

Ingénieur systèmes, réseaux et cybersécurité

RNCP38105 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326
Formacode(s)	31034, 24231, 31006, 31094, 31009
Code(s) ROME	M1806, M1803, M1805, M1802
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	18/10/2023
Date d'échéance	18/10/2026

Certificateur(s)

AFORP FORMATION (CFAI) · SIRET : 77572845400205

Partenaires habilités

14 organismes habilités, d'après la liste publiée par France compétences : 14 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
ASS DEVELOP APPRENTIS INDUST AQUITAIN	35109084000015	Former et organiser l'évaluation
ASSOCIATION DES NETICIENS	87927861200012	Former et organiser l'évaluation
ASS PROMOTION APPRENTISSAGE INDUSTRIES	39279259400039	Former et organiser l'évaluation
ASS REGION PROMOTION METALLURG	33453316300047	Former et organiser l'évaluation
ASS. SERVICES POUR INDUSTRIE ET COMMERCE	39902242500017	Former et organiser l'évaluation
CFAI ALSACE	38855948600070	Former et organiser l'évaluation
CFAI DE CHAMPAGNE ARDENNE	40120610700039	Former et organiser l'évaluation
CFAI DE CHAMPAGNE ARDENNE	40120610700062	Former et organiser l'évaluation
CFAI DIAFOR	39048242000028	Former et organiser l'évaluation
CFAI REGION NORD PAS-DE-CALAIS	30048880600120	Former et organiser l'évaluation

Liste complète des 14 partenaires habilités : <https://data.aktaconseil.fr/certifications/rncp38105-ingenieur-systemes-reseaux-et-cybersecurite/partenaires>

Résumé de la certification

OBJECTIFS ET CONTEXTE

L'AFORP a considéré très tôt la pertinence d'associer la cybersécurité au cœur même des systèmes d'information et des systèmes industriels.

Trop souvent, les architectes des systèmes d'information (et industriels) sont formés aux techniques du réseau, aux techniques du système, mais peu à la sécurité informatique. Cette dernière est souvent occultée ou non maîtrisée. De plus, la crise du COVID a complètement modifié les habitudes de travail des entreprises avec une explosion du travail à distance, et donc de tous les risques inhérents. Durant cette crise, on a vu (et on continue de voir) exploser le

nombre des attaques informatiques. Ces attaques sont dirigées vers les organismes étatiques, les grandes entreprises, les PME et TPE, mais également vers les collaborateurs travaillant depuis chez eux. En résumé, cette crise a de nouveau démontré, si cela était nécessaire, l'impérieuse urgence de sécuriser toutes les entreprises ayant un système d'information ou étant connectées, et de sensibiliser tous les collaborateurs des entreprises.

Enfin, si la cybersécurité est maintenant omniprésente au cœur des systèmes informatiques, l'intelligence artificielle se fait également une très belle place. Effectivement, aujourd'hui, les approches SDN, SDS, NFV, IBN et SD-WAN bouleversent les approches traditionnelles des réseaux. Elles initient une nouvelle façon de concevoir et d'appréhender les infrastructures réseau des entreprises avec des réductions des coûts, un accroissement de l'agilité, de la flexibilité, et de la rapidité de mise en œuvre et d'adaptation. Les tendances se succèdent et impactent fortement la conception même du réseau. SDN, SDS, NFV, IBN et SD-WAN sont devenus des briques de base pour préparer au mieux son réseau aux défis d'aujourd'hui et de demain.

ACTIVITÉS VISÉES

Les activités menées s'inscrivent dans le cycle de vie des opérations :

- Conception,
- Réalisation et exploitation
- Maintenance des Infrastructures Informatiques
- Sécurisation du système d'information (ISO27000, audits, analyse médico-légale après un crime informatique, remédiation, etc.)
- Evolution de ces infrastructures.

Le métier consiste, après les avoir réalisées, à garantir la disponibilité, l'intégrité, la confidentialité des données contenues dans le SI, ainsi que la performance et la sécurité des infrastructures techniques du Système d'Information de l'entreprise.

Les activités à mener, dans ce cadre, couvrent toutes les phases depuis l'étude et la conception du système jusqu'à la mise en production, l'exploitation et la sécurisation du SI.

Le métier comprend des activités très variées nécessitant de très fortes compétences tant techniques, qu'organisationnelles et humaines. Par exemple, dans le cadre de sa mission, l'Ingénieur systèmes, réseaux et cybersécurité doit être en capacité de :

- Définir l'architecture sécurisée d'un système informatique (compétences principalement techniques)
- Mettre en place un SMSI (Système de Management de la Sécurité Informatique) selon la norme ISO 27000 (compétences principalement organisationnelles)
- Ou encore adapter une infrastructure existante à une réflexion d'écoconception afin de réduire son empreinte énergétique.

