# Titre RNCP Niveau 6 Concepteur intégrateur d'infrastructures informatiques (systèmes et réseaux, applicatives, ou de sécurité) parcours Cybersécurité

## Présentation

### Publics / conditions d'accès

Cette formation est ouverte aux titulaires d'un diplôme Bac+2 en informatique.

Les titulaires d'un diplôme Bac+2 scientifique ou technique non informatique peuvent aussi suivre cette information après avoir acquis, au choix :

- les deux unités d'enseignement NFA031 (Programmation avec Java : notions de base) et NFA032 (Programmation Java : programmation objet)
- ou les deux unités d'enseignement NFP135 (Valeur d'Accueil et de Reconversion en Informatique 1) et NFP136 (Valeur d'Accueil et de Reconversion en Informatique 2), mais qui ne sont plus programmées à partir de septembre 2025.

L'accès à cette formation est aussi possible par la voie de la validation d'acquis de l'expérience (VAE) ou encore par la voie de la validation des études supérieures (VES). Des dispenses d'unités d'enseignement peuvent être accordées aux titulaires d'un diplôme Bac+3 en informatique.

### Objectifs

Ce titre de concepteur en architecture informatique option cybersécurité vise à développer la capacité de concevoir, développer et maintenir en condition opérationnelle une architecture de sécurité en respectant une démarche qualité, en tenant compte du contexte de l'entreprise, des attentes et besoins des utilisateurs et en veillant aux évolutions technologiques. Il fournit aussi les bases pour l'organisation et l'encadrement d'une équipe technique. A l'issue de sa formation, l'auditeur pourra, à titre d'exemple, exercer ses compétences dans le maintien en sécurité du système d'information de son entreprise. Il peut se voir confier la conduite d'une analyse des risques informatiques, la mise en œuvre de politiques de sécurité ou le rôle d'architecte de sécurité.

**Organisation de la formation**

Cette formation est composée :

- d'enseignements permettant d'acquérir les compétences de base,
- d'enseignements de spécialisation et d'ouverture,
- d'enseignements en management,
- et d'un enseignement d'anglais préparant l'auditeur au test de BULATS niveau II (ou équivalent).

Il est fortement recommandé aux auditeurs (si concernés) :

- de commencer leurs parcours par les unités d'enseignement associées aux compétences de base,
- de suivre l'enseignement d'anglais très tôt dans le parcours.

**Remarques :**

- Toute personne ayant validé SEC104, SEC106 ou SEC107 *avant octobre 2026* conserve ces crédits au titre des UE de cybersécurité avancée.
- Toute personne ayant validé SEC103 *avant octobre 2026* conserve ces 6 crédits au titre des 12 crédits à choisir parmi le bloc proposant au choix CCE208, DNT104, GDN100, GDN209, …, STA101
- SEC101 sera retirée du cursus à partir de septembre 2027.

Mis à jour le 12-06-2026

Fin d'accréditation au 21-12-2028

**Code : CRN0803A**

Titre RNCP Niveau 6

**Responsabilité nationale :** EPN05 - Informatique / Nicolas PIOCH

**Niveau CEC d'entrée requis :** Niveau 5 (ex Niveau III)

**Niveau CEC de sortie :** Niveau 6 (ex Niveau II)

**Mode d'accès à la certification :**

- Apprentissage
- Contrat de professionnalisation
- Validation des Acquis de l'Expérience
- Formation continue

**NSF :** Informatique, traitement de l'information, réseaux de transmission (326) , Analyse informatique, conception d'architecture de réseaux (326n) , Exploitation informatique (326u)

**Métiers (ROME) :** Responsable sécurité informatique (M1802) , Opérateur / Opératrice en cybersécurité (M1810) , Analyste en cybersécurité (M1805) , Ingénieur / Ingénieure sécurité web (M1802) , Ingénieur / Ingénieure sécurité informatique (M1802) , Expert / Experte sécurité, méthode et qualité informatique (M1802) , Expert / Experte sécurité informatique (M1802) , Expert / Experte en sécurité des systèmes d'exploitation (M1802) , Administrateur / Administratrice sécurité informatique (M1801) , Développeur / Développeuse de sécurité des systèmes d'information (M1805) , Expert / Experte en tests d'intrusion - sécurité des systèmes d'information (M1802) , Expert / Experte en sécurité des systèmes d'information (M1802) ,

- L'auditeur souhaitant obtenir une dérogation devra passer par la VES.

