

Ingénieur systèmes, réseaux et cybersécurité

RNCP38117 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326
Formacode(s)	31034, 24231, 31006, 31094, 31009
Code(s) ROME	M1802, M1804
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	18/10/2023
Date d'échéance	18/10/2028

Certificateur(s)

INSTITUT EUROPEEN F 2I · SIRET : 41904518200013

INSTITUT EUROPEEN F 2I · SIRET : 41904518200054

<https://www.institut-f2i.fr/>

Partenaires habilités

8 organismes habilités, d'après la liste publiée par France compétences : 8 à former.

Organisme	SIRET	Habilitation
DORANCO ESPACE MULTIMEDIA	38935885400054	Former
INSTITUT DU MARAIS - CHARLEMAGNE - POLLES	52840171400027	Former
LYCEE TECHNIQUE PRIVE ICOF	77988346100013	Former
M2S CAMPUS	82175021300034	Former
OGEC SAINT CHARLES SAINTE CROIX	79515810400013	Former
OGEC STE CATHERINE	78633676800035	Former
PRO SYSTEMES	37789199900023	Former
UFIP-IBF	41787833700043	Former

Résumé de la certification

OBJECTIFS ET CONTEXTE

Le fonctionnement de tout système d'information dépend de la qualité de la disponibilité de son réseau informatique. Afin d'optimiser le rendement en matière de qualité de services, de sécurité, de gestion des applications par lot, d'applications interactives et en temps réels, les réseaux sont omniprésents et deviennent de plus en plus complexes avec notamment les logiciels SDN, l'internet des objets (IoT) et d'autres technologies.

L'Ingénieur systèmes réseaux et cybersécurité est responsable de la mise en place, de l'intégration et de la maintenance des matériels et logiciels d'un système d'exploitation sur des serveurs internes ou situés dans des data centers hors de l'entreprise. Il peut intervenir dans le cadre de la mise en service de plateformes informatiques et de traitements distants, à la demande et mutualisés. Il définit les besoins et l'architecture informatique de l'entreprise. Il est garant du bon fonctionnement, de la stabilité et de la qualité du réseau, participe à son évolution, pilote l'accès

aux utilisateurs et assure l'équilibre entre le matériel, l'intégralité du système et les logiciels associés.

De manière générale, la fonction d'Ingénieur systèmes, réseaux et cybersécurité varie selon le type de structure et l'organisation de la DSI de l'entreprise, on peut distinguer trois types d'activités : il peut travailler pour des entreprises, des constructeurs ou pour des SSII.

ACTIVITÉS VISÉES

Mise en œuvre d'un processus d'audits des systèmes et réseaux d'une organisation

Analyse critique des architectures systèmes et réseaux existantes

Définir l'architecture systèmes et réseaux de l'organisation adaptée aux besoins et aux contraintes définis en amont du projet

Expertise et formulation de recommandations pertinentes des systèmes et réseaux

Conception d'une stratégie de développement des systèmes et réseaux sécurisée

Pilotage de la conception de l'infrastructure systèmes et réseaux sécurisée

Mise en place de la stratégie de configuration de routage

Mise en place de la stratégie de paramétrage des serveurs

Pilotage du déploiement de l'environnement logiciels et applicatifs

Analyse et prévention des risques d'intrusion et de rupture des systèmes et réseaux

Définition de la stratégie de paramétrage des équipements de sécurité

Gestion des comptes et contrôle des accès

Mise en place d'un processus de protection des données au repos et en transit

Définition des critères de mesure de la performance des systèmes et réseaux

Analyse des résultats de mesure de la performance

Optimisation de la performance de l'infrastructure systèmes et réseaux

Management des équipes intervenant sur les systèmes et les réseaux

Pilotage des projets de développement des organisations

Identification des évolutions probables dans l'utilisation des systèmes et réseaux de l'entreprise

Évaluation des investissements nécessaires

Accompagnement à la conduite du changement auprès des utilisateurs

Utilisation de l'anglais technique dans son activité professionnelle

COMPÉTENCES ATTESTÉES

Mettre en œuvre un processus d'audit des systèmes et réseaux en s'appuyant sur la mise en place d'une méthodologie d'inventaire et la planification des tests de l'architecture informatique, en coordonnant les équipes informatiques et les utilisateurs concernés afin de déterminer les modes d'utilisation des systèmes et réseaux par les parties prenantes internes et externes à l'entreprise.

