

Ingénieur diplômé de l'École nationale supérieure d'ingénieurs de Bretagne Sud, spécialité sécurité des systèmes d'information, en partenariat avec l'ITII Bretagne

RNCP16311 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Sigle	Titre ingénieur — Titre ingénieur
Code(s) NSF	326
Code(s) ROME	M1802, M1803, M1805, M1806, I1401
Type d'enregistrement	Enregistrement de droit
Date d'échéance	31/08/2021

Certificateur(s)

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

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

Résumé de la certification

OBJECTIFS ET CONTEXTE

A compléter (Reprise)

ACTIVITÉS VISÉES

L'ingénieurs en « cyberdéfense », assure la sécurité et les systèmes d'informations. Son rôle est de mesurer la problématique et la diversité de la menace, et d'y répondre par un ensemble de solutions à la fois méthodologiques, technologiques, organisationnelles, humaines, juridiques et déontologiques. Pour cela, il est amené à

- conduire une analyse de risques et de définir une politique de sécurité,
- mettre en œuvre un ensemble de solutions dans une approche globale et opérationnelle dans un environnement menaçant et évolutif,
- gérer des crises face à des attaques complexes,
- expertiser, réaliser et configurer techniquement la problématique,
- définir l'ensemble des procédures d'exploitation et d'administration des configurations,
- gérer des projets spécifiques de sécurité.

La formation de ces ingénieurs se situe au carrefour des diverses disciplines électronique, informatique, réseau, risque, management de projet, éthique, juridique et économique.

COMPÉTENCES ATTESTÉES

Compétences génériques de la spécialité :

Acquisition des connaissances scientifiques et technique et la maîtrise de leur mise en œuvre :

- la connaissance et la compréhension d'un large champ de sciences fondamentales et la capacité d'analyse et de synthèse qui leur est associée
- la capacité à effectuer des activités de recherche, fondamentale ou appliquée, à mettre en place des dispositifs expérimentaux, à s'ouvrir à la pratique du travail collaboratif
- la capacité à trouver l'information pertinente, à l'évaluer et à l'exploiter : compétence informationnelle

Adaptation aux exigences propres de l'entreprise et de la société :

- l'aptitude à prendre en compte les enjeux de l'entreprise : dimension économique, respect de la qualité, compétitivité et productivité, exigences commerciales, intelligence économique
- l'aptitude à prendre en compte les enjeux des relations au travail, d'éthique, de responsabilité, de sécurité et de santé au travail
- l'aptitude à prendre en compte les enjeux et les besoins de la société

La prise en compte de la dimension organisationnelle, personnelle et culturelle :

- la capacité à s'insérer dans la vie professionnelle, à s'intégrer dans une organisation, à l'animer et à la faire évoluer : exercice de la responsabilité, esprit d'équipe, engagement et leadership, management de projets, maîtrise d'ouvrage, communication avec des spécialistes comme avec des non-spécialistes
- la capacité à entreprendre et innover, dans le cadre de projets personnels ou par l'initiative et l'implication au sein de l'entreprise dans des projets entrepreneuriaux
- l'aptitude à travailler en contexte international : maîtrise d'une ou plusieurs langues étrangères et ouverture culturelle associée, capacité d'adaptation aux contextes internationaux
- la capacité à se connaître, à s'autoévaluer, à gérer ses compétences (notamment dans une perspective de formation tout au long de la vie), à opérer ses choix professionnels

Référentiel de compétences de la spécialité :