Suivant les entreprises et les missions confiées, son métier comprend tout ou partie des activités suivantes :

- Gérer le projet dans sa globalité
- Analyser et formaliser sous forme de spécifications les besoins du client, en proposant éventuellement un prototype (Proof of Concept ou POC), en identifiant des solutions et en définissant la stratégie de tests,
- Concevoir, réaliser, mettre en place et tester une partie ou l'ensemble d'une infrastructure système et réseau concourant à la réalisation d'un système d'information.
- Intégrer les différents composants système et réseau et valider l'ensemble du système d'information pour démontrer qu'il répond correctement aux exigences et aux besoins du client,
- Assurer le déploiement du système d'informations en prenant en considération les aspects de validation et de conduite du changement (formations, coaching, tutorat, etc.),
- Assurer le maintien en condition opérationnelle (maintenance et exploitation) du système en prenant en compte les aspects préventifs, correctifs mais également évolutifs du système. La gestion des matériels et logiciels, en particulier leur obsolescence, est également réalisée dans le cadre de ce maintien en condition opérationnelle,
- Assurer le maintien en condition de sécurité du système en prenant en compte les aspects organisationnels, réglementaires, d'audits, d'analyse médico-légale après un crime informatique (FORENSIC), de remédiation, mais également les aspects d'évolution du système,
- Mettre en place et gérer une cellule de crise à la suite d'un crime informatique

COMPÉTENCES ATTESTÉES

Recueillir et analyser les exigences du client

L'ingénieur systèmes, réseaux et cybersécurité doit être une personne capable d'identifier les besoins et d'obtenir la vue d'ensemble des exigences (transactionnelles, analytiques, formulaires et autres) du client, que celui-ci soit interne ou externe.

Il doit proposer une vision qui consiste à matérialiser et à fixer des objectifs pour le client, et communiquer cette vision aux principales parties prenantes.

Concevoir l'architecture, réaliser et déployer la solution technique

C'est lui qui est en charge de définir et d'argumenter sur la meilleure solution technique possible permettant de répondre aux besoins du client, de traduire ces dernières en spécifications techniques et non techniques, de faire les choix d'architecture, de réaliser l'ensemble des documents techniques, de réaliser un Proof of Concept (PoC), d'intégrer les différents composants du système, puis de déployer ce dernier, d'industrialiser la solution afin de la robustifier et enfin de mettre en place une démarche d'amélioration continue.

Dans ce cadre, il doit connaître et savoir utiliser toutes les innovations techniques et les dernières technologies de son domaine. On peut citer de manière non exhaustive le SD-WAN, l'IBN, le NFV, le SDN, le SDS, le Cloud, les Block Chain, etc...

Maintenir le système en condition opérationnelle et de sécurité

Le MCO ou maintien en condition opérationnelle est l'ensemble des stratégies définies par l'ingénieur systèmes, réseaux et Cybersécurité et nécessaires pour garantir que les applications, les infrastructures et les matériels soient disponibles à tout moment. En effet, les causes de dysfonctionnements sont très nombreuses : incendie, piratage, grève, vols de données ou de matériels, dégâts des eaux...

Le MCO n'est donc pas limité aux seules activités d'entretien et de réparation des différents équipements. Il s'étend à toutes les stratégies à mettre en œuvre pour qu'ils soient toujours performants durant leur cycle de vie, dont notamment le maintien et la prévention des risques.

De la même manière, l'ingénieur systèmes, réseaux et cybersécurité est en charge de la stratégie et de la définition du MCS (Maintien en Condition de Sécurité). Cela consiste pour lui à s'assurer que le profil de sécurité des outils ayant une composante numérique (système d'exploitation, applicatif logiciel, base de données, etc.) soit parfaitement à jour. En clair, il s'agit d'éviter toute tentative de cyberattaques et d'intrusions qui pourraient mettre à mal les données de l'entreprise, sa réputation ou le travail des équipes.

Gérer un projet international

Il doit collaborer avec des spécialistes métiers pluridisciplinaires (architectes, ingénieurs cybersécurité, ingénieurs réseaux, ingénieurs systèmes, ingénieurs de développement, cloud ...), piloter la réalisation du projet, animer ses équipes (conception, développement, tests, intégration, déploiement) et prendre en compte le développement des compétences individuelles et collectives de son équipe.

La gestion de projet doit pouvoir être réalisée indifféremment en langue française ou anglaise et l'ingénieur systèmes, réseaux et cybersécurité doit savoir travailler et tirer profit d'une équipe multiculturelle au sein de son projet.

