

Ingénieur diplômé de l'École nationale supérieure d'ingénieurs de Bretagne Sud de l'université de Bretagne-Sud, Sécurité des systèmes d'information et cybersécurité

RNCP42905 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Sigle	Titre ingénieur — Titre ingénieur
Code(s) NSF	326, 326m, 326n
Formacode(s)	31045, 31008, 24231, 32062, 15099
Code(s) ROME	M1802, M1804, M1806, M1810
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

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 Systèmes d'Information (ANSSI) et les différentes Lois de Programmation Militaire (LPM), fait de la formation en sécurité des systèmes d'information et cybersécurité (en particulier en cyberdéfense) une priorité de la France.

Pour répondre à ces besoins, les objectifs de la certification proposée par l'ENSIBS en sécurité des systèmes d'information et cybersécurité sont tout d'abord de permettre aux certifiés de comprendre les métiers de l'entité dont ils protègent les systèmes informatiques afin ensuite d'élaborer et mettre en œuvre des recommandations et solutions de cybersécurité adaptées. Pour cela, les différents pans suivants de la formation sont abordés : les activités liées à la sécurité des systèmes d'information et à la cybersécurité, telles que décrites dans le chapitre suivant.

ACTIVITÉS VISÉES

L'Ingénieur en sécurité des systèmes d'information et cybersécurité :

- Contribue à la conception et au maintien en conditions de sécurité des infrastructures informatiques (IT/Information Technology et OT/Operational Technology) des entités des domaines public comme privé, en particulier ceux qui délivrent un service réputé essentiel à la société et à l'économie
- Supervise ces infrastructures et contribue directement à leur défense face aux multiples menaces auxquelles elles font face
- Contribue, voire conduit la gouvernance en la matière, participe, voire conduit les audits techniques et organisationnels
- Conduit les analyses de risques et – au titre des responsabilités liées à la conformité - il s'assure du respect des normes (ex : ISO 27001) et des directives nationales et européennes (ex : NIS 2)
- Contribue à la formation du personnel en matière de sécurité des systèmes d'information et cybersécurité, et assume des responsabilités de consultant en la matière
- Conçoit et contribue à mettre en œuvre des plans de reprise et de continuité d'activité (PRA-PCA)
- Dirige l'équipe qui conduit des projets et accompagne les changements organisationnels
- Communique en interne et en externe dans un contexte multiculturel et international.

COMPÉTENCES ATTESTÉES

Piloter la stratégie de cyberdéfense :

- Recueillir, traiter et analyser l'information sur les risques métiers (menaces et vulnérabilités), en conformité avec les normes, les cadres juridiques et réglementaires, les meilleures pratiques, les fondamentaux scientifiques et techniques de l'informatique et de la sécurité des systèmes d'information, l'éthique, les aspects économiques et géopolitiques et la stratégie de l'organisation
- Planifier, et appliquer, signaler et communiquer l'analyse, l'évaluation et le traitement des risques
- Intégrer les principes de responsabilité sociétale, d'innovation technologique (IA, automatisation), tout en assurant leur adéquation avec la vision stratégique et les orientations-clés de l'organisation.

Promouvoir la culture cybersécurité et sa consolidation au sein de l'organisation :

- Gérer les incidents de sécurité des systèmes d'information
- Surveiller l'état de la cybersécurité en conformité avec les fondamentaux scientifiques et techniques de l'informatique et de la sécurité des systèmes d'information
- Assurer la continuité des opérations
- Atténuer l'impact des incidents de sécurité
- Préserver les preuves numériques de l'activité malveillante pour permettre les investigations, en conformité avec les normes, les cadres réglementaires et les meilleures pratiques
- Intégrer les principes d'éthique, de responsabilité sociétale et d'innovation technologique (IA pour la corrélation des événements, automatisation des réponses).

