

Sciences et ingénierie - Informatique et cybersécurité

RNCP42426 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 6
Sigle	Grade_Licence — Diplôme conférant le grade de Licence
Code(s) NSF	326, 326m, 326n
Formacode(s)	31045, 31008, 31034
Code(s) ROME	M1810, M1806, M1801
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

YNCREA OUEST · SIRET : 39779265600027

Résumé de la certification

OBJECTIFS ET CONTEXTE

Le numérique s'impose comme un secteur en croissance rapide et pourvoyeur massif d'emplois avec près de 151 000 emplois créés en 10 ans. Il n'est pas d'activité économique qui ne soit pas impactée par l'introduction des outils numériques. Le numérique à travers l'émergence de nouveaux modèles économiques est même en passe de transformer durablement des secteurs entiers de l'économie. Cette croissance est soutenue avant tout par les projets « SMACS » ou Social Média, Mobile applications, Data Analytics, Cloud computing et Sécurité informatique. En 2020, Syntec Numérique prévoyait, avant La COVID-19, que les SMACS atteindraient 16,5 milliards d'euros avec une croissance de +14,7%. Au final, même si ces prévisions furent démenties, les SMACS furent néanmoins les moteurs du marché du numérique avec une croissance de +3,2% en 2020. (source : numeriquemaitien-de-la-creation-demploi-en-2020/) De plus, le Campus Cyber a annoncé lors de son lancement début 2022 une pénurie actuelle de 15 000 spécialistes en cyber sécurité en France. Il convient donc d'ajuster l'offre de formation à cette demande au niveau national.

Le Bachelor CyberSécurité

a pour vocation à s'inscrire dans ce contexte général favorable puisque les compétences attestées à l'issue du programme permettent d'exercer précisément toutes les familles de métiers en lien avec le numérique et sa sécurisation.

La plupart des outils de cybersécurité sont conçus pour permettre l'identification et le signalement des activités malveillantes d'un type particulier ; mais bien souvent, il incombe au responsable de la défense et des cyber attaques de comprendre la signification d'une alerte dans son contexte élargi ; d'où l'intérêt de maîtriser son environnement et d'en identifier les menaces.

ACTIVITÉS VISÉES

L'administrateur d'infrastructures sécurisées administre les infrastructures informatiques dont il assure l'installation, le paramétrage, la sécurisation, le maintien en condition opérationnelle et en condition de sécurité.

Il propose et met en œuvre des solutions permettant de faire évoluer les infrastructures et contribue à la gestion des risques et à la politique de sécurité de l'entreprise.

Il installe, sécurise et met en exploitation les composants de l'infrastructure (serveurs, réseaux, hyperviseurs). Il en supervise le fonctionnement et en assure le support, dans le respect des bonnes pratiques méthodologiques.

Il met en œuvre et administre les moyens techniques permettant aux utilisateurs d'accéder aux données et aux

applications pouvant être hébergées sur différentes infrastructures (internes, externalisés, clouds privés ou publics), en assurant la sécurité des accès et la protection des données.

Il intègre les besoins liés à la mobilité dans la gestion de l'environnement de travail des utilisateurs.

L'administrateur d'infrastructures sécurisées applique la politique de sécurité de l'entreprise et contribue à son renforcement par l'étude et la mise en oeuvre de solutions techniques et également par des actions de sensibilisation et de diffusion de bonnes pratiques.

Il exerce ses missions dans le respect des méthodes, des normes et standards du marché, des règles de sécurité, et des contrats de service.

