

Ingénieur diplômé de l'Institut national des sciences appliquées Centre Val de Loire, spécialité sécurité informatique

RNCP40496 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Sigle	Titre ingénieur — Titre ingénieur
Code(s) NSF	326
Formacode(s)	31034, 31038, 31045, 32062, 15099
Code(s) ROME	M1805, M1810, M1803, M1802, M1801
Type d'enregistrement	Enregistrement de droit
Date d'échéance	31/08/2028

Certificateur(s)

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

INSTITUT NATIONAL DES SCIENCES APPLIQUEES CENTRE VAL DE LOIRE · SIRET : 13001833600011

Partenaires habilités

1 organisme habilité, d'après la liste publiée par France compétences : 1 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
CENTRE DE FORMATION – CAMPUS CCI CHER	18180001200096	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

L'évolution de plus en plus rapide de la technologie apporte chaque jour de nouvelles possibilités. La démocratisation d'Internet, la généralisation de l'utilisation des smartphones et l'émergence des objets connectés sont des exemples récents de cette évolution. Au niveau de l'entreprise, le système d'information est devenu l'un des points névralgiques car il concentre une grande partie de leur richesse, en particulier les données de l'entreprise et de ses clients. Ce sont autant d'objets de convoitises qui peuvent être obtenus par des attaques informatiques dont la presse se fait régulièrement écho. Même s'il est difficile d'évaluer le préjudice réel des attaques sur le système d'information, le nombre d'entreprises estimant avoir subi des pertes est en constante augmentation.

Cette nécessité de se protéger contre les attaques informatiques a été soulignée par le livre blanc de la Défense. En Europe, le manque d'experts en cybersécurité était estimé à 350 000 en 2022.

En France, l'ANSSI et les acteurs du secteur estiment que plus de 25 000 postes de spécialistes en cybersécurité sont actuellement vacants, un chiffre qui devrait atteindre 37 000 d'ici 2027 selon les projections de France Cybersecurity. Cette pénurie s'accroît alors que les attaques informatiques ont augmenté de 73% en volume depuis 2022. L'évolution rapide des technologies informatiques s'accompagne de l'émergence de nouvelles menaces de plus en plus sophistiquées. L'intelligence artificielle est désormais utilisée pour automatiser et optimiser les cyberattaques. La multiplication des attaques de type supply chain qui ciblent les chaînes d'approvisionnement logicielles représente également une menace majeure, comme l'ont montré les incidents SolarWinds et Log4j. Par ailleurs, la généralisation des environnements cloud et des architectures hybrides crée de nouvelles surfaces d'attaque, ainsi que l'expansion

de l'Internet des Objets (IoT).

Le but de cette certification est d'apporter les bases théoriques, technologiques et pratiques pour répondre à ces besoins.

La certification « Ingénieur diplômé de l'Institut National des Sciences Appliquées Centre Val de Loire, spécialité sécurité informatique » délivre des compétences en sécurité tels que sécurité système, sécurité Windows, sécurité réseau, cryptographie ou protection et anonymisation de données.

Elle garantit que les ingénieurs qui auront obtenu cette certification seront capables de concevoir et de déployer des solutions robustes de protection, de mettre en place des méthodologies d'analyse des risques et de sécurité, et de piloter des projets complexes dans un environnement en constante évolution. Elle répond ainsi aux besoins des organisations confrontées aux menaces croissantes sur leurs systèmes informatiques.

ACTIVITÉS VISÉES

Dans le cadre de la certification sécurité informatique, l'ingénieur exerce des responsabilités techniques et organisationnelles à différents niveaux, tout en mobilisant à la fois les compétences génériques de l'ingénieur (analyse, conception, pilotage de projets, management, communication) et les compétences spécifiques liées à la cybersécurité (conseil, audit, déploiement de solutions, gestion des incidents).

Les activités visées se structurent autour de grands domaines? :

A. Activités génériques de l'ingénieur

1. Conception et conduite de projets :

- Recueillir et analyser les besoins auprès des parties prenantes.
- Définir une architecture technique et planifier les ressources nécessaires.
- Piloter les étapes de réalisation (planification, suivi budgétaire, gestion des risques et des aléas).
- Animer des équipes pluridisciplinaires et assurer la communication avec l'ensemble des acteurs.