Capitaliser l'expérience et le savoir-faire dans la réalisation de solutions

Il contribue à rendre la création d'un système IT (Système d'Information d'Entreprise) ou OT (Système d'Information Industriel) plus rapide, plus facile, plus fiable et moins coûteuse, en développant un processus qui intègre l'expérience de son projet et les meilleures pratiques accumulées dans le recueil du besoin client, ainsi que la conception, le développement, l'intégration, le déploiement et l'exploitation des solutions mises en place.

Mettre en place une gouvernance de sécurité

Il s'agit, pour l'ingénieur systèmes, réseaux et cybersécurité de mettre en place des mesures techniques et organisationnelles garantissant un niveau de sécurité conforme aux différentes contraintes juridiques (LPM, LIL, RGPD, etc.), réglementaires (RGS, COB, HDS, etc.) ou de jurisprudence.

Réaliser une analyse médico-légale après un crime informatique

Il doit pouvoir, après un crime informatique (attaque, tentative d'intrusion, déni de services, etc.), analyser la façon dont a été réalisé le crime informatique, définir sa timeline (son déroulé temporel), recueillir l'ensemble des preuves permettant d'identifier le ou les coupables, savoir comment préserver ces preuves afin qu'elles restent recevables dans l'éventualité d'un procès.

Réaliser un audit sécurité

Il doit être capable de hacker (de manière éthique bien sûr) un système IT ou un système OT afin d'en déterminer l'ensemble des failles de sécurité, que celles-ci soient des failles réseaux, systèmes ou encore humaines.

Il doit pouvoir vérifier que le code des applications mises en place sur le système de l'entreprise ne présente pas de failles de développement offrant une zone d'attaque au système.

Il doit savoir rédiger le rapport d'audit afin que celui-ci :

- Puisse fournir des éléments techniques aux différents experts de l'entreprise
- Soit lisible pour un non initié à la cybersécurité et tout particulièrement par les dirigeants de l'entreprise concernée
- Fournisse les éléments de remédiation, c'est-à-dire de correction des failles trouvées

Blocs de compétences

RNCP38105BC01 — Gérer un projet international

LISTE DE COMPÉTENCES

Initialiser le projet

- Identifier les parties prenantes afin d'établir une communication et un rapport de confiance immédiat
- Choisir la méthode de gestion de projet adaptée au contexte et au client (classique, agilité, ...)
- Identifier la Core Team (équipe projet minimale) afin d'être à même de débiter le travail au plus vite
- Rédiger le plan de management de projet afin de pouvoir le partager avec le client et partir sur des bases communes
- Estimer les durées des différentes tâches afin de réaliser un planning de projet
- Estimer les coûts de chaque tâche afin de définir le coût prévisionnel estimé du projet
- Définir les indicateurs suivis afin de partager le tableau de bord projet
- Identifier les risques projet afin de sécuriser ce dernier
- Rédiger les fiches de risques afin de déterminer les solutions palliatives en cas de problème survenu
- Organiser une réunion de lancement afin de partager la vision du projet
- Conduire, indifféremment en français ou en anglais, avec assurance et professionnalisme la réunion de lancement, afin de rassurer le client

Conduire le projet

- Comprendre et s'exprimer en anglais sans problème, et ce, dans un contexte professionnel afin de pouvoir diriger une équipe projet internationale
- Accepter et exécuter les directives de sa direction afin de garantir la stratégie de son entreprise
- S'adapter lors d'interactions avec des personnes de cultures différentes afin d'accroître sa créativité
- Gérer les conflits au sein de l'équipe afin d'affiner son organisation et de gagner en productivité
- Renforcer la cohésion d'équipe afin de gagner en productivité
- Gérer les relations humaines afin de maintenir une efficacité au sein du projet
- Animer les revues de projet, indifféremment en français ou en anglais, internes et avec le client afin de traiter les points de blocage et de donner des informations d'avancement
- Suivre les dépenses budgétaires afin de rester dans l'enveloppe budgétaire définie initialement
- Communiquer de manière aisée à l'écrit comme à l'oral, en français comme en anglais, afin de transmettre des informations sur le projet
- Suivre et analyser les dérives du projet afin de réduire les écarts à échéance
- Gérer avec calme les événements inattendus afin de satisfaire et rassurer le client
- Négocier avec professionnalisme afin de construire une relation client gagnant/gagnant
- Gérer la sous-traitance afin de s'assurer de ne pas avoir de non-conformités ou de dérives à terminaison
- Développer les compétences individuelles et collectives de son équipe afin de rendre celle-ci de plus en plus performante
- Gérer son équipe projet afin de s'assurer de ne pas avoir de non-conformités ou de dérives aux termes du projet

