

Expert en systèmes d'information et sécurité

RNCP39394 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326
Formacode(s)	31008, 31006
Code(s) ROME	M1802, M1803, M1805, M1806, M1810
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	19/07/2024
Date d'échéance	19/07/2029

Certificateur(s)

ECOLE SUP INFORM COMMERCE · SIRET : 45303523000094

Partenaires habilités

4 organismes habilités, d'après la liste publiée par France compétences : 1 à former et organiser l'évaluation et 3 à former.

Organisme	SIRET	Habilitation
ACADENICE	91520875500024	Former
ADG	52004190600048	Former
AJ-FORMATION	79142898000035	Former
ECOLE SUP INFORM COMMERCE	45303523000094	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

Le paysage actuel des technologies de l'information évolue à une vitesse fulgurante, caractérisé par l'émergence rapide de nouvelles technologies telles que l'Internet des objets (IoT) et l'intelligence artificielle (IA). L'intégration généralisée de l'IoT et de l'IA dans les infrastructures informatiques augmente en effet considérablement la complexité des systèmes d'information.

Cette évolution, bien que prometteuse, expose également les organisations à des menaces de cybersécurité de plus en plus sophistiquées. Les cyberattaques, telles que les attaques de ransomware, les violations de données et les attaques ciblées, sont devenues monnaie courante. Les conséquences financières et réputationnelles des failles de sécurité soulignent l'impératif de renforcer la posture de sécurité des organisations. La sécurisation de ces environnements devient donc une priorité absolue pour garantir la résilience des entreprises face aux cybermenaces. Les réglementations en constante évolution, notamment le RGPD, imposent également des exigences strictes en matière de protection des données. La non-conformité peut entraîner, outre des sanctions financières importantes, des pertes considérables en matière de données.

Les entreprises ont besoin d'expertise en systèmes d'information et sécurité pour répondre à ces enjeux. Il est donc impératif d'investir dans la formation continue des professionnels existants, ainsi que de mettre à jour ou créer des programmes éducatifs spécialisés pour former de nouveaux talents pour répondre à la demande croissante.

La certification d'Expert en systèmes d'information et sécurité, garantit les compétences de ses titulaires à répondre adéquatement au besoin des entreprises et institutions sur ce métier.

ACTIVITÉS VISÉES

Gestion stratégique d'un système d'information et innovation : Pilotage de projet SI - Audit d'un système d'information - Management d'équipe - Intégration de pratiques inclusives et durables

Développement et mise en œuvre des technologies avancées et des services de sécurité : Développement et déploiement de plateforme applicative - Application de la data science - Intégration de l'IA - Renforcement de la sécurité

Mise en place et gestion des infrastructures numériques et de la cybersécurité : Gestion de l'infrastructure IT - Élaboration et renforcement des mesures de cybersécurité - Application de l'IA à la sécurité

Production et Intégration Sécurisés d'Objets Connectés (IoT) avec renforcement par l'IA : Développement de solutions IoT - Application de l'IA pour l'analyse et la sécurité - Intégration de pratiques de sécurité avancées

COMPÉTENCES ATTESTÉES

Piloter des projets interdisciplinaires en intégrant de nouvelles technologies et innovations afin de répondre aux enjeux stratégiques de l'entreprise, améliorer l'efficacité opérationnelle et renforcer la sécurité des systèmes d'information

Collaborer avec les équipes métier pour recueillir leurs besoins et défis spécifiques, et traduire ces besoins en solutions techniques viables qui soutiennent les objectifs stratégiques de l'entreprise

Définir le budget du projet et établir le plan stratégique en respectant les contraintes budgétaires et les échéances afin d'assurer la réalisation des objectifs fixés, maximiser le retour sur investissement et garantir la soutenabilité financière du projet

Optimiser la gestion du cycle de vie IT et piloter l'adoption des systèmes pour garantir une infrastructure technologique performante et évolutive

Évaluer les systèmes pour optimiser la performance et la sécurité

Aligner les systèmes d'information avec les tendances sectorielles et les objectifs stratégiques afin de stimuler l'innovation, favoriser la compétitivité de l'entreprise sur le marché, et soutenir une prise de décision éclairée

Mettre en œuvre des plans d'action et évaluer la résilience face aux cybermenaces