2. Recherche, innovation et veille technologique :

- Participer à l'exploration de nouvelles solutions, outils ou méthodes.
- Conduire des expérimentations, valider les choix techniques et analyser la valeur ajoutée pour l'entreprise.
- Mettre en place une veille continue sur les évolutions scientifiques et technologiques.

3. Management et intégration dans l'organisation :

- Manager et faire évoluer une équipe (communication, leadership, gestion des compétences).
- Participer à la définition et au déploiement de la stratégie de l'organisation ou du service.
- Prendre en compte les contraintes économiques, juridiques et environnementales.

4. Qualité, sécurité, responsabilité sociétale

- Intégrer les dimensions qualité et durabilité dans la conception et l'exploitation de solutions.
- Participer aux démarches de certification, d'amélioration continue et de gestion des risques.
- Respecter et faire respecter les normes en vigueur (santé, sécurité au travail, environnement).

B. Activités spécifiques à la spécialité sécurité informatique

1. Conseil et audit en cybersécurité

- Diagnostiquer le niveau de maturité d'une organisation en matière de sécurité des systèmes d'information.
- Établir un plan d'action pour corriger les vulnérabilités et anticiper les menaces.
- Sensibiliser et former les équipes, proposer des mesures organisationnelles et techniques adaptées.

2. Conception et architecture de solutions sécurisées

- Définir et mettre en œuvre des architectures sécurisées (réseau, systèmes, applications, cloud, IoT) répondant aux exigences métiers.
- Choisir les technologies et standards appropriés (cryptographie, authentification, virtualisation...).
- Vérifier l'interopérabilité des systèmes et leur conformité aux référentiels (ISO 27001, NIST, etc.).

3. Gestion des incidents et réponses aux attaques

- Mettre en place des systèmes de détection et de surveillance (SIEM, sondes, analyses de logs).
- Coordonner la réponse à un incident? : confinement, analyse forensique, remédiation et retour d'expérience.
- Élaborer et maintenir un plan de continuité et de reprise d'activité (PCA/PRA).

4. Pilotage de la sécurité et management des risques

- Évaluer les risques informatiques en s'appuyant sur des méthodes reconnues.
- Mettre en place et suivre les politiques de sécurité (PSSI), définir les procédures internes.
- Élaborer des tableaux de bord (indicateurs de sécurité, suivi de la conformité) et rendre compte à la direction.

5. Veille technologique et prospective en cybersécurité

- Analyser l'émergence de nouvelles menaces ou vulnérabilités.

- Tester et intégrer de nouvelles solutions de protection ou de détection.
- Anticiper les évolutions réglementaires et industrielles liées à la sécurité informatique.

À travers ces activités, l'ingénieur en sécurité informatique mobilise une double compétence :

- une maîtrise des fondamentaux de l'ingénieur (gestion de projet, management, approche systémique, communication)
- une expertise approfondie dans le domaine de la cybersécurité (conseil, audit, conception de solutions sécurisées, gestion des incidents).

Cette polyvalence lui permet de proposer et d'implémenter des solutions intégrées répondant aux exigences de performance, de fiabilité et de sécurité des organisations.

COMPÉTENCES ATTESTÉES

Mobiliser un large socle de connaissances scientifiques et techniques pour analyser et résoudre des problèmes complexes :

- Connaître et comprendre les principes fondamentaux de l'informatique (algorithmique, structures de données, architectures matérielles, mathématiques pour l'informatique)
- Analyser, modéliser et résoudre des problèmes nouveaux en mobilisant des méthodes appropriées

Concevoir et développer des solutions logicielles sûres et performantes :

- Analyser un cahier des charges, identifier les contraintes de performance et de sécurité
- Modéliser les fonctionnalités, choisir les architectures et modèles de conception adaptés
- Programmer dans divers langages en appliquant les bonnes pratiques de programmation sécurisée
- Mettre en place des environnements d'intégration continue, assurer la qualité et la maintenabilité du code

Administrer et sécuriser les infrastructures systèmes et réseaux :

- Installer, configurer et gérer des systèmes d'exploitation, des services réseau (serveurs, routeurs, pare-feu)
- Mettre en place des politiques de sécurité
- Mettre en place des infrastructures complexes sécurisées (virtualisation, cloud)
- Superviser la disponibilité, la fiabilité et la sécurité de l'infrastructure, diagnostiquer et résoudre des incidents complexes