Clore le projet

- Mesurer la satisfaction des parties prenantes afin de déterminer les axes d'amélioration
- Analyser le déroulement du projet afin de déterminer les erreurs qui ont eu lieu durant le projet
- Rédiger un rapport de clôture afin de partager l'expérience du projet avec l'ensemble des parties prenantes

MODALITÉS D'ÉVALUATION

- Mises en situations professionnelles reconstituées
- Passage du TOIEC
- Évaluation par l'entreprise
- Jeux de rôle
- Soutenance de la mission entreprise

RNCP38105BC02 — Recueillir et analyser les exigences du client

LISTE DE COMPÉTENCES

Recueillir les exigences du client

- Identifier les problèmes ou manques à l'origine du besoin afin de mieux comprendre ce dernier
- Identifier les différents types d'utilisateurs afin de prendre en compte les spécificités

- Extraire d'un cahier des charges les exigences du client afin de pouvoir les tracer de manière unitaire et être sûr de ne pas en oublier
- Identifier les enjeux afin de mieux cerner la problématique du client
- Identifier les exigences connexes afin de répondre au besoin du client
- Identifier, gérer et suivre les contraintes qualité afin de respecter les impératifs qualité
- Identifier, gérer et suivre les contraintes juridiques et légales afin de respecter les impératifs juridiques et légaux
- Reformuler la demande afin de s'assurer de la bonne compréhension du besoin
- Rédiger les documents formalisant les exigences afin de tracer l'ensemble des exigences sans en omettre

Réaliser l'analyse technique et fonctionnelle

- Rédiger les spécifications fonctionnelles du besoin afin de transcrire les exigences du client au sein du projet
- Rédiger les spécifications techniques du besoin, c'est à dire les méthodes, procédés, et technologies sélectionnées pour faire face aux contraintes de réalisation du projet
- Effectuer des tests exploratoires afin de valider les solutions techniques envisagées
- Choisir les technologies appropriées afin de réaliser l'ensemble des exigences client au mieux et au moindre coût
- Exposer la solution aux parties prenantes afin de partager les solutions techniques envisagées
- Identifier les fonctions représentatives des solutions techniques retenues afin de les mettre en application sur une maquette
- Formaliser les cas d'utilisation de chaque fonction retenue pour la maquette, afin de définir une manière de l'utiliser pour chacune d'elles
- Réaliser des maquettes afin de vérifier et prouver le bon fonctionnement de la solution technique retenue
- Rédiger un cahier de recette afin de permettre la validation de chaque fonction de la maquette
- Conduire une recette afin de prouver au client le bon fonctionnement des solutions techniques retenues

MODALITÉS D'ÉVALUATION

- Mises en situations professionnelles reconstituées
- Evaluation par l'entreprise
- Soutenance de la mission entreprise

RNCP38105BC03 — Concevoir l'architecture, réaliser et déployer la solution technique

LISTE DE COMPÉTENCES

Concevoir l'architecture de la solution

- Concevoir, de manière autonome, une architecture générale sécurisée (MFA, Workload, DMZ, gestion des identités, etc.) d'un système d'informations répondant aux spécifications techniques et fonctionnelles afin de répondre à l'ensemble des exigences du client
- Concevoir, de manière autonome, une architecture générale sécurisée d'un ICS (Industrial Control System) en réseau (HAN, NAN, BLÊME) répondant aux spécifications techniques et fonctionnelles afin de répondre à l'ensemble des exigences du client
- Intégrer des objets connectés (IOT) sécurisés dans une architecture ICS afin d'obtenir des données plus riches
- Identifier, au sein d'une architecture de système informatique, les données et services critiques afin de déterminer lesquels peuvent être externalisés (IaaS, PaaS, SaaS, CaaS)
- Adapter en CLOUD (privé, public, hybride et multicloud) une architecture existante afin d'externaliser une architecture "On Premise"
- Prendre en compte les spécifications non techniques (contraintes, normes) afin de garantir l'utilisation ultérieure du système informatique
- Réaliser les schémas d'architecture, notamment à l'aide de méthodes comme Merise, UML, AXIAL ou encore IDEF afin de donner une représentation fonctionnelle de celui-ci
- Rédiger les documents formalisant l'architecture afin de produire la documentation du projet
- Définir les impacts des changements afin de préparer la conduite du changement indispensable
- Communiquer les décisions d'architecture afin de partager les choix architecturaux avec le client
- Définir les règles de gestion des flux réseau (QoS : Quality Of Services) afin de garantir le bon fonctionnement des différents services mis à disposition de l'utilisateur final du système informatique
- Définir la politique de virtualisation du système informatique afin de détailler la stratégie d'automatisation du système informatique et de réduction des coûts de l'entreprise
- Concevoir une fabric pour pouvoir intégrer le SDN (Software Defined Network) au sein de l'architecture afin de gagner en nombre de manipulations nécessaires pour configurer les équipements
- Dissocier, à l'aide du SDS (Software Defined Storage) la gestion du stockage à l'aide d'un logiciel d'un système

informatique de la partie matérielle afin d'offrir plus de flexibilité à ce dernier