COMPÉTENCES ATTESTÉES

Compétences techniques :

- Administrer et sécuriser les réseaux informatiques d'une organisation en configurant les équipements réseau, les services de communication et les mécanismes de protection, sous la responsabilité d'un référent technique ou d'un responsable infrastructure, afin de garantir la disponibilité, l'intégrité et la confidentialité des échanges au sein du système d'information.
- Administrer et sécuriser des environnements systèmes hétérogènes en configurant les systèmes d'exploitation, les comptes utilisateurs, les droits d'accès et les politiques de sécurité, en collaboration avec les équipes techniques et les utilisateurs, afin d'assurer le bon fonctionnement et la protection des ressources du système d'information.
- Déployer, administrer et sécuriser une infrastructure de serveurs virtualisée en configurant les serveurs, hyperviseurs et ressources virtualisées, conformément aux besoins exprimés par l'organisation et aux procédures définies, afin d'assurer la continuité, la disponibilité et la résilience des services numériques.
- Appliquer les bonnes pratiques d'exploitation, de supervision et de qualité de service en respectant les procédures de sécurité, les normes en vigueur et les exigences de l'organisation, afin de contribuer au maintien en condition opérationnelle et en condition de sécurité des infrastructures informatiques.
- Développer des scripts et des outils d'automatisation dans un langage de programmation adapté afin d'automatiser les tâches d'administration, de déploiement et de sécurisation des infrastructures et services informatiques, en collaboration avec les équipes techniques du système d'information.
- Déployer, configurer et administrer les environnements de travail numériques et les services d'authentification des utilisateurs en tenant compte des besoins fonctionnels, des règles de sécurité et des usages des utilisateurs, afin de garantir un accès sécurisé aux ressources du système d'information.
- Installer, configurer et sécuriser les services d'une infrastructure informatique distribuée, tels que les services web, les bases de données, les services de fichiers, les services de noms ou les services d'adressage réseau, afin d'assurer la disponibilité, les performances et la sécurité des services numériques de l'organisation.
- Superviser les infrastructures informatiques et les services numériques à l'aide d'outils de surveillance et d'analyse afin de mesurer les performances, la disponibilité et les événements de sécurité, et de rendre compte des résultats aux équipes techniques et aux responsables de l'organisation.
- Contribuer à l'évolution d'une infrastructure informatique en proposant des solutions techniques répondant aux besoins fonctionnels, techniques et de cybersécurité exprimés par l'organisation, en collaboration avec les responsables de projet et les experts du système d'information.
- Évaluer le niveau de sécurité d'une infrastructure informatique en réalisant des tests, des analyses de vulnérabilités et des contrôles de conformité afin d'identifier les risques, signaler les incidents et proposer des mesures correctives adaptées au contexte de l'organisation.
- Mettre en œuvre les politiques et procédures de cybersécurité définies par l'organisation, en collaboration avec les équipes techniques et les responsables de la sécurité des systèmes d'information, afin de contribuer à la protection des infrastructures, des services numériques et des données.

Compétences transverses :

- Appliquer des méthodes de gestion de projet et planifier les actions à l'aide d'un outil adapté afin d'assurer le suivi collectif du projet, de prévoir sa complétion dans les temps impartis par les membres de l'équipe et de clore ce dernier en garantissant sa pérennité aux commanditaires et/ou clients.
- Mettre en place un système de veille technologique permettant de collecter, classifier et analyser l'information auprès des équipes afin d'orienter la prise de décisions techniques, l'innovation ou l'entrepreneuriat.
- Communiquer avec les utilisateurs, les équipes techniques, les prestataires et les responsables de projet afin de rendre compte de l'avancement des activités, signaler les incidents, formaliser les besoins et proposer des solutions adaptées au contexte du système d'information.
- Collaborer avec des équipes techniques, des utilisateurs et des partenaires issus d'environnements multiculturels

afin de contribuer à la réalisation de projets informatiques et cybersécurité dans un contexte professionnel national ou international.

- Identifier et prendre en compte les contraintes réglementaires, économiques, éthiques, sociétales et environnementales dans la conduite du projet

Blocs de compétences

RNCP42426BC01 — Administrer et sécuriser les infrastructures informatiques, systèmes et réseaux d'un système d'information

LISTE DE COMPÉTENCES

Administrer et sécuriser les réseaux informatiques d'une organisation en configurant les équipements réseau, les services de communication et les mécanismes de protection, sous la responsabilité d'un référent technique ou d'un responsable infrastructure, afin de garantir la disponibilité, l'intégrité et la confidentialité des échanges au sein du système d'information.