- Appliquer les référentiels et les normes, et documenter les procédures
- Renforcer les compétences en sécurité des systèmes embarqués et IoT
- S'appuyer sur l'intelligence artificielle (IA) pour analyser et renforcer la sécurité

Mettre en œuvre une démarche d'analyse de risques et d'audit de la cybersécurité :

- Identifier les menaces, vulnérabilités et impacts
- Concevoir et piloter un plan d'actions de sécurité, proposer des solutions techniques et organisationnelles
- Réaliser ou superviser des tests d'intrusion, des audits de configuration, en analyser les résultats et y remédier
- Organiser la gestion des incidents et des crises (détection, réponses, forensique, retours d'expérience)

Déployer et maintenir un système d'information fiable et conforme :

- Concevoir une architecture intégrant les exigences de performance, de disponibilité et de confidentialité
- Sélectionner et mettre en place les outils (virtualisation, conteneurs, bases de données, SIEM...) adaptés aux besoins métier

Piloter l'évolution du système d'information (mise à jour, migrations, innovations), tout en garantissant la continuité de service

- Assurer la conformité légale et réglementaire et négocier avec les parties prenantes internes/externes

Manager un projet informatique et animer une équipe technique :

- Définir l'objectif, le périmètre, les ressources et le planning, choisir une méthode de conduite de projet
- Coordonner les parties prenantes au projet, planifier et piloter l'avancement, gérer les risques et arbitrer
- Encadrer, motiver et faire monter en compétences les membres de l'équipe, gérer la communication et la répartition des tâches

- Évaluer la qualité des livrables, conduire un retour d'expérience et capitaliser les bonnes pratiques

Communiquer efficacement, en français et en anglais, auprès de différents interlocuteurs :

- Synthétiser et vulgariser un contenu technique complexe à destination de publics variés
- Rédiger des documents clairs et structurés
- Mener des réunions et présentations orales de manière professionnelle
- Démontrer une ouverture culturelle et un savoir-être favorisant le travail en contexte international et multiculturel

Prendre en compte les enjeux économiques, organisationnels et sociétaux dans la conception et l'exploitation des systèmes :

- Intégrer les impératifs de coût, de performance et de qualité dans les choix techniques ou organisationnels
- Identifier les risques humains, juridiques et éthiques liés aux technologies numériques
- Organiser et assurer la sensibilisation et la sécurisation des utilisateurs
- Anticiper les évolutions pour proposer des innovations ou des adaptations du système d'information

Conduire une démarche de veille et d'innovation en cybersécurité :

- Suivre l'état de l'art en matière de menaces, de vulnérabilités et de solutions de sécurité
- Identifier et expérimenter de nouvelles approches ou technologies
- Contribuer à la recherche, au développement ou à l'amélioration continue de méthodes et d'outils de cybersécurité

Développer des aptitudes d'autonomie, d'esprit critique et d'évolutivité dans la carrière :

- S'autoévaluer, mettre à jour ses connaissances en continu, gérer son projet professionnel
- Faire preuve de méthodologie, de rigueur et d'éthique dans la pratique quotidienne
- S'engager sur la qualité, la sécurité et la responsabilité sociétale dans toutes les décisions professionnelles

Blocs de compétences

RNCP40496BC01 — Concevoir et développer des solutions logicielles robustes

LISTE DE COMPÉTENCES

- Analyser et formaliser le besoin à partir d'un cahier des charges
- Concevoir l'architecture logicielle (séparation des couches, design patterns, diagrammes d'architecture)
- Programmer dans plusieurs langages en adoptant les bonnes pratiques (revues de code, tests unitaires, intégration continue)
- Implémenter des mécanismes de sécurité applicative (gestion d'authentification, contrôle d'accès, protection contre les injections, etc.)
- Optimiser la performance et la maintenabilité via des outils d'analyse

MODALITÉS D'ÉVALUATION

Les apprenants sont évalués à travers des mises en situation professionnelles (projets pédagogiques, projets technologiques, projets de recherche, projets transverses, stages, missions en alternance) et un contrôle continu, qui comporte :

- des évaluations individuelles (épreuves sur table ou sur machine),
- des rapports écrits et des soutenances orales portant sur les projets, stages ou missions réalisés en entreprise.