- Rédiger la PSSI (Politique de Sécurité du Système Informatique) afin de définir et expliquer la vision stratégique en termes de sécurité du système informatique

Sécuriser des systèmes industriels

- Adapter son architecture de sécurité à l'utilisation des capteurs et des actionneurs afin de sécuriser un système SCADA (ICS)

- Implémenter un système PAM (Privileged Access Management) dans une architecture ICS afin de limiter les risques de cybersécurité en gérant le contrôle des accès administratifs à l'ICS

Réaliser et déployer la solution

- Définir une organisation afin d'assurer le fonctionnement optimal du système informatique et son évolution, en respectant la structure existante et les contraintes qui lui sont liées
- Mettre en œuvre une méthode adaptée, en fonction du SI, de restitution des failles de sécurité, en signalant des recommandations plausibles, selon le contexte de l'entreprise afin de garantir le maintien en condition de sécurité du système informatique
- Intégrer la virtualisation des services au sein de l'architecture afin de réduire les équipements physiques nécessaires
- Mettre en œuvre le NFV (Network function virtualization) afin d'accélérer le déploiement de nouveaux services réseaux et de réduire le nombre d'équipements réseau nécessaires
- Intégrer des solutions de conteneurisation de l'architecture afin de migrer les applications vers des conteneurs
- Intégrer l'orchestration des conteneurs au sein de l'architecture afin d'automatiser le déploiement, la montée en charge et la mise en œuvre de conteneurs d'application sur des clusters
- Mettre en œuvre l'IBN (Intent-Based-Networking) afin de réaliser une mise en réseau basée sur les objectifs, de déterminer via l'IA (Intelligence Artificielle) comment exécuter et automatiser les tâches requises pour exploiter un réseau et de superviser l'architecture
- Intégrer le SDN (Software Defined Network) au sein de l'architecture afin de programmer les équipements actifs et donc de réduire les temps de déploiement
- Intégrer le SD-WAN (Software-defined wide-area-network) afin de déporter des services dans le CLOUD, de soulager ou remplacer les liaisons MPLS trop onéreuses pour l'entreprise et de conférer davantage d'agilité et de flexibilité
- Implémenter une solution de gestion du stockage (SDS) des données, transparente pour l'utilisateur final afin de gagner en agilité dans la gestion du système informatique
- Mettre en place une architecture de supervision de sécurité : un SOC (Security Operation Center) qui puisse détecter et filtrer les programmes malveillants, afin de lutter contre les menaces persistantes avancées
- Implémenter une solution de VOIP (Voix sur IP) et/ou de TOIP (Téléphonie sur IP) afin de fournir au système informatique des fonctionnalités de communications unifiées
- Implémenter une solution de MDM afin de gérer l'ensemble des périphériques mobiles de l'entreprise
- Intégrer l'ensemble des éléments réalisés séparément afin de vérifier qu'ils communiquent correctement et qu'ils fonctionnent ensemble
- Rédiger la documentation technique afin de produire la documentation du projet

Mettre en place une conduite du changement

- Rédiger la documentation à destination des opérationnels afin de faciliter l'utilisation du système informatique et leur adhésion à celui-ci
- Comprendre les causes des résistances afin de pouvoir mieux les contourner
- Identifier les porteurs du changement afin de créer un réseau de relais pour porter le changement localement
- Communiquer les changements afin d'avertir tous les utilisateurs de l'arrivée prochaine du système informatique et des apports de celui-ci.
- Préparer des supports de formations afin de pouvoir les remettre aux apprenants lors des sessions de formation au système informatique
- Organiser et animer des formations afin de faciliter la prise en main du système informatique