Documenter les résultats et assurer le suivi des améliorations afin de garantir la traçabilité des actions entreprises

Renforcer la culture de sécurité et instaurer un processus d'audit continu afin de minimiser les risques de cyberattaques et de violations de données

Constituer et manager des équipes pour atteindre les objectifs fixés, tout en intégrant des collaborateurs en situation de handicap afin de garantir l'inclusion au sein des équipes

Promouvoir l'accessibilité et le développement durable dans la conception des systèmes pour contribuer à l'économie circulaire

Engager les parties prenantes et évaluer l'impact pour une amélioration continue

Sélectionner et appliquer les technologies et méthodologies pertinentes afin d'optimiser les processus opérationnels, accroître l'efficacité et l'efficacité des projets

Améliorer l'expérience utilisateur et la prise de décision par l'analyse et l'IA afin de personnaliser les services, augmenter la satisfaction client, identifier de nouvelles opportunités de marché et optimiser les processus décisionnels, pour une meilleure performance opérationnelle et un avantage concurrentiel durable pour l'entreprise

Garantir la sécurité et la performance de la plateforme afin d'assurer une expérience utilisateur fiable et fluide, minimiser les risques de cyberattaques et de pannes, et soutenir la continuité des activités en maintenant des niveaux élevés de disponibilité et de réactivité des systèmes d'information.

Assurer l'alignement avec les besoins métier et une amélioration continue afin de s'assurer que la plateforme répond précisément aux besoins des équipes

Développer et intégrer des analyses de données avancées afin de dévoiler des insights stratégiques, optimiser la prise de décision fondée sur des données probantes, améliorer les performances opérationnelles, et identifier de nouvelles opportunités de croissance et d'innovation, contribuant ainsi à la transformation numérique et à la compétitivité de l'organisation.

Assurer la conformité, la communication et l'évaluation continue afin de garantir que les pratiques et procédures de l'entreprise respectent les normes réglementaires et les standards

Optimiser les processus et développer des solutions d'IA personnalisées afin d'automatiser et rationaliser les opérations, réduire les coûts et les délais, améliorer la précision et l'efficacité, et fournir des services et des produits plus adaptés

Renforcer la sécurité des plateformes logicielles avec l'IA, afin d'assurer la sécurité des données, protéger la confidentialité des informations des utilisateurs, prévenir les accès non autorisés et les fuites de données, et garantir

la conformité avec les réglementations en matière de protection des données, contribuant ainsi à la confiance et à la fidélité des clients ainsi qu'à la réputation de l'entreprise sur le marché.

Collaborer avec les équipes métier pour recueillir leurs besoins et adapter les solutions d'IA pour répondre à ces besoins.

Former les utilisateurs finaux à l'utilisation des nouveaux outils et systèmes basés sur l'IA pour maximiser leur adoption et leur utilité

Renforcer la sécurité des applications, des bases de données et des infrastructures utilisées pour le développement et l'analyse de données, ainsi que la protection contre les menaces et la conformité avec les normes

Optimiser et sécuriser l'infrastructure IT afin de garantir sa performance, sa fiabilité et sa résilience

Surveiller, gérer et innover pour la haute disponibilité afin d'assurer un accès constant et fiable aux services et aux applications critiques, minimiser les temps d'arrêt et les perturbations des opérations, et améliorer l'expérience utilisateur, contribuant ainsi à la satisfaction et à la fidélité des clients tout en soutenant les objectifs stratégiques de l'entreprise dans un marché compétitif

Élaborer et renforcer les mesures de cybersécurité à travers des approches innovantes et des technologies avancées pour protéger les actifs numériques contre les attaques internes et externes, tout en intégrant la conformité réglementaire

Implémenter l'intelligence artificielle dans les stratégies de sécurité pour anticiper, détecter et neutraliser les cybermenaces de manière proactive, améliorant ainsi la résilience des systèmes informatiques

Développer des solutions IoT innovantes pour améliorer l'efficacité opérationnelle et créer de nouvelles opportunités de service, en intégrant une fluidité dans les systèmes existants et en garantissant la sécurité des données

Utiliser l'intelligence artificielle pour analyser les données issues des dispositifs IoT et renforcer la sécurité des systèmes, permettant ainsi une meilleure prise de décision et une détection précoce des menaces