RNCP40496BC02 — Administrer et sécuriser les infrastructures systèmes et réseaux

LISTE DE COMPÉTENCES

- Installer et configurer les systèmes (Linux, Windows) ainsi que les services réseau (DNS, DHCP, VLAN, firewall, etc.)
- Installer et configurer des infrastructures Cloud privées ou publiques
- Mettre en place la supervision et la haute disponibilité
- Sécuriser l'architecture réseau (pare-feu, IDS/IPS, VPN, segmentation, annuaires, gestion des droits)
- Diagnostiquer les incidents (analyse des journaux, dépannage réseau, scripts d'automatisation)
- Documenter et maintenir la configuration pour assurer la traçabilité et la conformité

MODALITÉS D'ÉVALUATION

Les apprenants sont évalués à travers des mises en situation professionnelles (projets pédagogiques, projets technologiques, projets de recherche, projets transverses, stages, missions en alternance) et un contrôle continu, qui comporte :

- des évaluations individuelles (épreuves sur table ou sur machine),
- des rapports écrits et des soutenances orales portant sur les projets, stages ou missions réalisés en entreprise.

RNCP40496BC03 — Auditer la sécurité du système d'information, gouvernance et gestion des risques

LISTE DE COMPÉTENCES

- Conduire une analyse de risques selon les référentiels et évaluer la criticité des vulnérabilités
- Mettre en œuvre ou auditer un Système de Management de la Sécurité de l'Information? : définir les objectifs de sécurité, les politiques, les procédures
- Réaliser des tests d'intrusion (pentest réseau, web, applications) et analyser les résultats (scénarios d'attaque)
- Réaliser des analyses de logiciels (retro-ingénierie, vérification, complexité)

- Proposer un plan de traitement des risques (correctifs, plans d'action, priorisation budgétaire)
- Superviser la conformité réglementaire et la gouvernance (chartes, suivi des indicateurs de sécurité)

MODALITÉS D'ÉVALUATION

Les apprenants sont évalués à travers des mises en situation professionnelles (projets pédagogiques, projets technologiques, projets de recherche, projets transverses, stages, missions en alternance) et un contrôle continu, qui comporte :

- des évaluations individuelles (épreuves sur table ou sur machine),
- des rapports écrits et des soutenances orales portant sur les projets, stages ou missions réalisés en entreprise.

RNCP40496BC04 — Piloter des projets informatiques et manager l'innovation

LISTE DE COMPÉTENCES

- Élaborer et suivre un plan projet (planning, budget, ressources, gestion des risques) en s'appuyant sur des méthodologies
- Manager une équipe pluridisciplinaire (communication, leadership, motivation, négociation, arbitrage)
- Réaliser des revues d'avancement (indicateurs de suivi, tableaux de bord, reporting auprès des parties prenantes)
- Gérer les risques projet (aléas coûts/délais, dérives techniques) et piloter le changement (formation, accompagnement)
- Initier ou accompagner l'innovation (veille technologique, prototypage, retours d'expérience)

MODALITÉS D'ÉVALUATION

Les apprenants sont évalués à travers des mises en situation professionnelles (projets pédagogiques, projets technologiques, projets de recherche, projets transverses, stages, missions en alternance) et un contrôle continu, qui comporte :

- des évaluations individuelles (épreuves sur table ou sur machine),
- des rapports écrits et des soutenances orales portant sur les projets, stages ou missions réalisés en entreprise.

RNCP40496BC05 — Communiquer, intégrer les enjeux juridiques et sociétaux

LISTE DE COMPÉTENCES

- Rédiger et présenter des documents professionnels (rapports, notes de synthèse, présentations orales)
- Identifier les obligations légales (droit du numérique, RGPD, propriété intellectuelle) et évaluer l'impact sur les projets (gestion des données personnelles, open source)
- Prendre en compte les aspects éthiques, environnementaux (responsabilité sociale des entreprises - RSE) et humains (management, sociologie des organisations) dans les décisions techniques
- Utiliser l'anglais professionnel à l'écrit/oral (documentation technique, conférences, soutenances)
- Sensibiliser et former les équipes ou utilisateurs aux bonnes pratiques de sécurité et aux risques numériques (hygiène numérique)

MODALITÉS D'ÉVALUATION

Les apprenants sont évalués à travers des mises en situation professionnelles (projets pédagogiques, projets technologiques, projets de recherche, projets transverses, stages, missions en alternance) et un contrôle continu, qui comporte :

- des évaluations individuelles (épreuves sur table ou sur machine),
- des rapports écrits et des soutenances orales portant sur les projets, stages ou missions réalisés en entreprise.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