Administrer et sécuriser des environnements systèmes hétérogènes en configurant les systèmes d'exploitation, les comptes utilisateurs, les droits d'accès et les politiques de sécurité, en collaboration avec les équipes techniques et les utilisateurs, afin d'assurer le bon fonctionnement et la protection des ressources du système d'information.

Déployer, administrer et sécuriser une infrastructure de serveurs virtualisée en configurant les serveurs, hyperviseurs et ressources virtualisées, conformément aux besoins exprimés par l'organisation et aux procédures définies, afin d'assurer la continuité, la disponibilité et la résilience des services numériques.

Appliquer les bonnes pratiques d'exploitation, de supervision et de qualité de service en respectant les procédures de sécurité, les normes en vigueur et les exigences de l'organisation, afin de contribuer au maintien en condition opérationnelle et en condition de sécurité des infrastructures informatiques.

MODALITÉS D'ÉVALUATION

L'évaluation des acquis s'effectue dans le cadre d'un contrôle continu des connaissances par semestre. Chaque évaluation conduit à une note sur 20.

Devoirs écrits individuels

Examens de travaux pratiques individuels en laboratoires

Dans le cadre de projets (S1, S3 et S5) et/ou stage :

- Identifier des composants clés du système d'information
- Configurer les paramètres de base d'un réseau
- Configurer les utilisateurs, groupes, stratégies de groupe et politiques de sécurité
- Configurer les paramètres de sécurité avancés (pare-feux, VPN et audits de sécurité)
- Configurer des systèmes de surveillance et de détection d'intrusion (IDS/IPS)

RNCP42426BC02 — Déployer, intégrer et sécuriser les services et environnements numériques d'un système d'information distribué

LISTE DE COMPÉTENCES

Développer des scripts et des outils d'automatisation dans un langage de programmation adapté afin d'automatiser les tâches d'administration, de déploiement et de sécurisation des infrastructures et services informatiques, en collaboration avec les équipes techniques du système d'information.

Déployer, configurer et administrer les environnements de travail numériques et les services d'authentification des utilisateurs en tenant compte des besoins fonctionnels, des règles de sécurité et des usages des utilisateurs, afin de garantir un accès sécurisé aux ressources du système d'information.

Installer, configurer et sécuriser les services d'une infrastructure informatique distribuée, tels que les services web, les bases de données, les services de fichiers, les services de noms ou les services d'adressage réseau, afin d'assurer la disponibilité, les performances et la sécurité des services numériques de l'organisation.

MODALITÉS D'ÉVALUATION

L'évaluation des acquis s'effectue dans le cadre d'un contrôle continu des connaissances par semestre. Chaque évaluation conduit à une note sur 20. Devoirs écrits individuels, Examens de travaux pratiques individuels en laboratoires, présentations orales éventuellement en anglais, rapports et mémoire professionnel, dans le cadre de projets (S1, S2, S3, S4 et S5) et/ou stage/alternance :

- Développer des scripts et des programmes (Bash, C, python)
- Installer et configurer des systèmes d'exploitations (OS)

- Installer des serveurs et configurer leurs services (Web, Base de données, gestion de fichiers, nom de domaine (DNS), protocole de configuration du réseau (DHCP), ...)
- Configurer les paramètres de sécurité
- Configurer Active Directory (AD) et les serveurs de domaine
- Développer des fonctionnalités de base d'un système d'information
- Répondre aux besoins de l'organisation et des utilisateurs (authentification et gestion des accès)
- Mettre en place des mesures pour protéger les données et informations sensibles
- Tester la sécurité du système d'information

RNCP42426BC03 — Faire évoluer et optimiser l'infrastructure numérique et son niveau de sécurité

LISTE DE COMPÉTENCES

Superviser les infrastructures informatiques et les services numériques à l'aide d'outils de surveillance et d'analyse afin de mesurer les performances, la disponibilité et les événements de sécurité, et de rendre compte des résultats aux équipes techniques et aux responsables de l'organisation.