Sécuriser les systèmes d'information :

- Planifier, concevoir, déployer et évaluer les solutions de cybersécurité, matériels et services, en intégrant l'évaluation de la criticité des vulnérabilités
- Respecter les normes, cadres réglementaires, meilleures pratiques, en conformité avec les fondamentaux scientifiques et techniques de l'informatique et de la sécurité des systèmes d'information dès la conception et tout au long du cycle de vie des solutions de cybersécurité (infrastructures, systèmes, actifs, logiciels, matériels et services)
- Mobiliser la recherche appliquée et les technologies émergentes pour anticiper les menaces, concevoir des solutions innovantes et renforcer la résilience des systèmes critiques
- Veiller à la responsabilité sociétale et à l'éthique dans la mise en œuvre des dispositifs (sobriété numérique, impact environnemental, considérations sociétales).

Piloter les processus opérationnels et les projets complexes en cyberdéfense :

- Collaborer avec les équipes et les parties prenantes, de manière efficace sur la base d'une communication claire, une compréhension partagée des objectifs et des enjeux, des rôles et des responsabilités bien définis, une confiance mutuelle, le respect, et la gestion constructive des conflits
- Planifier de manière rigoureuse, réaliste, cohérente au regard des contraintes et exigences du donneur d'ordre, en restant flexible pour s'adapter aux changements
- Anticiper, évaluer et atténuer les risques potentiels dans une logique de responsabilité sociétale et de développement durable tout en gérant les exigences de confidentialité et arbitrages de sécurité, grâce à une bonne connaissance et compréhension de l'environnement de l'entreprise ou de l'organisation
- S'assurer que chaque action s'aligne sur les règles en vigueur, sur les fondamentaux scientifiques et techniques de l'informatique et de la sécurité des systèmes d'information ainsi que sur les normes de qualité et de sécurité.

Blocs de compétences

RNCP42905BC01 — Piloter la stratégie de cyberdéfense d'une entreprise ou d'une organisation

LISTE DE COMPÉTENCES

Recueillir, traiter et analyser l'information sur les risques métiers (menaces et vulnérabilités), en conformité avec les normes, les cadres juridiques et réglementaires, les meilleures pratiques, les fondamentaux scientifiques et techniques de l'informatique et de la sécurité des systèmes d'information, l'éthique, les aspects économiques et géopolitiques et la stratégie de l'organisation

Planifier, et appliquer, signaler et communiquer l'analyse, l'évaluation et le traitement des risques

Intégrer les principes de responsabilité sociétale, d'innovation technologique (IA, automatisation), tout en assurant leur adéquation avec la vision stratégique et les orientations clés de l'organisation

Promouvoir la culture cybersécurité et sa consolidation au sein de l'organisation.

MODALITÉS D'ÉVALUATION

Études de cas et projets sur les trois années : travaux individuels et en groupe

Exercice de crise cyber en 5ème année : évaluations individuelles et en groupe

Évaluation par l'entreprise tous les semestres

Soutenance orale en fin de formation devant un jury professionnel.

RNCP42905BC02 — Gérer les incidents de sécurité des systèmes d'information d'une entreprise ou d'une organisation

LISTE DE COMPÉTENCES

Surveiller l'état de la cybersécurité en conformité avec les fondamentaux scientifiques et techniques de l'informatique et de la sécurité des systèmes d'information

Assurer la continuité des opérations

Atténuer l'impact des incidents de sécurité

Préserver les preuves numériques de l'activité malveillante pour permettre les investigations, en conformité avec les normes, les cadres réglementaires et les meilleures pratiques

Intégrer les principes d'éthique, de responsabilité sociétale et d'innovation technologique (IA pour la corrélation des événements, automatisation des réponses).

MODALITÉS D'ÉVALUATION

Études de cas et projets sur les trois années : travaux individuels et en groupe

Exercice de crise cyber en 5ème année : évaluations individuelles et en groupe

Évaluation par l'entreprise tous les semestres

Soutenance orale en fin de formation devant un jury professionnel.