**Passerelles :**

*vers le Master Sécurité informatique, cybersécurité et cybermenaces*

- Pour l'année académique 2026-2027, le candidat qui souhaite poursuivre son cursus en Master devra avoir choisi et validé les UE suivantes dans chaque bloc :
  - dans les blocs d'UE cybersécurité, choisir RSX112 et CYB105
  - dans le premier bloc « 1 UE d'ouverture », choisir NFE115
  - dans le bloc « 1 UE de gestion de la qualité », choisir RCP103, RCP104 ou NFP101
  - dans le second bloc « 1 UE d'ouverture », choisir RSX103 ou SMB111
  - dans le bloc « 12 crédits », DNT104 est conseillé sans être obligatoire

*vers le diplôme Ingénieur informatique, parcours cybersécurité*

- Pour l'année académique 2026-2027, le candidat qui souhaite poursuivre son cursus en diplôme ingénieur devra avoir choisi et validé les UE suivantes dans chaque bloc :
  - dans les blocs d'UE cybersécurité, choisir RSX112 et CYB108
  - dans le premier bloc « 1 UE d'ouverture », choisir RCP105, RCP101, SMB101, NFP107, NFE114, NFE108, NSY103 ou GLG105
  - dans le bloc « 12 crédits », DNT104 et GDN100 sont conseillés sans être obligatoires

## Modalités de validation

Ce titre de « Concepteur en Architecte Informatique, option Cybersécurité » est délivré, par le jury diplômant du Cnam Paris, à tout auditeur remplissant les conditions suivantes :

- Validation de l'ensemble des unités d'enseignements de ce titre
- Obtention du niveau d'anglais B1 du CECRL
- Justification d'une expérience professionnelle :
  - de 2 ans à temps plein dans le domaine du diplôme
  - ou de 3 ans à temps plein dans un autre domaine complété par un stage d'au moins 3 mois en relation avec cette certification.
- Rédaction d'un rapport d'activité professionnelle décrivant cette expérience professionnelle.

La demande de délivrance du diplôme ainsi que celle de l'analyse de l'expérience professionnelle se font en ligne : voir les deux procédures.

**Remarques :**

- *Une unité d'enseignement ne peut être validée qu'une seule fois.*
- *La validation de l'expérience professionnelle se fait **en fin de parcours.***

# Compétences

- Capturer des exigences métiers, les traduire en un ensemble cohérent d'exigences fonctionnelles et non-fonctionnelles, les formaliser
- Participer à la rédaction d'un cahier des charges
- Analyser un cahier des charges et proposer des solutions techniques
- Élaborer un document de spécification technique servant d'appui à la mise en œuvre d'un composant du Système d'Information
- Mettre en œuvre une solution technique, associée à un composant du Système d'Information en respectant une spécification
- Élaborer des tests et les exécuter
- Rédiger un cahier de tests
- Intégrer un composant développé dans son environnement d'exploitation
- Piloter les phases de développement, de tests et d'intégration
- Conduire une analyse des risques informatiques

Auditeur / Auditrice en sécurité des systèmes d'information (M1802) , Architecte de sécurité des systèmes d'information (M1802) , Analyste en vulnérabilité de code logiciel (M1802) , Expert / Experte en cybersécurité (M1802) , Administrateur / Administratrice système informatique (M1801)

**Code répertoire :** RNCP38461

**Code CertifInfo :** 52840

**Contact national :**

EPN05 - Informatique - RNCP CIII

75003 Paris

par_RNCPCIII@lecnam.net

- Définir et rédiger les protocoles de validation informatique pour la qualification d’un composant du Système d’Information
- Coordonner les essais décrits dans les protocoles de validation et de qualification
- Investiguer sur les déviations
- Proposer et exécuter les mesures correctives
- Rédiger les rapports de qualification
- Piloter des projets informatiques
- Communiquer sur le projet en français ou en anglais
- Participer aux choix de progiciels, d’outils et/ou de technologies
- Assurer le rôle de support et d’assistance auprès des équipes informatiques dans le cadre de son périmètre d’expertise
- Rédiger des politiques de sécurité
- Mettre en œuvre des politiques de sécurité en installant ou en mettant à jour des équipements et logicielles de sécurité
- Administrer des dispositifs de Sécurité Opérationnelle en Services Managés
- Mettre en place un processus de supervisions avant incidents et post-mortem
- Résoudre des incidents de sécurité