Évaluer les architectures systèmes réseaux existantes, selon une méthodologie d'évaluation, au regard des besoins et comportements des utilisateurs identifiés, en exploitant les schémas et données techniques, afin d'identifier les failles et améliorations possibles du service rendu, et conseiller la Direction informatique sur des évolutions et solutions en techniques nouvelles.

Réaliser les entretiens d'audit organisationnel en prenant en compte tous les besoins des parties prenantes, en analysant les modes de circulation de l'information au sein de l'entreprise et les échanges avec l'extérieur (clients, fournisseurs, etc.) et en sélectionnant les ressources matérielles et logicielles (machines locales, externes, en cloud) afin de définir une infrastructure systèmes et réseaux adaptée.

Spécifier les besoins et comportements des utilisateurs en s'appuyant sur la description des scénarii utilisateurs, l'identification des besoins afin de déterminer les types de systèmes et réseaux adaptés (local, à distance, sans fil, etc.) aux besoins exprimés par les parties prenantes.

Concevoir une stratégie de développement des systèmes et réseaux conforme aux besoins exprimés, aux objectifs de la structure, et à la réglementation en matière de sécurisation informatique, de cybersécurité, d'éthique, de green IT et d'accessibilité, en s'appuyant sur l'audit organisationnel et technique, afin d'anticiper sur les besoins présents et futurs des différentes parties prenantes.

Piloter la conception d'une infrastructure systèmes et réseaux sécurisée en maîtrisant la méthodologie de conception des architectures systèmes et réseaux, en mobilisant les équipements réseaux en charge de la disponibilité des machines et des services, en respectant les recommandations techniques des constructeurs et les caractéristiques matérielles en termes de capacité ainsi que le budget afin de répondre aux besoins du projet défini.

Mettre en place une stratégie de configuration des protocoles de routage adaptés aux configurations, en se conformant aux besoins des utilisateurs et aux règles de sécurité informatique en vigueur, en vue de déterminer le

raccordement des postes à un ou plusieurs serveurs.

Analyser l'activité des serveurs et des réseaux, en se basant sur une analyse fonctionnelle de l'activité, le respect du schéma général de routage ainsi que la maîtrise de la notion de continuité d'activité ou de service en vue de mettre en place une stratégie de paramétrage des serveurs conforme aux configurations.

Mettre en place une stratégie de paramétrage des serveurs à partir des indicateurs définis, de l'estimation prévisionnelle des usages (capacity planning), de la quantification et de la hiérarchisation des risques de rupture afin d'anticiper les risques de rupture et ainsi garantir la disponibilité des serveurs.

Piloter le déploiement de l'environnement logiciels et applicatifs en analysant la compatibilité des applications et des logiciels utilisés avec les systèmes d'exploitation et le matériel utilisé, afin de prévenir les risques de dysfonctionnement et d'assurer la continuité de l'activité (PCA).

Recenser les points de vulnérabilité de l'architecture informatique, en s'appuyant sur la mise en œuvre des normes et recommandations notamment en matière de cybersécurité afin de définir des processus de gestion de crise et ainsi anticiper tout type d'incident sur les systèmes et réseaux informatiques de l'entreprise.

Utiliser des scénarii d'attaques de réseaux, selon les recommandations de l'ANSSI, en mettant en place des alertes adaptées aux risques, en définissant des processus de gestion de crise, en élaborant un processus de bascule adaptées aux configurations sur les réseaux secondaires et en formant les équipes informatiques et les utilisateurs afin de prévenir les risques en matière de sécurité.

Délimiter des zones de sensibilité en se basant sur une cartographie des zones réseaux, la mise en œuvre des systèmes d'alarmes et de protection intégrés au système d'information afin de définir une stratégie de paramétrage des équipements de sécurité.

Analyser les besoins de connexions des différentes catégories d'utilisateurs en prenant en compte les tailles et types de données, en vue de superviser le paramétrage des accès aux réseaux de l'entreprise, dans des conditions de sécurité optimales.

Analyser les possibilités d'accès à distance à partir d'un recensement exhaustif, par l'équipe systèmes et réseaux, afin de sélectionner des protocoles adaptés aux besoins des utilisateurs (taille et types de données partagées etc.).