Industrialiser la solution

- Mettre en œuvre l'intégration continue afin de vérifier que le résultat des modifications du système informatique ne produit pas de régression
- Industrialiser le déploiement de la solution afin de simplifier l'opération pour le client, notamment à l'aide de différents outils DEVOPS (par exemple : ANSIBLE, PUPPET, CHEF, ...)
- Automatiser le déploiement, par le biais de scripting, de programmation d'équipements actifs, de provisioning afin

de réduire les coûts et les risques d'erreurs humaines

MODALITÉS D'ÉVALUATION

- Mises en situations professionnelles reconstituées
- Evaluation par l'entreprise
- Jeux de rôle
- Soutenance de la mission entreprise

RNCP38105BC04 — Maintenir le système en condition opérationnelle et de sécurité

LISTE DE COMPÉTENCES

Gérer les faits techniques et les évolutions

- Définir et rédiger la stratégie de maintenance curative afin de garantir la gestion des dysfonctionnements du système informatique sur la durée
- Mettre en œuvre des outils de suivi des faits techniques et des demandes d'évolution afin de suivre les futures modifications à réaliser
- Corriger des faits techniques afin d'améliorer la qualité du système informatique
- Proposer des solutions de contournement à des faits techniques afin de permettre au client d'utiliser le système informatique lorsqu'une correction n'est pas possible ou pas réalisable rapidement
- Maintenir une base de connaissances afin de partager les informations avec l'ensemble des parties prenantes
- Réaliser une veille technologique afin de pouvoir proposer des évolutions pour le système informatique
- Communiquer les modifications afin d'avertir le client de l'évolution et l'amélioration du système informatique

Mettre en place une démarche d'amélioration continue

- Déterminer les indicateurs de qualité afin de prouver au client la démarche d'amélioration continue mise en place
- Analyser les indicateurs de qualité afin de palier certaines dérives
- Améliorer la qualité du système informatique afin de garantir la satisfaction du client et de créer de nouvelles opportunités d'affaire avec ce dernier
- Mettre en œuvre des méthodes de suivi afin de garantir la traçabilité de toutes les actions réalisées
- Adopter une démarche d'amélioration continue de la sécurité afin de respecter les soucis de performances économiques de l'entreprise

Maintenir en condition opérationnelle et de sécurité

- Définir et rédiger la stratégie de maintenance préventive afin de garantir le bon fonctionnement du système informatique sur la durée
- Identifier et mettre en œuvre les outils de supervision de système et réseau (NOC : Network Operation Center) afin de garantir le fonctionnement du système informatique sur la durée
- Réaliser les requêtes corrélées d'analyse de sécurité afin de garantir la détection des attaques du système informatique
- Rédiger l'ensemble des documents de sûreté de fonctionnement du SI, en se conformant aux règles d'hygiène informatique édictées par l'ANSSI (Agence Nationale de Sécurité des SI) afin de garantir le partage de l'information avec l'ensemble des parties prenantes
- Mettre en place un SMSI (Système de Management de la Sécurité Informatique) conforme à l'ISO 27001 afin de gérer les risques relatifs à l'information au moyen de processus, et de définir les différentes responsabilités.
- Réaliser une analyse des risques de sécurité (EBIOS ou ISO 27005) afin de mieux sécuriser le système informatique.
- Mettre en œuvre une démarche d'urbanisation de système informatique afin de transformer ce dernier, et de prévoir les plans d'évolution à moyen terme (2-5 ans)
- Mettre en œuvre la PSSI afin d'appliquer la stratégie de sécurité de l'entreprise
- Gérer les droits d'accès aux différentes ressources du système informatique en appliquant le principe du moindre privilège afin de garantir une utilisation des ressources conformément aux principes énoncés dans la PSSI
- Garantir l'intégrité des données du système informatique afin de se prémunir contre toute manipulation de celles-ci
- Mettre en œuvre une politique de routage adaptée au besoin de l'entreprise afin de d'optimiser la gestion des flux au sein de l'architecture
- Assurer une veille de sécurité afin d'éviter les attaques de type zéro day
- Vérifier par le biais de sites spécialisés (CERT, NIST, CVE, etc.) que de nouvelles failles de sécurité n'ont pas été détectées sur des composants de l'architecture du système informatique afin de maintenir le niveau de sécurité recherché
- Mettre en place un plan de continuité d'activité et de reprise d'activité afin de minimiser les temps d'interruption du

système informatique conformément à la norme ISO 22301

- Réaliser des analyses de contenu approfondies (DLP : Data Loss Prevention) afin d'identifier, de contrôler et de protéger l'information
- Calculer le RTO (Recovery Time Objective) et le RPO (Recovery Point Objective) afin de calculer les coûts associés à ces mesures et de garantir les performances économiques de l'entreprise
- Implémenter des solutions de résilience des infrastructures du système informatique afin de garantir une disponibilité optimale de celui-ci
- Mettre en œuvre une gestion de crise afin de s'assurer que les dispositifs mis en place sont opérationnels et en mesure de faire face à tous types de situations de crise informatique

