité des produits et équipements), également dans le secteur des services de cybersécurité (audit et conseil, mise en oeuvre de la cybersécurité, infogérance et exploitation).

ACTIVITÉS VISÉES

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

Concevoir l'architecture de sécurité : il s'assure que les choix techniques et technologiques des projets et métiers respectent les exigences de sécurité de l'organisation. Il constitue l'autorité technique sur les architectures de sécurité, définit les modèles de sécurité et accompagne le développement des architectures de sécurité au sein du SI, en cohérence avec la stratégie IT et les politiques de sécurité de l'organisation.

Assurer un développement orienté sécurité : il intervient en appui des équipes de développement afin d'accompagner les développeurs dans la prise en compte des exigences de sécurité. Il teste la sécurité des développements et suit la correction des vulnérabilités identifiées.

Développer des solutions de sécurité : le développeur de solutions de sécurité intervient au sein de sociétés d'éditions de produits informatiques. Il assure les spécifications et la conception de solutions et de produits de sécurité adaptés au contexte des menaces de cybersécurité.

Intégrer des solutions de sécurité : il contribue au choix de l'architecture de la solution de sécurité et en assure l'assemblage au sein du SI. Il intègre dans l'environnement de production la solution de sécurité et en assure le déploiement. Il peut également assurer l'exploitation et le maintien en conditions opérationnelles dans la durée à travers la fourniture d'un service de sécurité managé.

Réaliser des recherches en sécurité des systèmes d'information : il se consacre à l'expérimentation et au progrès de sa discipline. Il met en oeuvre, aux frontières de plusieurs champs scientifiques constitués, ses acquis techniques et académiques au service d'une problématique de sécurité au plus haut niveau scientifique. Il mobilise des connaissances expertes pour contribuer à l'émergence de technologies novatrices et de savoirs inédits. Il participe au développement de produits, de procédés ou de services innovants.

COMPÉTENCES ATTESTÉES

L'ingénieur diplômé en informatique et cybersécurité de l'ENSIBS a la spécificité :

- d'intégrer la propriété de sécurité tout au long du cycle de vie d'un logiciel ;
- de modéliser et architecturer les systèmes afin de maîtriser leur complexité ;
- d'appliquer les méthodes de l'approche agile à tous les niveaux de ses projets ;
- de sécuriser les données utilisées par les systèmes qu'elle, ou il, produit ;
- d'exploiter les données du système à des fins de sécurité ;
- d'expertiser et de qualifier des systèmes sur le plan de la sécurité ;
- de conduire des projets de dimension internationale ;
- de communiquer et de convaincre sur le bienfondé des solutions proposées.

Il a également 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 oeuvre, organiser et optimiser les activités de management opérationnel des systèmes complexes.

Blocs de compétences

RNCP37726BC01 — Mettre en oeuvre le management opérationnel pour le développement de produits et de services en cybersécurité, 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
Critiquer, remettre en cause ses décisions et 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

Travaux individuels et en groupes, mises en situation, comprenant une production écrite ou orale

RNCP37726BC02 — Conduire agilement des projets complexes en développement de produits de cybersécurité

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

Mises en situation et réalisation de projets en groupe avec production effective, restitutions écrites et orales

RNCP37726BC03 — Développer l'innovation et une démarche de recherche pour les applications informatiques

LISTE DE COMPÉTENCES

Réaliser des études bibliographiques
Construire des expérimentations respectant les règles de l'art
Connaître les différentes approches de validations de solutions de cybersécurité innovantes
Connaître les principes et les méthodes de la veille technologique dans le domaine de la cybersécurité
Connaître les outils qui permettent de préserver la propriété intellectuelle
Connaître et promouvoir les techniques nouvelles (innovation, vulgarisation, information, formation) dans le domaine de la cybersécurité
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, principalement en cybersécurité, de ses interlocuteurs

MODALITÉS D'ÉVALUATION

Évaluation par projet, mise en situation réelle ou simulée, exposé oral et rédaction de compte rendu.
Travail en petits groupes sur des sujets de cybersécurité fournis par les entreprises partenaires et encadrés par elles.

RNCP37726BC04 — Assurer la sécurité des entreprises à travers leurs systèmes et leurs données

LISTE DE COMPÉTENCES

Discerner les différents concepts de la sécurité logicielle
Respecter les normes de gouvernance des systèmes d'information et de communication
Appliquer et maîtriser le maintien en condition opérationnelle et le soutien logistique intégré
Appliquer et maîtriser les méthodes statistiques pour la sécurité des données
Exploiter les techniques de classification et d'analyse cybersécurité à partir d'un modèle de données
Exploiter les techniques de projection et de prédiction de vulnérabilités ou de risques à partir d'un modèle de données

Appliquer et maîtriser l'ingénierie des tests (fonctionnels et de sécurité)

Connaître les principes et outils de scan de vulnérabilités logicielles

Appliquer et maîtriser l'ingénierie de la qualification cybersécurité

MODALITÉS D'ÉVALUATION

Évaluation des séquences académique

Mises en situation encadrées individuelles et/ou en binôme : de conception, test et développement de programmes sur différents supports, d'analyse d'articles scientifiques ou techniques.