Identifier les failles du logiciel de messagerie en se basant sur les risques de piratages des comptes et des données, en définissant des chaînes d'authentification uniques (fédération d'identité, Single Sign-On (SSO)) et l'architecture logique des services d'identité (IAM, forêts, domaines et relations d'approbation Active Directory) en vue de mettre en place un processus de prévention et de sensibiliser les utilisateurs aux bonnes pratiques de protection et de prévention des intrusions informatiques.

Mettre en place un processus de protections des données au repos et en transit en définissant des formats et des modalités de stockage et d'archivage des données, en configurant les bases de données en respectant la réglementation en vigueur (Règles de sécurisation, RGPD, etc.), en s'assurant de l'adéquation des plateformes d'échange, de transfert et de partage de fichiers et de données dans le but de répondre à des besoins logistiques et opérationnels.

Analyser les besoins de protection de données en ayant recourt à la méthodologie d'analyse, en respectant les normes en vigueur et recommandations en matière de sécurisation des données en vue de rechercher et mettre en œuvre des solutions de cryptage adaptées.

Définir des critères de mesure de la performance des systèmes et réseaux en mobilisant les méthodes de tests de mesure de performance, en élaborant des outils de mesure de performance et en définissant des métriques pertinentes et leurs seuils d'alerte afin de mesurer les performances de systèmes et réseaux informatiques.

Analyser les niveaux de performance de l'infrastructure des systèmes et réseaux en se basant sur les indicateurs des niveaux/seuils de performance, le choix des référentiels théoriques, l'analyse et la présentation des résultats et les capacités de commutation théoriques afin d'évaluer les systèmes et réseaux d'organisations et ainsi identifier les problèmes récurrents.

Optimiser la performance de l'infrastructure systèmes et réseaux en étudiant les risques éventuels de modification des systèmes et réseaux, les résultats de mesures de performance pour identifier les zones de défaillance afin de proposer des mesures correctives automatisées dans le cadre du processus d'amélioration continue.

Estimer les possibilités de gains de performances des systèmes et réseaux en se basant sur les risques éventuels de modification de réseaux et systèmes, la localisation des zones de défaillance en vue de concevoir et d'organiser des interventions d'amélioration de la performance des systèmes et réseaux informatiques.

Analyser les coûts et les risques éventuels de modification des systèmes et réseaux en analysant les conditions de mise en place d'axes d'amélioration afin de conseiller des décideurs.

Manager les équipes qui interviennent sur les systèmes et réseaux en établissant un planning projet présentant les risques éventuels de modification de systèmes et réseaux, en définissant les feuilles de route des membres de

l'équipe, en recensant les compétences nécessaires, en mettant en œuvre la méthode agile afin de mobiliser des ressources compétentes sur des étapes déterminées.

Analyser les évolutions programmées de besoins ou d'activités à partir d'une méthodologie d'études, d'analyse des enjeux du développement de nouvelles solutions systèmes et réseaux dans le but d'identifier les modifications d'architecture à effectuer et ainsi rédiger le cahier des charges relatifs aux types de solutions recherchées.

Réaliser des enquêtes auprès d'utilisateurs types en respectant la méthodologie d'enquête afin d'identifier des besoins en termes d'intégration de fonctionnalités ou de possibilités d'utilisation spécifiques.

Réaliser des études de faisabilité en prenant en compte les enjeux stratégiques et financiers pour évaluer des possibilités de développement et de mise en place de solutions spécifiques sécurisées.

Estimer des coûts de mise en place et de maintenance sur la durée du cycle de vie des systèmes et réseaux en prenant en comptes les besoins de l'entreprise pour les intégrer aux budgets prévisionnels d'investissements.

Anticiper des conséquences d'interventions sur les systèmes et réseaux en se basant sur la méthodologie d'accompagnement du changement (rédaction et diffusion des compte-rendu, documentation) pour élaborer des programmes d'accompagnement adaptés des utilisateurs.

Identifier des besoins de formation des utilisateurs des systèmes et réseaux à travers une analyse des compétences afin de programmer des sessions de formations

individuelles ou collectives adaptées et inclusives.

Maîtriser l'anglais technique dans son activité professionnelle afin de mener une veille efficace et comprendre une information technique relative à l'infrastructure systèmes et réseaux en anglais.