Intégrer des pratiques de sécurité avancées dans la conception et le déploiement des solutions IoT, en utilisant l'IA pour anticiper, détecter et répondre de manière proactive aux vulnérabilités et aux attaques cybernétiques

Blocs de compétences

RNCP39394BC01 — Pilotage stratégique de la gestion, de la sécurité et de l'innovation d'un système d'information

LISTE DE COMPÉTENCES

Piloter des projets interdisciplinaires en intégrant de nouvelles technologies et innovations afin de répondre aux enjeux stratégiques de l'entreprise, améliorer l'efficacité opérationnelle et renforcer la sécurité des systèmes d'information

Collaborer avec les équipes métier pour recueillir leurs besoins et défis spécifiques, et traduire ces besoins en solutions techniques viables qui soutiennent les objectifs stratégiques de l'entreprise

Définir le budget du projet et établir le plan stratégique en respectant les contraintes budgétaires et les échéances afin d'assurer la réalisation des objectifs fixés, maximiser le retour sur investissement et garantir la soutenabilité financière du projet

Optimiser la gestion du cycle de vie IT et piloter l'adoption des systèmes pour garantir une infrastructure technologique performante et évolutive

Évaluer les systèmes pour optimiser la performance et la sécurité

Aligner les systèmes d'information avec les tendances sectorielles et les objectifs stratégiques afin de stimuler l'innovation, favoriser la compétitivité de l'entreprise sur le marché, et soutenir une prise de décision éclairée

Mettre en œuvre des plans d'action et évaluer la résilience face aux cybermenaces

Documenter les résultats et assurer le suivi des améliorations afin de garantir la traçabilité des actions entreprises

Renforcer la culture de sécurité et instaurer un processus d'audit continu afin de minimiser les risques de cyberattaques et de violations de données

Constituer et manager des équipes pour atteindre les objectifs fixés, tout en intégrant des collaborateurs en situation de handicap afin de garantir l'inclusion au sein des équipes

Promouvoir l'accessibilité et le développement durable dans la conception des systèmes pour contribuer à l'économie circulaire

Engager les parties prenantes et évaluer l'impact pour une amélioration continue

MODALITÉS D'ÉVALUATION

Soutenance d'une partie du rapport d'expérience professionnelle

RNCP39394BC02 — Optimisation des services et de la sécurité du système d'information par le développement et la mise en œuvre de technologies avancées

LISTE DE COMPÉTENCES

Sélectionner et appliquer les technologies et méthodologies pertinentes afin d'optimiser les processus opérationnels, accroître l'efficacité et l'efficacité des projets

Améliorer l'expérience utilisateur et la prise de décision par l'analyse et l'IA afin de personnaliser les services, augmenter la satisfaction client, identifier de nouvelles opportunités de marché et optimiser les processus décisionnels, pour une meilleure performance opérationnelle et un avantage concurrentiel durable pour l'entreprise

Garantir la sécurité et la performance de la plateforme afin d'assurer une expérience utilisateur fiable et fluide, minimiser les risques de cyberattaques et de pannes, et soutenir la continuité des activités en maintenant des niveaux élevés de disponibilité et de réactivité des systèmes d'information.

Assurer l'alignement avec les besoins métier et une amélioration continue afin de s'assurer que la plateforme répond précisément aux besoins des équipes

Développer et intégrer des analyses de données avancées afin de dévoiler des insights stratégiques, optimiser la prise de décision fondée sur des données probantes, améliorer les performances opérationnelles, et identifier de nouvelles opportunités de croissance et d'innovation, contribuant ainsi à la transformation numérique et à la compétitivité de l'organisation.

Assurer la conformité, la communication et l'évaluation continue afin de garantir que les pratiques et procédures de l'entreprise respectent les normes réglementaires et les standards

Optimiser les processus et développer des solutions d'IA personnalisées afin d'automatiser et rationaliser les opérations, réduire les coûts et les délais, améliorer la précision et l'efficacité, et fournir des services et des produits plus adaptés

Renforcer la sécurité des plateformes logicielles avec l'IA, afin d'assurer la sécurité des données, protéger la confidentialité des informations des utilisateurs, prévenir les accès non autorisés et les fuites de données, et garantir la conformité avec les réglementations en matière de protection des données, contribuant ainsi à la confiance et à la fidélité des clients ainsi qu'à la réputation de l'entreprise sur le marché.