# Enseignements

| | |
|---|---|
| Outils mathématiques pour Informatique | UTC501 |
| Principes fondamentaux des Systèmes d'exploitation | UTC502 |
| Paradigmes de programmation | UTC503 |
| Systèmes d'Information et Bases de Données | UTC504 |
| Introduction à la cyberstructure de l'internet : réseaux et sécurité | UTC505 |

1 UE au choix d'anglais à choisir parmi

| | |
|---|---|
| Anglais général pour débutants | ANG100 |
| Anglais professionnel | ANG330 |

1 UE de cybersécurité à choisir parmi :

| | |
|---|---|
| Sécurité des réseaux | RSX112 |
| Contrôle d'accès et Gestion des identités numériques | CYB105 |
| Cybersécurité : référentiel, objectifs et déploiement | SEC101 |

1 UE de réseaux informatiques à choisir parmi :

| | |
|---|---|
| Réseaux et protocoles pour l'Internet | RSX101 |
| Technologies pour les applications en réseau : contribution au profil NetDevOps | RSX102 |

1 UE d'ouverture à choisir parmi :

| | |
|---|---|
| Modélisation, optimisation, complexité et algorithmes | RCP105 |
| Recherche opérationnelle et aide à la décision | RCP101 |
| Systèmes d'exploitation : principes, programmation et virtualisation | SMB101 |
| Systèmes de gestion de bases de données | NFP107 |
| Systèmes d'information web | NFE114 |
| Introduction à la gestion de données à large échelle | NFE115 |
| Méthodologies des systèmes d'information | NFE108 |
| Linux : principes et programmation | NSY103 |

| | |
|---|---|
| Architectures des systèmes informatiques | NSY104 |
| Applications réparties | NSY014 |
| Génie Logiciel et Architecture Cloud Native | GLG105 |
| Programmation Fonctionnelle : des concepts aux applications web | NFP119 |
| Programmation avancée | NFP121 |

| | |
|---|---|
| Conduite d'un projet informatique | NSY115 |

2 UE de cybersécurité avancée à choisir parmi :

| | |
|---|---|
| Sécurité des réseaux | RSX112 |
| Menaces informatiques et codes malveillants : analyse et lutte | SEC102 |
| Durcissement et mise en œuvre de mesures de sécurité avancées pour les données, les réseaux et les systèmes (Hardening) | CYB108 |
| Contrôle d'accès et Gestion des identités numériques | CYB105 |

1 UE de gestion de la qualité à choisir parmi :

| | |
|---|---|
| Évaluation de performances | RCP103 |
| ITIL et la gestion des services des systèmes d'information | NFE155 |
| Audit des systèmes d'information | NFE130 |
| Test et Validation du Logiciel | GLG101 |
| Optimisation en informatique | RCP104 |
| Programmation orientée objet en Python, Java et autres | NFP101 |

1 UE d'ouverture à choisir parmi :

| | |
|---|---|
| Architecture d'Entreprise et Urbanisation des Systèmes d'Information | NFE107 |
| Ingénierie des processus et systèmes d'information | NFE109 |
| Réseaux mobiles et sans fil | RSX116 |
| Systèmes et applications répartis pour le cloud | SMB111 |
| Conception et urbanisation de services réseau | RSX103 |

