

Cybersécurité (fiche nationale)

RNCP39495 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Sigle	MASTER — Master
Code(s) NSF	110, 114, 326
Formacode(s)	31045, 24293
Code(s) ROME	M1801, M1802, M1805, M1806, M1810
Type d'enregistrement	Enregistrement de droit
Date d'échéance	31/08/2029

Certificateur(s)

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

UNIVERSITE DE RENNES · SIRET : 13003051300019

UNIVERSITE DE CAEN NORMANDIE · SIRET : 19141408500016

ECOLE NATIONALE SUPERIEURE D'INGENIEURS DE CAEN · SIRET : 19141720300012

Résumé de la certification

OBJECTIFS ET CONTEXTE

Le master est un diplôme national de l'enseignement supérieur conférant à son titulaire le grade universitaire de master. Il confère les mêmes droits à tous ses titulaires, quel que soit l'établissement qui l'a délivré.

Le master atteste l'acquisition d'un socle de connaissances et de compétences majoritairement adossées à la recherche dans un champ disciplinaire ou pluridisciplinaire. Le master prépare à la poursuite d'études en doctorat comme à l'insertion professionnelle immédiate après son obtention, et est organisé pour favoriser la formation tout au long de la vie.

Les parcours de formation en master tiennent compte de la diversité et des spécificités des publics accueillis en formation initiale et en formation continue.

ACTIVITÉS VISÉES

- La gestion de la sécurité des systèmes d'information
- La gestion de projets de sécurité
- La conception et le maintien d'un SI et d'applications sécurisés
- La formalisation de bonnes pratiques en matière de sécurité des systèmes d'information
- L'évaluation des risques d'attaques et les conséquences potentielles sur une organisation
- L'analyse de la sécurité des applications et des vulnérabilités
- La réalisation d'audit de la sécurité des systèmes d'information
- La réalisation de tests d'intrusion
- La détection d'attaques et d'intrusions
- La veille normative, technique et réglementaire sur les nouvelles attaques et vulnérabilités
- Le suivi d'activités par la création et la mise à jour d'indicateurs et de tableaux de bord
- La gestion des incidents et des crises de sécurité
- La sensibilisation et la formation des collaborateurs à la sécurité informatique
- Le respect des normes et réglementations en vigueur
- Le travail en équipe, la gestion d'équipe, la collaboration avec l'ensemble des services d'une organisation
- Le conseil et l'expertise auprès d'organisations tierces

COMPÉTENCES ATTESTÉES

Compétences transversales

- Identifier les usages numériques et les impacts de leur évolution sur le ou les domaines concernés par la mention
- Se servir de façon autonome des outils numériques avancés pour un ou plusieurs métiers ou secteurs de recherche du domaine
- Mobiliser des savoirs hautement spécialisés, dont certains sont à l'avant-garde du savoir dans un domaine de travail ou d'études, comme base d'une pensée originale
- Développer une conscience critique des savoirs dans un domaine et/ou à l'interface de plusieurs domaines
- Résoudre des problèmes pour développer de nouveaux savoirs et de nouvelles procédures et intégrer les savoirs de différents domaines
- Apporter des contributions novatrices dans le cadre d'échanges de haut niveau, et dans des contextes internationaux
- Conduire une analyse réflexive et distanciée prenant en compte les enjeux, les problématiques et la complexité d'une demande ou d'une situation afin de proposer des solutions adaptées et/ou innovantes en respect des évolutions de la réglementation
- Identifier, sélectionner et analyser avec esprit critique diverses ressources spécialisées pour documenter un sujet et synthétiser ces données en vue de leur exploitation
- Communiquer à des fins de formation ou de transfert de connaissances, par oral et par écrit, en français et dans au moins une langue étrangère
- Gérer des contextes professionnels ou d'études complexes, imprévisibles et qui nécessitent des approches stratégiques nouvelles
- Prendre des responsabilités pour contribuer aux savoirs et aux pratiques professionnelles et/ou pour réviser la performance stratégique d'une équipe
- Conduire un projet (conception, pilotage, coordination d'équipe, mise en œuvre et gestion, évaluation, diffusion) pouvant mobiliser des compétences pluridisciplinaires dans un cadre collaboratif
- Analyser ses actions en situation professionnelle, s'autoévaluer pour améliorer sa pratique dans le cadre d'une démarche qualité
- Respecter les principes d'éthique, de déontologie et de responsabilité sociale et environnementale
- Prendre en compte la problématique du handicap et de l'accessibilité dans chacune de ses actions professionnelles