Collaborer avec les équipes métier pour recueillir leurs besoins et adapter les solutions d'IA pour répondre à ces besoins.

Former les utilisateurs finaux à l'utilisation des nouveaux outils et systèmes basés sur l'IA pour maximiser leur adoption et leur utilité

Renforcer la sécurité des applications, des bases de données et des infrastructures utilisées pour le développement et l'analyse de données, ainsi que la protection contre les menaces et la conformité avec les normes

MODALITÉS D'ÉVALUATION

Soutenance d'une partie du rapport d'expérience professionnelle

RNCP39394BC03 — Mise en place, gestion et optimisation des infrastructures numériques et de la cybersécurité par l'IA

LISTE DE COMPÉTENCES

Optimiser et sécuriser l'infrastructure IT afin de garantir sa performance, sa fiabilité et sa résilience

Surveiller, gérer et innover pour la haute disponibilité afin d'assurer un accès constant et fiable aux services et aux applications critiques, minimiser les temps d'arrêt et les perturbations des opérations, et améliorer l'expérience utilisateur, contribuant ainsi à la satisfaction et à la fidélité des clients tout en soutenant les objectifs stratégiques de l'entreprise dans un marché compétitif

Élaborer et renforcer les mesures de cybersécurité à travers des approches innovantes et des technologies avancées pour protéger les actifs numériques contre les attaques internes et externes, tout en intégrant la conformité réglementaire

Implémenter l'intelligence artificielle dans les stratégies de sécurité pour anticiper, détecter et neutraliser les cybermenaces de manière proactive, améliorant ainsi la résilience des systèmes informatiques

MODALITÉS D'ÉVALUATION

Soutenance d'une partie du rapport d'expérience professionnelle

RNCP39394BC04 — Développement, intégration et exploitation d'Objets Connectés (IoT) sécurisés, avec renforcement par l'IA

LISTE DE COMPÉTENCES

Développer des solutions IoT innovantes pour améliorer l'efficacité opérationnelle et créer de nouvelles opportunités de service, en intégrant une fluidité dans les systèmes existants et en garantissant la sécurité des données

Utiliser l'intelligence artificielle pour analyser les données issues des dispositifs IoT et renforcer la sécurité des systèmes, permettant ainsi une meilleure prise de décision et une détection précoce des menaces

Intégrer des pratiques de sécurité avancées dans la conception et le déploiement des solutions IoT, en utilisant l'IA pour anticiper, détecter et répondre de manière proactive aux vulnérabilités et aux attaques cybernétiques

MODALITÉS D'ÉVALUATION

Soutenance d'une partie du rapport d'expérience professionnelle

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Les experts en systèmes d'information et sécurité sont recherchés dans une grande variété d'entreprises, tant dans le secteur public que dans le secteur privé : Les grandes entreprises & grandes sociétés, qu'elles soient actives dans les secteurs de la technologie, de la finance, de la santé ou d'autres domaines, ont des besoins importants en matière de cybersécurité et de gestion des systèmes d'information ; les organisations / agences gouvernementales à tous les niveaux (national, régional, local) ont besoin de spécialistes en systèmes d'information et sécurité pour protéger les données sensibles et les infrastructures critiques ; les entreprises spécialisées dans la fourniture de solutions de sécurité informatique, telles que les sociétés de cybersécurité, embauchent régulièrement des experts en systèmes d'information et sécurité ; les fournisseurs de services cloud et les entreprises de technologie qui offrent des services d'hébergement et de stockage de données ont besoin de professionnels de la cybersécurité pour assurer la protection des données de leurs clients ; les établissements d'enseignement supérieur et de recherche, comme les universités, les collèges et les centres de recherche recrutent des experts en systèmes d'information et sécurité pour aider à protéger les données sensibles de la recherche et à prévenir les cybermenaces.

TYPE D'EMPLOIS ACCESSIBLES

Expert en système d'information et sécurité - Chef de Projet en systèmes d'information - Consultant systèmes d'information - Architecte cloud - Architecte de bases de données - Architecte de sécurité des systèmes d'information - Architecte système d'information - Auditeur en système d'information - Data manager

Expert en cybersécurité - Expert en technologie Internet et multimédia - Expert méthodes et outils en informatique - Expert méthodes et qualité informatique - Ingénieur sécurité web - Ingénieur système informatique - Ingénieur système réseau informatique

RÈGLEMENTATIONS D'ACTIVITÉ

Le métier d'expert en systèmes d'information et sécurité n'est pas réglementé. Cependant, selon le secteur d'activité dans lequel il évolue, il peut être contraint par un cadre réglementaire qu'il devra maîtriser.