Blocs de compétences

RNCP38117BC01 — PILOTER LA CONCEPTION D'UNE INFRASTRUCTURE SYSTEMES, RESEAUX SECURISEE ET RESPECTUEUSE DE LA POLITIQUE RSE D'UNE ORGANISATION

LISTE DE COMPÉTENCES

Mettre en œuvre d'un processus d'audit des systèmes et réseaux en s'appuyant sur la mise en place d'une méthodologie d'inventaire et la planification des tests de l'architecture informatique, en coordonnant les équipes informatiques et les utilisateurs concernés afin de déterminer les modes d'utilisation des systèmes et réseaux par les parties prenantes internes et externes à l'entreprise.

Evaluer les architectures systèmes réseaux existantes, selon une méthodologie d'évaluation, au regard des besoins et comportements des utilisateurs identifiés, en exploitant les schémas et données techniques, afin d'identifier les failles et améliorations possibles du service rendu, et conseiller la Direction informatique sur des évolutions et solutions en techniques nouvelles.

Réaliser les entretiens d'audit organisationnel en prenant en compte tous les besoins des parties prenantes, en analysant les modes de circulation de l'information au sein de l'entreprise et les échanges avec l'extérieur (clients, fournisseurs, etc.) et en sélectionnant les ressources matérielles et logicielles (machines locales, externes, en cloud) afin de définir une infrastructure systèmes et réseaux adaptée.

Spécifier les besoins et comportements des utilisateurs en s'appuyant sur la description des scénarii utilisateurs, l'identification des besoins afin de déterminer les types de systèmes et réseaux adaptés (local, à distance, sans fil, etc.) aux besoins exprimés par les parties prenantes.

Concevoir une stratégie de développement des systèmes et réseaux conforme aux besoins exprimés, aux objectifs de la structure, et à la réglementation en matière de sécurisation informatique, de cybersécurité, d'éthique, de green IT et d'accessibilité, en s'appuyant sur l'audit organisationnel et technique, afin d'anticiper sur les besoins présents et futurs des différentes parties prenantes.

Piloter la conception d'une infrastructure systèmes et réseaux sécurisée en maîtrisant la méthodologie de conception des architectures systèmes et réseaux, en mobilisant les équipements réseaux en charge de la disponibilité des machines et des services, en respectant les recommandations techniques des constructeurs et les caractéristiques matérielles en termes de capacité ainsi que le budget afin de répondre aux besoins du projet défini.

MODALITÉS D'ÉVALUATION

Evaluation n°1 - Mise en situation professionnelle (C1 à C6) : Mise en œuvre d'un processus d'audit des systèmes et réseaux informatiques de l'organisation

RNCP38117BC02 — SUIVRE ET METTRE EN ŒUVRE LE DEPLOIEMENT DE L'INFRASTRUCTURE SYSTEMES ET RESEAUX SECURISEE ADAPTEE AUX BESOINS

LISTE DE COMPÉTENCES

Mettre en place une stratégie de configuration des protocoles de routage adaptés aux configurations, en se conformant aux besoins des utilisateurs et aux règles de sécurité informatique en vigueur, en vue de déterminer le raccordement des postes à un ou plusieurs serveurs.

Analyser l'activité des serveurs et des réseaux, en se basant sur une analyse fonctionnelle de l'activité, le respect du schéma général de routage ainsi que la maîtrise de la notion de continuité d'activité ou de service en vue de mettre en place une stratégie de paramétrage des serveurs conforme aux configurations.

Mettre en place une stratégie de paramétrage des serveurs à partir des indicateurs définis, de l'estimation prévisionnelle des usages (capacity planning), de la quantification et de la hiérarchisation des risques de rupture afin d'anticiper les risques de rupture et ainsi garantir la disponibilité des serveurs.

Piloter le déploiement de l'environnement logiciels et applicatifs en analysant la compatibilité des applications et des logiciels utilisés avec les systèmes d'exploitation et le matériel utilisé, afin de prévenir les risques de dysfonctionnement et d'assurer la continuité de l'activité (PCA).

MODALITÉS D'ÉVALUATION

Evaluation n°2 – Mise en situation professionnelle (C7 à C10) : Gérer un projet de configuration de tout ou partie d'un système et réseaux d'entreprise.

RNCP38117BC03 — ELABORER LA STRATEGIE DE SECURISATION DE L'INFRASTRUCTURE INFORMATIQUE

LISTE DE COMPÉTENCES

Recenser les points de vulnérabilité de l'architecture informatique, en s'appuyant sur la mise en œuvre des normes et recommandations notamment en matière de cybersécurité afin de définir des processus de gestion de crise et ainsi anticiper tout type d'incident sur les systèmes et réseaux informatiques de l'entreprise.