12 crédits à choisir parmi :

| | |
|---|---|
| Conception et facilitation d'ateliers collaboratifs | CCE208 |

| | |
|---|---|
| Droit du numérique | DNT104 |
| Management de projet | GDN100 |
| Coaching et dynamiques collaboratives des équipes d'innovation | GDN209 |
| Union européenne : enjeux et grands débats | UEU001 |
| Mondialisation et Union européenne | UEU002 |
| Droit du travail : relations individuelles | DRS101 |
| Organisation du travail et des activités | DSY005 |
| Démarches et outils de l'organisateur | DSY006 |
| Théories & formes des organisations | DSY103 |
| Mercatique I : Les Etudes de marché et les nouveaux enjeux de la Data à l'heure de l'IA | ESC101 |
| Management et organisation des entreprises | MSE102 |
| Management social et humain | TET101 |
| Management d'équipe et communication en entreprise | TET102 |
| Analyse des données : méthodes descriptives | STA101 |

| | |
|---|---|
| Test anglais | UA2B40 |
| Expérience professionnelle et rapport d'activité | UAAL0V |

# Blocs de compétences

| Code, N° et intitulé du bloc | Liste de compétences |
| --- | --- |
| CRN08B10<br><br>RNCP38461BC01<br><br>Concevoir un composant informatique utilisable dans l'infrastructure applicative, système, technique ou de la sécurité d'un Système d'Information d'une entreprise | Analyser le/les sous-système(s) du système d'information concerné par le composant informatique à concevoir afin de comprendre son intérêt, rôle, interactions avec le sous –système.<br><br>Participer à l'organisation et l'animation des réunions de travail en anglais ou en français afin d'apporter son concours au recueil des exigences/besoins des utilisateurs (exigences métiers).<br><br>Recueillir, en s'appuyant sur les méthodes et outils d'analyse (approche par les buts, ..) des besoins, les exigences de toutes les parties prenantes (exigences fonctionnelles et non-fonctionnelles) associées au composant informatique à concevoir.<br><br>Vérifier la conformité des exigences/besoins identifiés avec les normes (ISO27000x,…) et réglementations (RGPD, règlementation liée à l'accessibilité ..) en vigueur dans le contexte national et international de l'entreprise.<br><br>Traduire les exigences fonctionnelles et non fonctionnelles du métier dans un langage formel ou semi-formel (UML,…) en utilisant des méthodes de spécification des besoins afin de s'assurer de leur compréhension, leur clarté, leur exhaustivité, et de leur cohérence.<br><br>Participer à la rédaction, en anglais ou en français, du cahier des charges du composant informatique à concevoir en s'appuyant sur les modèles standards (normes ISO29148,…) en vigueur dans l'entreprise. |

| Code, N° et intitulé du bloc | Liste de compétences |
| --- | --- |
| CRN08B20<br><br>RNCP38461BC02<br><br>Développer, tester et intégrer un composant informatique dans l'infrastructure applicative, système, technique ou de sécurité d'un Système d'Information d'une entreprise | Préparer la mise en œuvre d'une solution technique détaillée (réunir les logiciels, choisir les outils et les paramétrer, rédiger les procédures …) afin de réaliser une solution technique.<br><br>Mettre en œuvre une solution technique associée à un composant informatique du SI et documentée dans une spécification technique, en agissant dans le respect des normes de développement (ex. qualité) et du cahier des charges et en suivant une méthodologie de construction afin de produire le composant.<br><br>Elaborer les tests et rédiger les cahiers de tests en transcrivant les exigences fonctionnelles et non fonctionnelles sous forme de cas de tests et en s'aidant de méthodes de tests appropriées (test d'intrusion, test de vulnérabilité, les tests unitaires, tests d'intégration ,…) afin de valider la solution technique produite.<br><br>Exécuter, ou faire exécuter par son équipe, les différents tests unitaires en analysant le comportement d'un composant ou des éléments constituants le composant à l'aide d'outils (WireShark, Kali linux, OWASP, …) afin d'identifier d'éventuelles anomalies et de définir les réajustements à faire pour chacune des anomalies détectées.<br><br>Appliquer les réajustements proposés par son équipe ou par un partenaire dans le respect des exigences afin de produire ou faire produire une nouvelle version de tout ou partie du composant.<br><br>Intégrer le composant développé dans son environnement d'exploitation, tout en respectant les procédures établies et le cahier de charges afin de le rendre opérationnel au sein du SI.<br><br>Vérifier l'exploitabilité du composant développé et intégré sous un environnement de pré-production afin de le rendre opérationnel au sein du Système d'information. |