Il doit également être au fait du RGPD et veiller au respect des réglementations en matière de confidentialité et de protection des données, tenir compte des contraintes liées à la sécurité des données, des solutions et des infrastructures, et veiller à la conformité aux pratiques et procédures de l'entreprise, ainsi qu'aux normes réglementaires et aux standards.

Marché du travail

Indicateurs au niveau des familles professionnelles (FAP) des métiers visés, agréés au niveau national — France Travail / DARES (open data).

Tension de recrutement (DARES 2024)	Élevée (4/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 3 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible, Lien formation-emploi
Salaire médian (mensuel)	2 912 €

Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (41 % des actifs en emploi)
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique · tension 4/5 (Élevée) M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique · tension 4/5 (Élevée) M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom · tension 5/5 (Très élevée) M2X91 — Chefs de projet et directeurs de service informatique · tension 4/5 (Élevée) M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom · tension 3/5 (Modérée) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	43 955
Jugés difficiles à recruter	50 %
Emplois saisonniers	2 %
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom M2X91 — Chefs de projet et directeurs de service informatique M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

MODALITÉS D'ACCÈS

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

PRÉREQUIS À L'ENTRÉE EN FORMATION

Être titulaire d'un titre de niveau 6 et/ou avoir exercé en tant que Concepteur développeur d'applications ou d'Administrateur réseaux

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

4 professionnels du secteur non intervenant dans l'établissement, dont l'un est président du jury

1 membre de l'ESIC (Directrice ou Responsable pédagogique)

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	7 146 €
Selon la branche	6 658 € – 7 341 €
Prise en charge	Branches concernées
7 146 €	Valeur par défaut · 204 branches
7 341 €	CPNE de l'ingénierie, des services informatiques et du conseil, CPNEFP ICGV entreprises de la viande
7 185 €	CPNE Branche Caoutchouc, CPNEFP de la métallurgie

6 658 €	CPNE des industries de santé (CPNEIS), CPNE du Commerce de détail et de gros à prédominance alimentaire
7 219 €	CPNEFP Commerce à distance
6 750 €	CPNEFP de la branche des prestataires de services du secteur tertiaire
6 665 €	CPNEF de la Publicité

Base légale

Date de décision	19/07/2024
Durée de l'enregistrement	5 ans
Date d'échéance de l'enregistrement	19/07/2029
Date de dernière délivrance possible	19/07/2033

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2023	10	0	86 %	—
2022	15	1	100 %	—
2021	6	0	100 %	60 %

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP34237

CORRESPONDANCES (PAR BLOCS)

RNCP34342, RNCP35078, RNCP35284, RNCP35544, RNCP35588, RNCP36297, RNCP38114

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://esic-online.com/nos-certifications/expert-en-systemes-dinformation-et-securite-6>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/39394/>

Où se former

Formations référencées	13
Organismes	2
Régions couvertes	1
Prix indicatif	1 500 € – 9 000 €

Offre de formation — MonCompteFormation (Caisse des Dépôts), licence ouverte.

Se former en apprentissage

Formations en apprentissage	1
-----------------------------	---

Organismes gestionnaires (CFA)	1
Organismes formateurs	1
Régions couvertes	1
Départements couverts	1
Organismes certifiés Qualiopi	1
Sessions	de 10/2025 à 03/2028

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

Entrées et sorties de formation

Entrées en formation	6
Parcours menés à terme	2
Taux d'achèvement	33 %
Période	04/2025 – 04/2026

Entrées et sorties — Caisse des Dépôts (open data), tous organismes confondus.

Demande CPF — formations engagées

Dossiers CPF engagés	12
Montant total engagé	43 800 €
Coût moyen par dossier	3 650 €
Durée moyenne	212 h
Période	02/2025 – 09/2026
France compétences	85 %
OPCO	12 %
Reste à charge titulaire	3 %

Formations engagées via le CPF — Caisse des Dépôts (open data), tous organismes confondus.