RNCP42905BC03 — Sécuriser les systèmes d'information d'une entreprise ou d'une organisation

LISTE DE COMPÉTENCES

Planifier, concevoir, déployer et évaluer les solutions de cybersécurité, matériels et services, en intégrant l'évaluation de la criticité des vulnérabilités

Respecter les normes, cadres réglementaires et meilleures pratiques en conformité avec les fondamentaux scientifiques et techniques de l'informatique et de la sécurité des systèmes d'information dès la conception et tout au long du cycle de vie des solutions de cybersécurité (infrastructures, systèmes, actifs, logiciels, matériels et services)

Mobiliser la recherche appliquée et les technologies émergentes pour anticiper les menaces, concevoir des solutions innovantes et renforcer la résilience des systèmes critiques

Veiller à la responsabilité sociétale et à l'éthique dans la mise en œuvre des dispositifs (sobriété numérique, impact environnemental, considérations sociétales).

MODALITÉS D'ÉVALUATION

Études de cas et projets sur les trois années : travaux individuels et en groupe

Exercice de crise cyber en 5ème année : évaluations individuelles et en groupe

Évaluation par l'entreprise tous les semestres

Soutenance orale en fin de formation devant un jury professionnel.

RNCP42905BC04 — Piloter les processus opérationnels et les projets complexes en cybersécurité

LISTE DE COMPÉTENCES

Collaborer avec les équipes et les parties prenantes, de manière efficace sur la base d'une communication claire, une compréhension partagée des objectifs et des enjeux, des rôles et des responsabilités bien définis, une confiance mutuelle, le respect, et la gestion constructive des conflits

Planifier de manière rigoureuse, réaliste, cohérente au regard des contraintes et exigences du donneur d'ordre, en restant flexible pour s'adapter aux changements

Anticiper, évaluer et atténuer les risques potentiels dans une logique de responsabilité sociétale et de développement durable tout en gérant les exigences de confidentialité et arbitrages de sécurité, grâce à une bonne connaissance et compréhension de l'environnement de l'entreprise ou de l'organisation

S'assurer que chaque action s'aligne sur les règles en vigueur, sur les fondamentaux scientifiques et techniques de l'informatique et de la sécurité des systèmes d'information, ainsi que sur les normes de qualité et de sécurité.

MODALITÉS D'ÉVALUATION

Études de cas et projets sur les trois années : travaux individuels et en groupe

Exercice de crise cyber en 5ème année : évaluations individuelles et en groupe

Évaluation par l'entreprise tous les semestres

Soutenance orale en fin de formation devant un jury professionnel.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Grands secteurs « classiques » :

- Banque, assurance, services financiers (protection des données clients, lutte contre la fraude)
- Industrie et industrie 4.0 (automobile, énergie, chimie, transport, logistique, etc.)
- Santé et médico-social (hôpitaux, laboratoires, mutuelles, e-santé)
- Technologies de l'information et du numérique : ESN/SSII, éditeurs logiciels, cloud providers, opérateurs télécoms, datacenters
- Commerce en ligne, distribution, plateformes numériques (protection des SI e-commerce, données de paiement, comptes clients).

Secteurs souverains et sensibles :

- Défense, armement, industrie de sécurité, entreprises travaillant pour les ministères régaliens
- Administrations publiques et collectivités, opérateurs d'importance vitale / OSE (énergie, eau, transport, télécoms, finance, santé).

Types de structures où l'on trouve ces postes :

- Grandes entreprises privées (groupes industriels, banques, assureurs).
- Entreprises de services numériques et cabinets de conseil / audit en cybersécurité.
- Organismes publics, hôpitaux, universités, opérateurs d'infrastructures critiques.

En pratique, dès qu'un secteur dépend fortement de systèmes d'information connectés et de données sensibles, il devient un terrain possible pour un ingénieur en cybersécurité.

TYPE D'EMPLOIS ACCESSIBLES

Analyste de la menace cybersécurité

Analyste réponse aux incidents de sécurité

Responsable du SOC

Responsable du CSIRT

Consultant en cybersécurité

Auditeur de sécurité technique.

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)	2 833 €
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)	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)	32 434
Jugés difficiles à recruter	52 %
Emplois saisonniers	1 %
Familles professionnelles (FAP)	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, 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 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 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

Date de dernière délivrance possible 31/08/2030

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2025	71	1	78 %	80 %
2024	81	3	88 %	90 %
2023	88	—	93 %	87 %
2022	52	—	89 %	100 %
2021	55	—	83 %	92 %

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP35799

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/42905/>