- Sociétés de services et de conseil en informatique
- Banques, assurances et institutions financières
- Opérateurs en télécommunication et fournisseurs d'accès internet
- Industries et groupes de haute technologie
- Industries aéronautique et de la défense
- Administrations publiques, collectivités et organismes de défense
- Commerce, distribution et e-commerce
- Santé et laboratoires

- Éditeurs de logiciels de sécurité
- Prestataires Cloud et centres de données
- Start-up spécialisées en cybersécurité

TYPE D'EMPLOIS ACCESSIBLES

- Ingénieur recherche et développement
- Ingénieur études et développement en systèmes d'information
- Ingénieur développement système embarqué
- Ingénieur développement sécurisé
- Ingénieur études/développement
- Ingénieur en sécurité Cloud
- Ingénieur en sécurité des données
- Architecte de conception d'ensemble
- Intégrateur en cyberdéfense
- Consultant en sécurité informatique
- Ingénieur supervision réseaux
- Ingénieur DevOps
- Pentester / ingénieur tests d'intrusion
- Analyste SOC (Security Operations Center)
- Ingénieur réseau et sécurité
- Chef de projet cybersécurité / IT
- Responsable de la sécurité des systèmes d'information (RSSI) / adjoint RSSI
- Consultant cloud security
- Chef de projet IT
- Ingénieur sécurité des données
- Ingénieur sécurité d'infrastructures
- Ingénieur défense réseau
- Architecte de solutions de sécurité
- Directeur cybersécurité
- Architecte sécurité
- Cryptologue
- Administrateur de solutions de sécurité
- Responsable du SOC
- Responsable du CSIRT
- Analyste réponse aux incidents de sécurité
- Gestionnaire de crise de cybersécurité
- Analyste de la menace cybersécurité
- Formateur en cybersécurité
- Intégrateur de solutions de sécurité
- Chercheur en sécurité des systèmes d'information
- Security service delivery manager

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 initiale, Formation continue, Apprentissage, Contrat de professionnalisation, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

Formation initiale :

- sous statut étudiant : élèves issus d'une Classe préparatoire aux grandes écoles (CPGE) mathématiques, physique et informatique (MPI), mathématiques et physique (MP), physique et sciences de l'ingénieur (PSI), physique et technologie (PT), technologie et sciences industrielles (TSI).
- sous statut apprenti : élèves issus d'un BUT 2 ou 3 (Bachelor Universitaire de Technologie), Licence 2ème année, Licence 3ème année, Master 1ère année, Master 2ème année à dominante scientifique/informatique.

COMPOSITION DU JURY — FORMATION INITIALE, FORMATION CONTINUE, APPRENTISSAGE, CONTRAT DE PROFESSIONNALISATION, VAE

Jury de diplôme annuel composé du directeur de l'établissement, du directeur des formations et de la vie étudiante, professeur des universités, de cinq directeurs de département, enseignants-chercheurs et enseignants, et d'enseignants en poste à l'INSA Centre Val de Loire selon la spécialité d'ingénieur.

Financement en alternance (NPEC)

Niveau de prise en charge d'un contrat d'apprentissage par les OPCO, fixé par France compétences par branche professionnelle (CPNE).

Prise en charge usuelle	8 668 €
Selon la branche	7 440 € – 9 077 €
Prise en charge	Branches concernées
8 668 €	Valeur par défaut · 203 branches

9 077 €	CPNE des Télécoms, CPNEFP Mutualité, CPNEFP Transformation Laitière, CPNEFP de la branche des industries de produits alimentaires élaborés
8 647 €	CPNE des industries de santé (CPNEIS), CPNEFP ICGV entreprises de la viande
8 500 €	CPNE Branche Caoutchouc, CPNEFP de la métallurgie
8 100 €	CPNE Banque
7 440 €	CPNE de l'ingénierie, des services informatiques et du conseil

Base légale

Date d'échéance de l'enregistrement 31/08/2028

Liens avec d'autres certifications

ANCIENNES VERSIONS
RNCP25759

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://syllabus.insa-cvl.fr/fr/maquette/list?dept=1&status=1>

<https://syllabus.insa-cvl.fr/fr/maquette/list?dept=1&status=2>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/40496/>

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 06/2028

Catalogue des formations en apprentissage — réseau des Carif-Oref. Sans frais pour l'alternant : formation financée par l'OPCO de la branche (NPEC).