Projets en groupe, dont le projet d'assimilation, éventuellement avec des étudiants issus d'autres filières et d'autres disciplines, sur des scénarios interactifs imposés ou à proposer, avec restitution écrite et orale par les différents membres du groupe de cahiers des charges et systèmes numériques.

Études de cas et questionnaires de vérification du savoir et du savoir-faire en matière de programmation, paradigmes informatiques, bases de données, réseaux, architecture et architecture logicielle, web.

Évaluation des séquences entreprises

Rapports présentant des projets menés en entreprise, écrits par l'élève tout au long du parcours de formation.

Évaluation du savoir-faire et du savoir-être de l'élève par le maître d'apprentissage tout long de la formation.

RNCP37726BC05 — Modéliser et construire des systèmes informatiques et leurs données

LISTE DE COMPÉTENCES

Connaître et savoir appliquer les mathématiques et la statistique de base pour les besoins de la cybersécurité

Comprendre les interfaces numériques liées à l'utilisation conjointe de l'informatique avec l'électronique, l'automatique et la mécanique

Comprendre et utiliser le matériel, les systèmes d'exploitation et les réseaux ainsi que les techniques de virtualisation

Être capable d'utiliser les différents langages de modélisation, d'analyse et de programmation des systèmes

Exploiter l'urbanisation et l'architecture des systèmes à logiciel prépondérant

Gérer des systèmes d'informations et des données

Appliquer et maîtriser l'ingénierie (méthodes, outils, normes, procédures, modélisation) des besoins et des exigences (cahier des charges)

Appliquer et maîtriser l'ingénierie de l'intégration et de l'interopérabilité

Appliquer et maîtriser l'ingénierie du déploiement

Appliquer et maîtriser les fondements mathématiques du chiffrement

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

Évaluation des séquences académique

Mises en situation encadrées individuelles et/ou en binôme : de conception, test et développement de programmes sur différents supports, d'analyse d'articles scientifiques ou techniques.

Projets en groupe, dont le projet d'assimilation, éventuellement avec des étudiants issus d'autres filières et d'autres disciplines, sur des scénarios interactifs imposés ou à proposer, avec restitution écrite et orale par les différents membres du groupe de cahiers des charges et systèmes numériques.

Études de cas et questionnaires de vérification du savoir et du savoir-faire en matière de programmation, paradigmes informatiques, bases de données, réseaux, architecture et architecture logicielle, web.

Évaluation des séquences entreprises

Rapports présentant des projets menés en entreprise, écrits par l'élève tout au long du parcours de formation.

Évaluation du savoir-faire et du savoir-être de l'élève par le maître d'apprentissage tout long de la formation.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Le large spectre de compétences techniques, scientifiques et managériales de l'ingénieur, en Informatique et cybersécurité, lui permet d'exercer les activités suivantes :

- Informatique et Cybersécurité
- Programmation, conseil et autres activités informatiques ;
- Activités des services financiers, hors assurance et caisses de retraite ;

- Activités d'architecture et d'ingénierie ;
- Activités de contrôle et analyses techniques ;
- Activités de location et location-bail ; Administration publique et défense ; sécurité sociale obligatoire.

TYPE D'EMPLOIS ACCESSIBLES

Le large spectre de compétences techniques, scientifiques et managériales de l'ingénieur, en Informatique et cybersécurité, lui permet d'exercer les métiers suivants :

- Ingénieur d'étude et de développement
- Ingénieur intégrateur de systèmes sécurisés
- Ingénieur qualités (sécurité) – méthodes informatiques et Cybersécurité
- Consultant en ingénierie informatique et Cybersécurité
- Architecte système sécurisé
- Chef de projets système
- Directeur de systèmes d'informations et de communication
- Responsable de la Sécurité des Systèmes d'Information

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)	2 892 €
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) M2X91 — Chefs de projet et directeurs de service informatique · tension 4/5 (Élevée) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	42 073
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 M2X91 — Chefs de projet et directeurs de service informatique M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

MODALITÉS D'ACCÈS

Formation initiale, Formation continue, Apprentissage, Contrat de professionnalisation, Candidature individuelle, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

Niveau 5 scientifique ou technique

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

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.

COMPOSITION DU JURY — APPRENTISSAGE

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. Le directeur du CFA est invité au jury de diplôme.

COMPOSITION DU JURY — 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.

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.

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	8 100 €
Selon la branche	8 089 € – 8 324 €
Prise en charge	Branches concernées
8 100 €	Valeur par défaut · 202 branches
8 324 €	CPNE de l'ingénierie, des services informatiques et du conseil, CPNEF de l'audiovisuel, CPNEFP dans les établissements d'enseignement privés sous contrat
8 274 €	CPNE des Télécoms, CPNE des industries de santé (CPNEIS), CPNEFP ICGV entreprises de la viande
8 155 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager, CPNEFP du Négoce de l'ameublement
8 089 €	CPNE Branche Caoutchouc, CPNEFP de la métallurgie
8 122 €	CPNEFP Commerce à distance

Base légale

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

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP35796

NOUVELLE(S) CERTIFICATION(S)
RNCP42398

Pour plus d'informations

LIEN VERS LE DESCRIPTIF
<https://www-ensibs.univ-ubs.fr>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/37726/>