Utiliser des scénarii d'attaques de réseaux, selon les recommandations de l'ANSSI, en mettant en place des alertes adaptées aux risques, en définissant des processus de gestion de crise, en élaborant un processus de bascule adaptées aux configurations sur les réseaux secondaires et en formant les équipes informatiques et les utilisateurs afin de prévenir les risques en matière de sécurité.

Délimiter des zones de sensibilité en se basant sur une cartographie des zones réseaux, la mise en œuvre des systèmes d'alarmes et de protection intégrés au système d'information afin de définir une stratégie de paramétrage des équipements de sécurité.

Analyser les besoins de connexions des différentes catégories d'utilisateurs en prenant en compte les tailles et types de données, en vue de superviser le paramétrage des accès aux réseaux de l'entreprise, dans des conditions de sécurité optimales.

Analyser les possibilités d'accès à distance à partir d'un recensement exhaustif, par l'équipe systèmes et réseaux, afin de sélectionner des protocoles adaptés aux besoins des utilisateurs (taille et types de données partagées etc.).

Identifier les failles du logiciel de messagerie en se basant sur les risques de piratages des comptes et des données, en définissant des chaînes d'authentification uniques (fédération d'identité, Single Sign-On (SSO)) et l'architecture logique des services d'identité (IAM, forêts, domaines et relations d'approbation Active Directory) en vue de mettre en place un processus de prévention et de sensibiliser les utilisateurs aux bonnes pratiques de protection et de prévention des intrusions informatiques.

Mettre en place un processus de protections des données au repos et en transit en définissant des formats et des modalités de stockage et d'archivage des données, en configurant les bases de données en respectant la réglementation en vigueur (Règles de sécurisation, RGPD, etc.), en s'assurant de l'adéquation des plateformes d'échange, de transfert et de partage de fichiers et de données dans le but de répondre à des besoins logistiques et opérationnels.

Analyser les besoins de protection de données en ayant recourt à la méthodologie d'analyse, en respectant les normes en vigueur et recommandations en matière de sécurisation des données en vue de rechercher et mettre en œuvre des solutions de cryptage adaptées.

MODALITÉS D'ÉVALUATION

Evaluation n°3 : Mise en situation professionnelle (C11 à C18) : Analyse de la sécurité d'un système et réseau d'entreprise

RNCP38117BC04 — MANAGER LA PERFORMANCE DES SYSTEMES ET RESEAUX D'UNE ORGANISATION

LISTE DE COMPÉTENCES

Définir des critères de mesure de la performance des systèmes et réseaux en mobilisant les méthodes de tests de mesure de performance, en élaborant des outils de mesure de performance et en définissant des métriques pertinentes et leurs seuils d'alerte afin de mesurer les performances de systèmes et réseaux informatiques.

Analyser les niveaux de performance de l'infrastructure des systèmes et réseaux en se basant sur les indicateurs des niveaux/seuils de performance, le choix des référentiels théoriques, l'analyse et la présentation des résultats et les capacités de commutation théoriques afin d'évaluer les systèmes et réseaux d'organisations et ainsi identifier les problèmes récurrents.

Optimiser la performance de l'infrastructure systèmes et réseaux en étudiant les risques éventuels de modification des systèmes et réseaux, les résultats de mesures de performance pour identifier les zones de défaillance afin de proposer des mesures correctives automatisées dans le cadre du processus d'amélioration continue.

Estimer les possibilités de gains de performances des systèmes et réseaux en se basant sur les risques éventuels de modification de réseaux et systèmes, la localisation des zones de défaillance en vue de concevoir et d'organiser des interventions d'amélioration de la performance des systèmes et réseaux informatiques..

Analyser les coûts et les risques éventuels de modification des systèmes et réseaux en analysant les conditions de mise en place d'axes d'amélioration afin de conseiller des décisionnaires.

Manager les équipes qui interviennent sur les systèmes et réseaux en établissant un planning projet présentant les risques éventuels de modification de systèmes et réseaux, en définissant les feuilles de route des membres de l'équipe, en recensant les compétences nécessaires, en mettant en œuvre la méthode agile afin de mobiliser des ressources compétentes sur des étapes déterminées.