| Code, N° et intitulé du bloc | Liste de compétences |
| --- | --- |
| CRN08B30<br><br>RNCP38461BC03<br><br>Analyser et qualifier l'infrastructure applicative, système, technique ou de sécurité d'un Système d'Information d'une entreprise | Mettre en place des solutions de recueil des incidents pouvant survenir sur l'infrastructure applicative (Request Tracker, ITop, GLPI,etc…), des tableaux de bord de suivi des incidents et de qualité des infrastructures applicatives de l'entreprise afin de répondre et traiter les incidents de l'infrastructure applicative (lenteur de réponse d'application, dysfonctionnement ou crash de d'application, etc ...).<br><br>Analyser les incidents (indisponibilité des ressources, problème de transfert de données, etc..) survenus sur un composant de l'infrastructure applicative en s'appuyant sur des méthodes d'analyse des incidents appropriées ( ITIL,etc ..) afin d'y remédier.<br><br>Résoudre ou faire résoudre par son équipe tout signalement d'incidents survenus dans l'infrastructure applicative (correction de bug, optimisation d'une base, révision de l'interface utilisateur, ,), en tenant compte de l'analyse effectuée préalablement afin de rétablir et de garantir la continuité du service offert.<br><br>Appliquer ou faire appliquer par son équipe les directives de sécurité associées à l'infrastructure applicative (déploiement des mises à jour, chiffrement des données, anonymisation des données sensibles, sauvegarde, gestion des droits d'accès aux applicatifs, … etc ) afin de garantir la continuité du service offert.<br><br>Échanger avec les utilisateurs (entretiens, enquêtes) sur les applicatifs afin de recueillir les améliorations qu'ils souhaitent (ergonomie des interfaces, amélioration du temps de réponse des applicatifs,).<br><br>Gérer le portefeuille applicatif (montée des versions, ajout de fonctionnalités, révision du paramétrage d'un progiciel, migration, etc.), en appliquant les améliorations souhaitées par les utilisateurs afin de maintenir leur satisfaction ou en s'appuyant sur les indicateurs et axes d'analyse dans les différents domaines liés à l'exploitation du logiciel.<br><br>Assurer une veille technologique sur les composants stratégiques de l'infrastructure applicative (les systèmes de gestion de bases de données, des solutions métier) afin de répondre à des besoins futurs (montée en version des logiciels, ergonomie et accessibilité de l'interface, automatisation des fonctionnalités de l'infrastructure applicative).<br><br>Assurer ou coordonner la maintenance corrective des applicatifs afin de garantir la continuité des services offerts par les applicatifs.<br><br>Optimiser l'organisation et les performances des composants de l'infrastructure applicative en réalisant des statistiques des performances d'accès (optimisation des requêtes d'accès aux bases de données, etc) afin de maintenir la qualité de service préconisée. |

| Code, N° et intitulé du bloc | Liste de compétences |
| --- | --- |
| CRN08B63<br><br>RNCP38461BC06<br><br>Maintenir les conditions de sécurité d'un système d'information et de son infrastructure de sécurité | Mettre en place des solutions de supervision des infrastructures de sécurité de l'entreprise (outils SIEM tel que : splunk, ELK, IDS...) afin de répondre et traiter incidents de sécurité (déni de service, intrusions, ..).<br><br>Réaliser une veille sur les vulnérabilités (logicielles et matérielles) des composants de l'infrastructure informatique afin de se conformer à la politique de sécurité (appliquer les mises à jour sur les systèmes informatiques de l'entreprise tel que : PATCH de sécurité, renforcement des authentifications, ETC,..).<br><br>Analyser les incidents de sécurité à partir de traces ou de codes informatiques (codes malveillants, journaux d'évènements,) survenus sur un composant de l'infrastructure informatique en s'appuyant par exemple sur des méthodes d'analyse inverse automatisées tel que : le « fuzzing » d'analyse de codes binaires ou manuelles tel que l'analyse statique afin d'y remédier.<br><br>Anticiper les incidents de sécurité, au moyen d'outils de la cyber threat intelligence (OpenCTI) et en appréhendant les nouvelles menaces et contremesures afin d'assurer le maintien des conditions opérationnelles de sécurité et de prendre en compte les évolutions liées aux menaces émergentes et systémiques (stuxnet, pegasus, rançongiciels, phishing,).<br><br>Assurer ou coordonner la réponse à un incident de sécurité par exemple en situation de crise afin de garantir la continuité ou la reprise des services offerts par le système d'information de l'entreprise.<br><br>Optimiser les infrastructures de sécurité en réalisant des campagnes de métrologie et/ou audits (mettre à niveau et faire évoluer les règles de parefeux, mettre à niveau les règles de corrélation des SIEM, …) afin de maintenir les conditions de sécurité préconisée. |