Contribuer à l'évolution d'une infrastructure informatique en proposant des solutions techniques répondant aux besoins fonctionnels, techniques et de cybersécurité exprimés par l'organisation, en collaboration avec les responsables de projet et les experts du système d'information.

Évaluer le niveau de sécurité d'une infrastructure informatique en réalisant des tests, des analyses de vulnérabilités et des contrôles de conformité afin d'identifier les risques, signaler les incidents et proposer des mesures correctives adaptées au contexte de l'organisation.

Mettre en œuvre les politiques et procédures de cybersécurité définies par l'organisation, en collaboration avec les équipes techniques et les responsables de la sécurité des systèmes d'information, afin de contribuer à la protection des infrastructures, des services numériques et des données.

MODALITÉS D'ÉVALUATION

L'évaluation des acquis s'effectue dans le cadre d'un contrôle continu des connaissances par semestre. Chaque évaluation conduit à une note sur 20. Devoirs écrits individuels, Examens de travaux pratiques individuels en laboratoires, présentations orales éventuellement en anglais, rapports et mémoire professionnel, dans le cadre de projets (S1, S2, S3, S4 et S5) et/ou stage/alternance? :

- Identifier les composants clés d'un système embarqué (SOC) et du système d'information à surveiller
- Comprendre les besoins de son organisation et de ses utilisateurs
- Élaborer un plan de projet détaillé
- Protéger les données et les informations sensibles
- Installer et configurer des outils de surveillance et de gestion du système d'information
- Configurer des alertes de sécurité et de l'ensemble des outils de surveillance
- Tester la sécurité d'un système d'information
- Tester le fonctionnement global de l'ensemble d'un système d'information
- Identifier et dépanner les problèmes courants
- Développer des rapports de sécurité détaillés pour les différents acteurs de son organisation

RNCP42426BC04 — Contribuer à la conduite de projet dans ses dimensions innovantes, collaboratives et responsables

LISTE DE COMPÉTENCES

Appliquer des méthodes de gestion de projet et planifier les actions à l'aide d'un outil adapté afin d'assurer le suivi collectif du projet, de prévoir sa complétion dans les temps impartis par les membres de l'équipe et de clore ce dernier en garantissant sa pérennité aux commanditaires et/ou clients.

Mettre en place un système de veille technologique permettant de collecter, classer et analyser l'information auprès des équipes afin d'orienter la prise de décisions techniques, l'innovation ou l'entrepreneuriat.

Communiquer avec les utilisateurs, les équipes techniques, les prestataires et les responsables de projet afin de rendre compte de l'avancement des activités, signaler les incidents, formaliser les besoins et proposer des solutions adaptées au contexte du système d'information.

Collaborer avec des équipes techniques, des utilisateurs et des partenaires issus d'environnements multiculturels afin de contribuer à la réalisation de projets informatiques et cybersécurité dans un contexte professionnel national ou international.

Identifier et prendre en compte les contraintes réglementaires, économiques, éthiques, sociétales et environnementales dans la conduite du projet

MODALITÉS D'ÉVALUATION

L'évaluation des acquis s'effectue dans le cadre d'un contrôle continu des connaissances par semestre. Chaque évaluation conduit à une note sur 20.

Devoirs écrits individuels

Examens de travaux pratiques individuels en laboratoires

Dans le cadre d'un projet et/ou alternance,

le/la candidat(e) doit :

- Évaluer les moyens nécessaires pour atteindre les objectifs du projet,
- Fixer les étapes de réalisation du projet, Déterminer les durées et les marges de chaque étape,
- Définir les méthodes de suivi associées, réaliser un planning à l'aide d'un outil adapté
- Réaliser un état de l'art des méthodologies et outils en explicitant le choix des sources,
- Proposer une analyse de la fiabilité des sources utilisées
- Répondre aux questionnements des différents interlocuteurs,

Adapter son langage à son interlocuteur, rédiger un compte rendu d'avancement

- Effectuer un travail de groupe sur projet (en équipe multiculturelle réelle ou simulée) :
- Observer les interactions lors des réunions de groupe, Évaluation du livrable final du projet (rapport, présentation, prototype, etc.)