Mettre en place une gouvernance de sécurité

- Prendre en compte la LPM (Loi de Programmation Militaire) afin de garantir que les OIV (Organismes d'Intérêts Vitaux) mettent en place des mesures techniques et organisationnelles garantissant un niveau de sécurité conforme
- Prendre en compte le RGS (Référentiel Général de Sécurité) afin de renforcer la confiance des usagers dans les services électroniques mis à disposition par les autorités administratives
- Prendre en compte le RGPD (Règlement Général sur la Protection des Données) afin de protéger les personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
- Mettre en place le standard UL 2900 spécifiant les exigences de cybersécurité, afin de réaliser l'ensemble des tests auxquels un logiciel ou un système informatique doit être soumis pour obtenir la conformité.
- Comprendre les obligations réglementaires de sécurité liées au domaine d'activité d'une entreprise (COB [Commission des Opérations de Bourse], HDS [Hébergement Données Santé], etc.) afin d'être en conformité

Réaliser une analyse médico-légale après un crime informatique

- Maîtriser les techniques de Forensic numérique afin de pouvoir les mettre en œuvre et les implémenter judicieusement après une attaque d'un système informatique
- Définir la timeline du crime informatique afin de comprendre les différentes étapes et les vecteurs d'attaque
- Savoir comment conserver les preuves de l'attaque afin de pouvoir les utiliser lors d'un procès
- Savoir expliquer à son équipe les principes d'une analyse médico-légale après un crime informatique afin de pouvoir mieux manager techniquement celle-ci.

Réaliser un audit sécurité

- Savoir expliquer ce qu'est un audit de sécurité afin de mieux manager techniquement son équipe
- Savoir identifier et utiliser les failles de sécurité réseau afin de pénétrer un système informatique et de proposer des solutions de remédiation
- Savoir identifier et utiliser les failles de sécurité système afin de pénétrer un système informatique et de proposer des solutions de remédiation
- Savoir identifier et utiliser les failles de sécurité humaines afin de pénétrer un système informatique et de proposer des solutions de remédiation
- Savoir rédiger un rapport d'audit afin de le rendre compréhensible par les non-initiés
- Réaliser des tests de pénétration et de vulnérabilités afin de vérifier la bonne sécurisation du système informatique
- Réaliser un audit de code afin de vérifier que le code développé (applications mobile et Web) ne présente pas de failles de sécurité, conformément à la méthodologie OWASP
- Réaliser le fuzzing d'un logiciel afin d'injecter des données aléatoires dans ses entrées et de vérifier ainsi s'il y a des défauts de sécurité à corriger
- Calculer le CVSS (Common Vulnerability Scoring System) afin d'évaluer la criticité des vulnérabilités
- Déterminer le risque financier des vulnérabilités en fonction du CVSS afin de d'identifier les coûts associés à celles-ci

Réaliser un anti-virus

- Faire du reverse engineering sur un virus afin de comprendre son fonctionnement
- Définir les algorithmes à même de contrer le mode de fonctionnement d'un virus afin de créer un anti-virus
- Développer des tests unitaires, des tests d'intégration et des tests d'acceptations afin de simplifier et de sécuriser la future qualification de l'anti-virus

Communiquer sur la cybersécurité

- Sensibiliser les utilisateurs du système informatique à l'hygiène informatique et aux risques liés à la cybersécurité afin de réduire les failles potentielles liées aux risques humains
- Sensibiliser les VIP de l'entreprise aux risques liés à la cryptologie post-quantique afin de proposer des solutions palliatives et de les intégrer à la matrice de traçabilité des risques

MODALITÉS D'ÉVALUATION

- Mises en situations professionnelles reconstituées
- Evaluation par l'entreprise
- Jeux de rôle
- Soutenance de la mission entreprise

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Secteur d'activité et taille des entreprises ou services employeurs

De nos jours, tout type d'entreprise possède un système d'information et est ainsi concerné par cette certification.

- Tous secteurs, toutes entreprises ou administrations qui disposent d'un système d'information et/ou d'un système industriel.
- Les entreprises industrielles ou commerciales, les SSII qui offrent des services de type infogérance et intégration de solution réseaux.
- Les fabricants d'équipements réseaux, les opérateurs télécoms
- Etc.

Responsabilité et autonomie caractérisant les postes ciblés

Les infrastructures informatiques sont présentes dans toutes les entreprises quelle que soit leur taille :

- Des grandes structures (plusieurs centaines de serveurs et plusieurs milliers d'utilisateurs) ;
- Des petites et moyennes entreprises (quelques dizaines de serveurs et quelques centaines d'utilisateurs).

