Le Répertoire National des Certifications Professionnelles (RNCP)

Résumé descriptif de la certification **Code RNCP : 16311**

Intitulé

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

AUTORITÉ RESPONSABLE DE LA CERTIFICATION	QUALITÉ DU(ES) SIGNATAIRE(S) DE LA CERTIFICATION
Commission des titres d'ingénieurs (CTI), Ministère chargé de l'enseignement supérieur	Président de l'Université de Bretagne Sud, Recteur Chancelier des Universités, Directeur de l'Ecole Nationale Supérieure d'Ingénieurs de Bretagne Sud (ENSIBS)

Niveau et/ou domaine d'activité

I (Nomenclature de 1969)

7 (Nomenclature Europe)

Convention(s) :

Code(s) NSF :

326 Informatique, traitement de l'information, réseaux de transmission

Formacode(s) :

Résumé du référentiel d'emploi ou éléments de compétence acquis

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 situent au carrefour des diverses disciplines électronique, informatique, réseau, risque, management de projet, éthique, juridique et économique.

Compétences génrérique de la spécialité :

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

- 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, maitrise 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 cyberespace
• 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

Secteurs d'activité ou types d'emplois accessibles par le détenteur de ce diplôme, ce titre ou ce certificat

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 telécom, 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.

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

Codes des fiches ROME les plus proches :

M1802 : Expertise et support en systèmes d'information
M1803 : Direction des systèmes d'information
M1805 : Études et développement informatique
M1806 : Conseil et maîtrise d'ouvrage en systèmes d'information
I1401 : Maintenance informatique et bureautique

Modalités d'accès à cette certification

Descriptif des composantes de la certification :

Sciences de base : 15 ECTS
Mathématiques
Informatique Modélisation et programmation
Architecture des systèmes réseaux
Science de la spécialisation : 45 ECTS
Ingénierie des systèmes
Sécurité/Electronique
Analyse des risques
Sécurité des réseaux
Analyse des vulnérabilités numériques
Principe de protection des développements
Systémique de la menace
Détection et analyse des attaques
Stratégie de réaction faces aux attaques
Ingénierie et exploitation d'un centre opérationnel de cybersécurité

Evaluation de la résistance des systèmes

Sciences humaines, économiques, sociales et juridiques : 24 ECTS

Sciences économiques et de gestion

Droit et règlementation en cybersécurité

Gestion de crise - le rapport aux autres – Maîtrise des situations complexes

Méthodologie d'analyse des risques

Gestion de crise – la capacité à mener

Management stratégique

Connaissance du contexte professionnel

Langues et International : 6 ECTS

Anglais

Ouverture à l'international

Période en entreprise: 90 ECTS

Descriptif des évaluations de la certification

Les trois années de scolarité à l'ENSIBS correspondent à l'obtention de **180 ECTS** *(European Credits Transfer System), chaque semestre comptant pour 30 ECTS. Chaque UE validée donne droit à un certain nombre d'ECTS. Les projets sont considérés comme des matières d'UE à part entière*

Les évaluations se font:

- pour chaque UE de l'ENSIBS par un contrôle continu et/ou par un contrôle final de fin de semestre qui donne un grade ECTS

- pour chaque semestre par un jury qui évalue l'acquisition des compétences à l'ENSIBS et celles acquises en entreprise selon le schéma de l'apprentissage. Le jury de fin de semestre décide de la validation des UE ainsi que des grades attribués aux étudiants pour les UE validées : A, B, C, D ou E,

- un projet de fin d'étude et un mémoire final de dernière année soutenu devant un jury mixte ENSIBS- entreprise qui porte sur la totalité des acquis.

Validité des composantes acquises : illimitée

CONDITIONS D'INSCRIPTION À LA CERTIFICATION	OUI	NON	COMPOSITION DES JURYS
Après un parcours de formation sous statut d'élève ou d'étudiant		X	
En contrat d'apprentissage	X		Jury d'attribution composé de : enseignants, enseignants chercheurs de l'ENSIBS et professionnels en entreprises partenaires
Après un parcours de formation continue	X		Jury d'attribution composé de : enseignants, enseignants chercheurs de l'ENSIBS et professionnels en entreprises partenaires
En contrat de professionnalisation	X		Jury d'attribution enseignants, enseignants chercheurs de l'ENSIBS et professionnels en entreprises partenaires
Par candidature individuelle	X		Jury d'attribution composé de : enseignants, enseignants chercheurs de l'ENSIBS et professionnels en entreprises partenaires
Par expérience dispositif VAE	X		Jury de recrutement d'attribution composé de : enseignants, enseignants chercheurs de l'ENSIBS et professionnels en entreprises partenaires

	OUI	NON
Accessible en Nouvelle Calédonie		X
Accessible en Polynésie Française		X

LIENS AVEC D'AUTRES CERTIFICATIONS	ACCORDS EUROPÉENS OU INTERNATIONAUX

Base légale

Référence du décret général :

Articles D612-33 à D612-36 du code de l'éducation (grade de master)

Référence arrêté création (ou date 1er arrêté enregistrement) :

Arrêtédu 13 janvier 2014 fixant la liste des écoles habilitées à délivrer un titre d'ingénieur diplômé

Référence du décret et/ou arrêté VAE :

Références autres :

Pour plus d'informations

Statistiques :

www.univ-*ubs*.fr/*suioip.*

Autres sources d'information :

http:/www.univ-ubs.fr

http:/www.ensibs.univ-ubs.fr

Lieu(x) de certification :

Université de Bretagne Sud

BP 92116

56321 Lorient cedex

Lieu(x) de préparation à la certification déclarés par l'organisme certificateur :

Université de Bretagne Sud

ENSIBS

Rue André Lwoff

BP 573

56017 VANNES

Historique de la certification :

Création de l'ENSIBS en mai 2007

ouverture de la spécialité "sécurité des systèmes d'information" (cyberdéfense) en septembre 2013