- analyser le risque cybernétique
- analyser la menace et diagnostiquer le mode opératoire des attaquants
- étudier les vulnérabilités matérielles et logicielles ainsi que les attaques sur les infrastructures
- comprendre l'interconnexion et l'évolutivité à grande échelle des systèmes dans le cyberspace
- définir une politique de sécurité
- Construire la sécurité dynamique des infrastructures dans une approche système
- résoudre des problèmes complexes de niveau système (de nature technologique) par un panel de solutions à la fois méthodologiques, technologiques, organisationnelles, humaines, juridiques et déontologiques
- concevoir, réaliser et mettre en oeuvre un ensemble de solutions de sécurité
- concevoir, réaliser et mettre en oeuvre la protection des systèmes des Opérateurs d'Infrastructures Vitales (OIV)
 - conduire une approche systémique de la sécurité pour sécuriser des systèmes industriels, des systèmes d'information, des systèmes financiers, des systèmes d'armes...
- gérer des crises cybernétiques
- concevoir, développer et exploiter un centre opérationnel de cybersécurité
- détecter dynamiquement les attaques
- réagir en situation de gestion de crise en conformité avec le cadre juridique, les doctrines d'emploi et les règles d'engagement de la cyberdéfense
- expertiser, auditer et évaluer les résistances des configurations techniques des systèmes
- adopter un comportement éthique et déontologique en situation de gestion de crise
- communiquer pendant une crise
- Manager des projets complexes de sécurité des systèmes

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Les secteurs d'activité visés sont principalement ceux des Opérateurs d'Infrastructures Vitales des domaines suivants (250 OIV sont recensés en France) :

- L'Etat et l'Armée, les Banques et les Finances, les Opérateurs Internet et télécom, l'Energie : EDF, Nucléaire, pétrole, Gestion de l'eau, l'Automobile, la Naval, l'Aéronautique, l'Espace, la Santé, le Transport : routier, portuaire, aérien, Electronique

Les secteurs d'activités suivants sont aussi adressés par cette formation :

- Les Entreprises industrielles ou de services qui réalisent, maintiennent et supervisent les infrastructures des Opérateurs d'Infrastructures Vitales,
- Toutes entreprises industrielles, PME ou de services dont le système d'information est ouvert sur l'Internet.

Les secteurs d'activités couverts par cette formation sont donc très étendus.

TYPE D'EMPLOIS ACCESSIBLES

Les principaux types d'emplois accessibles par le détenteur du diplôme d'ingénieur sont les suivants:

- Ingénieur expert en cybersécurité – cyberdéfense
- Ingénieur « cyber architecte »
- Manager d'un centre opérationnel de cybersécurité
- Chef de projet en management de la sécurité
- Auditeur technique ou organisationnel,
- Ingénieur R&D en sécurité,
- Ingénieur sécurité des systèmes,
- Développeur et intégrateur de sécurité de produits COTS,
- Evaluateur sécurité,
- Superviseur sécurité,
- Conseiller en cybersécurité

RÈGLEMENTATIONS D'ACTIVITÉ

A compléter (Reprise)

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)	2 912 €
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) 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)	43 955
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 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

PRÉREQUIS À L'ENTRÉE EN FORMATION

A compléter (Reprise)

COMPOSITION DU JURY — FORMATION CONTINUE

Jury d'attribution composé de :

enseignants, enseignants chercheurs de l'ENSIBS et professionnels en entreprises partenaires

COMPOSITION DU JURY — APPRENTISSAGE

Jury d'attribution composé de :

enseignants, enseignants chercheurs de l'ENSIBS et professionnels en entreprises partenaires

COMPOSITION DU JURY — CONTRAT DE PROFESSIONNALISATION

Jury d'attribution

enseignants, enseignants chercheurs de l'ENSIBS et professionnels en entreprises partenaires

COMPOSITION DU JURY — CANDIDATURE INDIVIDUELLE

Jury d'attribution composé de :

enseignants, enseignants chercheurs de l'ENSIBS et professionnels en entreprises partenaires

COMPOSITION DU JURY — VAE

Jury de recrutement d'attribution composé de :

enseignants, enseignants chercheurs de l'ENSIBS et professionnels en entreprises partenaires

Base légale

Date d'échéance de l'enregistrement 31/08/2021

Liens avec d'autres certifications

NOUVELLE(S) CERTIFICATION(S)

RNCP35799

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/16311/>