MODALITÉS D'ÉVALUATION

Evaluation n°4 - Mise en situation professionnelle (C19 à C24) : Amélioration des performances d'une infrastructure informatique d'entreprise

RNCP38117BC05 — ELABORER UNE STRATEGIE DE GESTION DES NOUVEAUX PROJETS INFORMATIQUES D'UNE ORGANISATION

LISTE DE COMPÉTENCES

Analyser les évolutions programmées de besoins ou d'activités à partir d'une méthodologie d'études, d'analyse des enjeux du développement de nouvelles solutions systèmes et réseaux dans le but d'identifier les modifications d'architecture à effectuer et ainsi rédiger le cahier des charges relatifs aux types de solutions recherchées.

Réaliser des enquêtes auprès d'utilisateurs types en respectant la méthodologie d'enquête afin d'identifier des besoins en termes d'intégration de fonctionnalités ou de possibilités d'utilisation spécifiques.

Réaliser des études de faisabilité en prenant en compte les enjeux stratégiques et financiers pour évaluer des possibilités de développement et de mise en place de solutions spécifiques sécurisées.

Estimer des coûts de mise en place et de maintenance sur la durée du cycle de vie des systèmes et réseaux en prenant en comptes les besoins de l'entreprise pour les intégrer aux budgets prévisionnels d'investissements.

Anticiper des conséquences d'interventions sur les systèmes et réseaux en se basant sur la méthodologie d'accompagnement du changement (rédaction et diffusion des compte-rendu, documentation) pour élaborer des programmes d'accompagnement adaptés des utilisateurs.

Identifier des besoins de formation des utilisateurs des systèmes et réseaux à travers une analyse des compétences afin de programmer des sessions de formations individuelles ou collectives adaptées et inclusives.

MODALITÉS D'ÉVALUATION

Evaluation n° 5 - Mise en situation professionnelle (C25 à C30) : Elaboration d'une stratégie de gestion des nouveaux projets informatiques

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Le secteur de l'informatique est un secteur en constante évolution, qui englobe de nombreux domaines tels que le développement de logiciels, les systèmes d'information, les réseaux, la cybersécurité, l'intelligence artificielle, la réalité virtuelle, la blockchain, etc. En France, l'industrie informatique est l'un des secteurs les plus dynamiques de

l'économie, avec une forte croissance ces dernières années.

La pandémie de COVID-19 a accéléré la transformation numérique des entreprises, stimulant la demande pour les technologies de l'information et de la communication (TIC). Les entreprises cherchent à moderniser leurs infrastructures, à améliorer l'expérience utilisateur, à développer de nouveaux produits et services numériques, et à protéger leurs données contre les cyberattaques. Par conséquent, les professionnels qualifiés en informatique sont très demandés sur le marché du travail.

Les compétences les plus recherchées dans le secteur de l'informatique en France sont liées aux technologies émergentes, telles que l'intelligence artificielle, la cybersécurité, la blockchain, le cloud computing, la réalité virtuelle et augmentée. Les entreprises recherchent des professionnels qualifiés et créatifs capables d'apporter des solutions innovantes à leurs besoins en matière de technologies de l'information.

Le secteur de l'informatique en France est caractérisé par une forte concurrence, mais également par des salaires compétitifs et de bonnes perspectives de carrière. Les diplômés en informatique peuvent trouver des emplois dans une grande variété d'entreprises, allant des start-ups aux grandes entreprises en passant par les institutions publiques. Les métiers les plus courants dans le secteur de l'informatique comprennent les développeurs de logiciels, les ingénieurs systèmes et réseaux, les analystes de données, les ingénieurs en cybersécurité, les architectes cloud et les chefs de projet informatique.

TYPE D'EMPLOIS ACCESSIBLES

- Ingénieur/ Expert systèmes et réseaux ;
- Ingénieur/Expert réseaux ;
- Ingénieur/Expert systèmes ;
- Architecte réseaux informatiques ;
- Expert en communication et réseaux ;
- Expert réseaux et télécoms ;
- Ingénieur/Expert en sécurité informatique ;
- Ingénieur plateformes de services ;
- Ingénieurs sécurité web ;
- Consultant réseaux informatiques ;
- Responsable sécurité informatique.