| Code, N° et intitulé du bloc | Liste de compétences |
| --- | --- |
| CRN08B70<br><br>RNCP38461BC07<br><br>Analyser, organiser et piloter des projets informatiques de développement d'une infrastructure applicative, système, technique ou de sécurité d'un Système d'Information d'une entreprise. | Analyser les caractéristiques du projet (objectifs, contraintes, risques, contexte, …) afin de définir le planning de réalisation du projet (ordonnancement et échéances des actions, ..).<br><br>Participer aux choix de progiciels, d'outils et/ou de technologies, en veillant au respect du cahier des charges, en réalisant une veille technologique et en mobilisant des expertises afin d'assurer la réussite du projet.<br><br>Utiliser les méthodes gestion de projet (cycle en V, méthodes AGILE, …) et outils (JIRA, CONFLUENCE, diagramme de Gantt, ..) en veillant au respect du cahier des charges et au respect des exigences de qualité et de sécurité ainsi qu'au respect des réglementations en vigueur (PCI DSS, RGPD, …) afin de piloter des projets de développement informatique.<br><br>Communiquer régulièrement à l'oral et à l'écrit sur l'état d'avancement du projet et les aléas potentiels (délais, couts, volume et qualité des fonctionnalités) à sa hiérarchie ou au donneur d'ordres en interne et externe, en anglais ou en français, en fonction de l'interlocuteur (l'équipe de projet et/ou la maîtrise d'ouvrage).<br><br>Animer une petite équipe d'un à six informaticiens (fixer des objectifs, répartir l'activité, motiver, évaluer, etc.), en s'appuyant sur des méthodes de gestion d'équipes et des outils collaboratifs (Daily meeting, scrum board,..) afin de répondre à une demande de développement ou de déploiement d'un composant.<br><br>Mettre en place et affecter à chaque collaborateur de l'équipe les actions à réaliser dans le cadre du projet en tenant compte des objectifs du projet (qualitatifs et quantitatifs) et des compétences de chacun afin de mener à terme un projet de conception/ développement/évolution d'un composant d'infrastructure applicative, système, technique ou de sécurité d'un Système d'Information d'une entreprise.<br><br>Assurer le rôle de support technique et d'assistance auprès des équipes informatiques dans le cadre de son périmètre d'expertise (assistance en cas de blocage, élaboration de supports de formation, tutoriels d'intégration et utilisation, FAQ, ..) afin de garantir la qualité technique du projet.<br><br>Assurer et adapter la communication interne et externe, en anglais ou en français, en fonction de l'interlocuteur (l'équipe de projet et/ou la maîtrise d'ouvrage).<br><br>Appliquer, en lien avec la cellule handicap / service RH de l'entreprise, les procédures et aménagements adaptées à la situation des personnes en situation de handicap intégrées dans le projet (postes de travail, moyens de communication, outils de collaboration et de communication adaptés,…) au regard des éventuels préconisations émises par le médecin du travail afin de structurer la prise en compte du handicap au sein de l'équipe informatique.<br><br>Rédiger en français ou en anglais de l'ensemble des livrables du projet (manuels d'utilisation, manuels d'intégration, manuel de déploiement, manuels d'exploitation, etc. ) afin d'en assurer l'utilisation optimale par les entités cible de l'entreprise ( exploitants, équipe de la mise en production, utilisateurs du service et/ou de l'application,/ du composant informatique,…). |