

Ingénieur diplômé de l'École nationale supérieure d'ingénieurs de Bretagne Sud de l'université de Bretagne-Sud, spécialité Informatique et cybersécurité

RNCP42398 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Sigle	Titre ingénieur — Titre ingénieur
Code(s) NSF	110, 310, 326
Formacode(s)	31006, 31096, 31024, 32062, 31028
Code(s) ROME	M1802, M1805, M1806, M1803
Type d'enregistrement	Enregistrement de droit
Date d'échéance	31/08/2027

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.

Ainsi, la certification proposée par la formation d'ingénieur ENSIBS dans la spécialité Informatique et cybersécurité, qui comporte deux parcours, vient répondre parfaitement à ces besoins prioritaires de deux manières : former des spécialistes capables de concevoir des systèmes informatiques sécurisés par conception (parcours Cybersécurité du logiciel) et des spécialistes capables de sécuriser les données critiques des systèmes et exploiter les masses de

données, souvent disponibles sur la toile, pour anticiper les potentielles attaques.

ACTIVITÉS VISÉES

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

Activité 1 : 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.

Activité 2 : 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.

Activité 3 : 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.

Activité 4 : 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.

Activité 5 : Piloter des projets

Il assure la formation des utilisateurs et celle des collaborateurs, ainsi que le développement de ces derniers. Il coordonne des équipes pluridisciplinaires dans le cadre de projets de conception ou d'évolution de systèmes d'information sécurisés.

Il supervise l'intégration des sous-systèmes en veillant à la compatibilité technique et aux exigences de sécurité. Pour cela, il utilise des outils collaboratifs et adopte une approche agile pour améliorer la réactivité et l'innovation.

Activité 6 : Communiquer

Il communique efficacement, avec les parties prenantes, sur les résultats techniques, la prise en compte des contraintes économiques et réglementaires. Il montre l'adéquation de la conduite des projets avec les exigences environnementales et sociétales.

Activité 7 : Réaliser des recherches en sécurité des systèmes d'information

Il se consacre à l'expérimentation et au progrès de sa discipline. Il met en œuvre, 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 a, d'abord, les compétences professionnelles du socle commun ingénieur ENSIBS :

- s'insérer dans la vie professionnelle, s'intégrer dans une organisation, l'animer et la faire évoluer : exercice de la responsabilité, engagement et leadership, gestion de projets, travailler en collaboration et communiquer au sein d'équipes diversifiées et pluridisciplinaires ;
- gérer et piloter des projets informatiques et de cybersécurité dans la durée en exploitant les pratiques managériales respectueuses ;
- prendre en compte les enjeux de l'entreprise et à rendre compte de son action : dimension économique, respect des exigences sociales et environnementales, respect de la qualité, compétitivité et productivité, exigences commerciales et intelligence économique ;
- intégrer dans ses conduites les responsabilités éthiques et professionnelles, prendre en compte les enjeux des relations au travail, de sécurité et de santé au travail et de diversité ;
- accompagner les transitions, notamment numériques, énergétiques et environnementales, en intégrant les impératifs écologiques et climatiques ;
- discerner le bon niveau de communication selon l'interlocuteur ;
- travailler en contexte international et multiculturel : maîtriser une ou plusieurs langues étrangères et ouverture culturelle associée, s'adapter aux contextes internationaux et de coopération sur des enjeux planétaires collectifs ;
- entreprendre et innover, dans le cadre de projets personnels en informatique et en cybersécurité, ou par l'initiative

et l'implication au sein de l'entreprise dans des projets entrepreneuriaux.

Puis, des compétences qui lui sont spécifiques lui permettant :

- 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 bien-fondé des solutions proposées.

Blocs de compétences

RNCP42398BC01 — Mettre en œuvre 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 et cybersécurité 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 et où la cybersécurité est une exigence majeure
- 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
- Maîtriser les fondamentaux scientifiques et technologiques en informatique et cybersécurité.

MODALITÉS D'ÉVALUATION

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.

RNCP42398BC02 — Conduire des projets en développement de produits de cybersécurité

LISTE DE COMPÉTENCES

- Piloter des projets complexes en appliquant les approches agiles : 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 entrepreneuriale
- Maîtriser les fondamentaux scientifiques et technologiques en informatique et cybersécurité.

MODALITÉS D'ÉVALUATION

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.

RNCP42398BC03 — 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 validation de solutions innovantes
- Connaître les principes et les méthodes de la veille technologique
- Connaître les outils qui permettent de préserver la propriété intellectuelle
- Connaître et promouvoir les techniques nouvelles (innovation, vulgarisation, information, formation)
- 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 socioculturel et du niveau de compétences techniques de ses interlocuteurs
- Maîtriser les fondamentaux scientifiques et technologiques en informatique et cybersécurité.

MODALITÉS D'ÉVALUATION

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

RNCP42398BC04 — Assurer la sécurité informatique des entreprises pour 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
- Exploiter les techniques de classification et d'analyse à partir d'un modèle de données
- Exploiter les techniques de projection et de prédiction 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.

MODALITÉS D'ÉVALUATION

Évaluation des séquences académiques :

- 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 en entreprise :

- 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.

RNCP42398BC05 — Modéliser et construire des systèmes informatiques et leurs données

LISTE DE COMPÉTENCES

- Connaître et savoir appliquer les mathématiques et la statistique de base
- 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.

MODALITÉS D'ÉVALUATION

Évaluation des séquences académiques :

- 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 en entreprise :

- 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, majoritairement, dans les secteurs d'activité suivants :

- Sociétés de logiciels et services numériques
- Sociétés de programmation, conseil et autres activités informatiques
- Sociétés d'enquêtes et sécurité
- Enseignement public et privé
- Organismes de recherche et développement scientifique
- Administration publique et défense
- Industrie
- Banques.

TYPE D'EMPLOIS ACCESSIBLES

Les principaux types de postes accessibles pour un ingénieur en Informatique et cybersécurité sont :

- 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, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

Le parcours certifiant est en cinq ans.

Être titulaire d'une certification de niveau 5 ou 6 dans les domaines scientifiques et techniques liés à l'informatique et aux mathématiques pour une entrée en année 3 du parcours certifiant.

Être titulaire d'un diplôme de niveau 4 pour une entrée en année 1 du parcours certifiant.

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, qui le préside, ainsi que 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, qui le préside, ainsi que 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 : Le jury est composé du directeur de l'école, qui le préside, ainsi que de 2 enseignants-chercheurs et d'1 professionnel qualifié au titre de la certification visée.

Base légale

Date d'échéance de l'enregistrement 31/08/2027

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2025	34	—	82 %	100 %
2024	30	—	84 %	94 %
2023	35	—	100 %	100 %
2022	36	—	93 %	100 %
2021	33	—	92 %	100 %

Liens avec d'autres certifications

ANCIENNES VERSIONS
RNCP37726

Pour plus d'informations

LIEN VERS LE DESCRIPTIF
www.ensibs.fr
www.univ-ubs.fr

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/42398/>

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).