RÉGLEMENTATIONS D'ACTIVITÉ

Le métier d'Ingénieur systèmes, réseaux et cybersécurité n'est un métier réglementé. Néanmoins, des contraintes réglementaires s'exercent dans son quotidien (Droits et obligations des normes de sécurisation des données, des réseaux et des systèmes, référentiel général d'interopérabilité (RGI), référentiel général de sécurité (RGS), futur règlement DSA, plan de sécurisation du SI, obligations réglementaires et normatives du marché, RGPD, etc.) mais aussi l'éthique et la prise en compte des situations de handicap.

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)	Très élevée (5/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 4 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible, Lien formation-emploi
Salaire médian (mensuel)	2 795 €
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)	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) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	30 552
Jugés difficiles à recruter	53 %
Emplois saisonniers	1 %
Familles professionnelles (FAP)	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 M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

Être titulaire d'une certification de niveau 6 (EU) ou d'un diplôme équivalent ou disposer d'une expérience professionnelle dans le domaine.

PRÉREQUIS À LA VALIDATION

La certification complète s'obtient par la validation des 5 blocs qui la constituent, complétée de la validation d'une compétence transversale en anglais technique : "Maîtriser l'anglais technique dans son activité professionnelle afin de mener une veille efficace et comprendre une information technique relative à l'infrastructure systèmes et réseaux en anglais", établie par l'évaluation de la capacité du candidat à rédiger un compte-rendu de veille technologique ou réglementaire en français depuis des sources anglophones.

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

Le jury de délivrance de la certification professionnelle est constitué de quatre membres dont :

- trois sont des professionnels extérieurs à l'organisme certificateur avec à minima 2 années d'expérience professionnelle dans le domaine visé par la certification professionnelle, sans lien avec le candidat, n'ayant pas été formateur dans le parcours du candidat, n'appartenant pas à l'organisme certificateur ;
- un représentant de l'organisme certificateur.

Un Président extérieur à l'autorité de certification est désigné(e) par la Directrice Générale de l'Institut Européen F2i.

COMPOSITION DU JURY — VAE

Le jury de délivrance de la certification professionnelle est constitué de quatre membres dont :

- trois sont des professionnels extérieurs à l'organisme certificateur avec à minima 2 années d'expérience professionnelle dans le domaine visé par la certification professionnelle, sans lien avec le candidat, n'ayant pas été formateur dans le parcours du candidat, n'appartenant pas à l'organisme certificateur ;
- un représentant de l'organisme certificateur.

Un Président extérieur à l'autorité de certification est désigné(e) par la Directrice Générale de l'Institut Européen F2i.

Les jurés ainsi qualifiés peuvent occuper les postes suivants :

- Responsable pédagogique de la formation / Directeur pédagogique ;
- Des formateurs ;
- Des professionnels certifiés, qualifiés en gouvernance d'entreprise spécialisée dans le Numérique ;
- Des professionnels expérimentés (au moins 2 ans) dans le secteur d'activité du Numérique,
- Des experts sur les thèmes abordés en formation (universitaires, chercheurs, consultants, salariés de structures spécialisées, ...).

Les jurés sont en activité professionnelle et n'ont pas de lien personnel ni professionnel avec l'un des candidats présentés à la certification, préalablement au passage de l'examen.

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	6 636 €
Selon la branche	6 636 € – 6 885 €
Prise en charge	Branches concernées
6 636 €	Valeur par défaut · 209 branches
6 885 €	CPNE des Télécoms, CPNEF de l'audiovisuel, CPNEFP ICGV entreprises de la viande
6 656 €	CPNEFP des jardineries et graineteries

Base légale

Date de décision	18/10/2023
Durée de l'enregistrement	5 ans
Date d'échéance de l'enregistrement	18/10/2028
Date de dernière délivrance possible	18/10/2032

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2022	95	0	92 %	—
2021	76	1	97 %	79 %
2020	64	1	92 %	80 %
2019	14	0	100 %	93 %

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP36010

CORRESPONDANCES (PAR BLOCS)

RNCP34553, RNCP35612, RNCP35786, RNCP36010, RNCP36197, RNCP36296, RNCP36855

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://www.institut-f2i.fr/formations/ingenieur-reseaux-et-systemes/>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/38117/>

Se former en apprentissage

Formations en apprentissage	7
Organismes gestionnaires (CFA)	5

Organismes formateurs	5
Régions couvertes	4
Départements couverts	4
Organismes certifiés Qualiopi	5
Sessions	de 09/2025 à 07/2028

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