- Réaliser des jeux de rôle ou mises en situation interculturelles :

Cas pratiques simulant des conflits ou défis interculturels à résoudre collectivement,

- Réaliser un Journal de bord / autoévaluation / évaluation croisée :

Journal réflexif sur les dynamiques de l'équipe et les adaptations culturelles, Feedback des pairs sur la collaboration au sein de l'équipe

- Réaliser un Entretien oral ou soutenance : Présentation de l'expérience de travail en équipe interculturelle, Réponses à des questions portant sur les comportements adoptés et les apprentissages réalisés

- Réaliser une étude de cas / dossier projet :

Analyse d'un projet réel ou fictif intégrant les différentes contraintes, Proposition de solutions ou d'adaptations prenant en compte ces contraintes

- Réaliser un projet tutoré ou travail de groupe : Élaboration d'un projet intégrant explicitement les aspects réglementaires, économiques, éthiques, sociétaux et environnementaux

- Réaliser une soutenance orale / présentation : Argumentation des choix réalisés dans la gestion du projet en lien avec les contraintes identifiées

- Réaliser un rapport de stage ou retour d'expérience : Analyse critique de la prise en compte des contraintes dans un contexte professionnel vécu

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Les différents secteurs d'activité concernés sont principalement :

Entreprise de services du numérique (ESN) ;

les Direction des Systèmes d'Information (DSI) ;

les PME/PMI

les Collectivités territoriales ou service public.

TYPE D'EMPLOIS ACCESSIBLES

Administrateur systèmes et réseaux (et sécurité).

Administrateur systèmes (et sécurité).

Administrateur réseaux (et sécurité).

Administrateur d'infrastructures.

Superviseur infrastructure et réseaux.

Responsable infrastructure systèmes et réseaux.

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	Lien formation-emploi, Manque de main-d'œuvre disponible
Salaire médian (mensuel)	2 704 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (35 % 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) 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)	14 307
Jugés difficiles à recruter	46 %
Emplois saisonniers	2 %
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en 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 initiale, Apprentissage, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

Pour accéder au parcours de formation menant à la certification, les candidats doivent être titulaires du baccalauréat général (toutes options confondues, avec au moins 1 option scientifique) ou titulaires du baccalauréat technologique STI2D ou titulaires du baccalauréat professionnel CIEL.

PRÉREQUIS À LA VALIDATION

Pour accéder à la certification les candidats devront avoir validé tous les modules de formation ainsi que les critères suivants :

- La validation d'une maîtrise de l'anglais, validé par le cadre européen commun de référence pour les langues, de niveau B1 (utilisateur indépendant) est un prérequis à la validation du diplôme.
- Dans le cadre des contraintes de la commission des titres ingénieurs, l'élève devra valider durant son passage à l'école une mobilité internationale, d'une durée minimale de quatre semaines consécutives à réaliser avant l'entrée en deuxième année.
- Un stage associatif ou ouvrier, d'une durée minimale de 4 semaines consécutives, est à effectuer en fin de première année. Il peut être couplé avec la mobilité internationale. Le poste du stagiaire doit s'intégrer dans un travail d'équipe, qu'il s'agisse d'un stage ouvrier (chaîne de production, manutention, livraison, conditionnement, maintenance, accueil, administration) ou d'un stage en association. Dans les deux cas, le stagiaire découvre l'univers professionnel sous différentes facettes : relations hiérarchique, charge de travail, relations professionnelles (alliances, conflits, coopération).

COMPOSITION DU JURY — FORMATION INITIALE, APPRENTISSAGE

Le Directeur Général de Yncréa Ouest (1 voix délibérative)

Le Directeur des études de site (1 voix délibérative)

Le Responsable de la formation par apprentissage (1 voix délibérative)

15 enseignants de l'établissement (les responsables de domaine professionnel, 1 voix délibérative chacun)

Base légale

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

Date de dernière délivrance possible	30/08/2031
--------------------------------------	------------

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

isen-ouest.fr

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/42426/>