Dans les grandes entreprises, le champ d'activité est plus spécialisé. Dans les petites et moyennes entreprises, le champ est plus ouvert. Les jeunes diplômés devront donc être capables de prendre en charge toutes les activités du spectre d'intervention.

Les jeunes diplômés occupent des postes d'architecte junior système, réseau et sécurité, avec des évolutions de carrière de type directeur des systèmes d'information. Ils sont en charge d'une mission qu'ils doivent assurer en toute autonomie, fréquemment dans des contextes multi-langues, et ceci avec un engagement de résultats. Ils doivent fréquemment :

- Organiser leur planning de travail ;
- Gérer leur équipe de personnels ;
- Mener à bien des réunions clientes ;
- Gérer le budget alloué ;
- Rendre compte à leur hiérarchie et l'alerter si besoin.

TYPE D'EMPLOIS ACCESSIBLES

Les 3 intitulés de postes les plus fréquemment rencontrés pour cette certification sont :

- Ingénieur en cybersécurité
- Ingénieur système et/ou réseau
- Ingénieur DEVOPS

Suivant les secteurs et le périmètre du poste, les intitulés suivants sont également rencontrés :

- Consultant (système, réseau ou cybersécurité)
- Architecte système / réseau / cybersécurité
- Directeur de projet informatique
- Urbaniste du système informatique
- Directeur du système informatique
- Directeur / Responsable de la sécurité des systèmes informatiques
- Pentesteur
- Auditeur cybersécurité
- Analyste de la menace
- Responsable SOC
- Développeur de solution de sécurité
- Responsable / analyste CSIRT
- Gestionnaire de crise
- Analyste FORENSIC
- DEVSECOPS

RÉGLEMENTATIONS D'ACTIVITÉ

Le métier d'ingénieur systèmes, réseaux et cybersécurité n'est pas un métier réglementé. Néanmoins, l'ingénieur systèmes, réseaux et cybersécurité doit, dans le cadre de ses missions, tenir compte des droits, obligations et normes en matière de sécurisation et de gestion de données pour garantir sa mise en conformité. Il doit prendre en compte les obligations réglementaires en vigueur et notamment le RGPD (Règlement Général sur la Protection des Données).

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)	2 892 €
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) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	42 073
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 M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

MODALITÉS D'ACCÈS

Formation continue, Apprentissage, Contrat de professionnalisation, Candidature individuelle, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

Poursuite d'études :

- Titre niveau 6 informatique
- Licence Informatique
- Licence Professionnelle informatique

Reconversion :

- Master acquis dans une matière scientifique (mécanique, chimie, biologie, matériaux, électronique, etc.)
- Diplôme d'ingénieur dans un domaine autre qu'informatique (mécanique, chimie, biologie, matériaux, électronique, etc.)

PRÉREQUIS À LA VALIDATION

Pour valider la certification, les 4 blocs de compétences doivent être validés, et les candidats doivent obtenir le TOIEC niveau B2 (minimum de 785 points).

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

Le jury est composé de 5 personnes : 50% représentants de salariés, 50% représentant employeurs.

Le président du jury est désigné par l'ensemble des membres du jury.

Tous les membres du jury sont extérieurs à l'AFORP, aucun d'entre eux n'enseigne à l'AFORP et aucun d'entre eux n'encadre d'apprenants de l'AFORP.

Tous les membres du jury sont experts de leur domaine technique.

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	8 600 €
Selon la branche	7 500 € – 9 290 €
Prise en charge	Branches concernées
8 600 €	Valeur par défaut · 206 branches
9 290 €	CPNE de l'ingénierie, des services informatiques et du conseil, CPNEFP de la branche des industries de produits alimentaires élaborés, CPNIEFP dans la coopération agricole
8 668 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager
8 500 €	CPNEFP de la métallurgie
8 436 €	CPNEFP dans les établissements d'enseignement privés sous contrat
7 500 €	CPNE des industries de santé (CPNEIS)

Base légale

Date de décision	18/10/2023
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	18/10/2026
Date de dernière délivrance possible	18/10/2030

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2022	63	2	100 %	—
2021	47	0	100 %	89 %

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP36121

NOUVELLE(S) CERTIFICATION(S)

RNCP42822

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/38105/>

Se former en apprentissage

Formations en apprentissage	2
Organismes gestionnaires (CFA)	2
Organismes formateurs	2
Régions couvertes	2
Départements couverts	2
Organismes certifiés Qualiopi	2
Sessions	de 09/2024 à 08/2029

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