Compétences spécifiques

- Réaliser un état des lieux de l'organisation en cybersécurité et conduire une analyse des risques en utilisant la méthodologie la mieux adaptée
- Définir la Politique Sécurité des Systèmes d'Information (PSSI) et la traduire en procédures et bonnes pratiques
- Identifier les ressources nécessaires à la mise en œuvre et au maintien de la PSSI (humaines, techniques et financières)
- Communiquer, sensibiliser et/ou former les employés de l'organisation au respect de la Politique Sécurité
- Définir et/ou déployer les plans de reprise ou de continuité d'activités en fonction des menaces potentielles et de leurs impacts
- Manager une équipe et/ou collaborer au sein d'une équipe autour de projets communs en y intégrant les préoccupations sociales, environnementales et éthiques
- Rendre compte à la Direction de l'organisation et aux autorités compétentes du niveau de maturité de l'organisation en cybersécurité et des solutions mises en œuvre
- Assurer une veille technique, réglementaire sur les nouvelles vulnérabilités et menaces émergentes ainsi qu'une veille des incidents géopolitiques
- Veiller au respect des normes, de la réglementation française, européenne et internationale en vigueur, et des interfaces avec la CNIL (Commission Nationale de l'Informatique et Libertés), du CERT-FR (Computer emergency response team - Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques) et CSIRT (Computer Security Incident Response Team - équipe spécialisée dans la gestion des incidents de sécurité informatique)
- Gérer et/ou suivre un projet de sécurisation des infrastructures à partir d'un cahier des charges et d'un budget défini et en appliquant la méthodologie de projet la plus adéquate
- Analyser la sécurité d'un SI ou Système et évaluer les risques de potentielles attaques et de nouvelles vulnérabilités
- Concevoir, développer et intégrer des solutions sécurisées en respectant les normes et bonnes pratiques en vigueur

- Choisir et intégrer un système de chiffrement adapté à un contexte donné
- Choisir et implémenter des protocoles de sécurité
- Utiliser et développer des outils d'analyse de code et de rétro-ingénierie
- Rendre compte de l'avancée des projets et évaluer régulièrement l'efficacité des solutions mises en place afin d'implémenter les actions d'amélioration nécessaires
- Anticiper, détecter les attaques et investiguer leur impact afin de mettre en place les mesures adéquates de remédiation
- Identifier les partenaires internes et/ou externes pour réaliser des audits techniques de sécurité, des attaques et pentest (tests d'intrusion) du système d'information et des applications selon les normes en vigueur
- Rédiger les rapports d'audits, d'incidents et des tests et les communiquer à l'organisation et aux autorités compétentes
- Mettre en place une cellule de crise en mobilisant des ressources (humaines, techniques, financières), en définissant le périmètre d'actions, les règles de fonctionnement et les modes de réaction à adopter en cas de crise
- Mettre en œuvre le plan de continuité d'activité ou de reprise d'activités en cas de crise majeure
- Définir et mettre en place tout axe d'amélioration nécessaire en fonction de l'évolution des attaques et des nouvelles vulnérabilités
- Etablir les enjeux de sécurité des SI des différents secteurs d'activités et profils d'organisation
- Alerter la Direction d'une organisation tierce sur les risques encourus en matière de cybersécurité et préconiser les solutions à mettre en œuvre
- Communiquer, conseiller et apporter une assistance technique aux utilisateurs afin que ceux-ci s'approprient les outils et respectent la stratégie définie en matière de sécurité
- Réaliser des travaux de recherche et prospection en cybersécurité dans les domaines techniques, scientifiques et réglementaires

Blocs de compétences

RNCP39495BC01 — Mettre en œuvre les usages avancés et spécialisés des outils numériques

LISTE DE COMPÉTENCES

- Identifier les usages numériques et les impacts de leur évolution sur le ou les domaines concernés par la mention
- Se servir de façon autonome des outils numériques avancés pour un ou plusieurs métiers ou secteurs de recherche du domaine

MODALITÉS D'ÉVALUATION

Chaque certificateur accrédité met en œuvre les modalités qu'il juge adaptées : rendu de travaux, mise en situation, évaluation de projet, etc.

Ces modalités d'évaluation peuvent être adaptées en fonction de la voie d'accès à la certification.

RNCP39495BC02 — Mobiliser et produire des savoirs hautement spécialisés

LISTE DE COMPÉTENCES

- Mobiliser des savoirs hautement spécialisés, dont certains sont à l'avant-garde du savoir dans un domaine de travail ou d'études, comme base d'une pensée originale
- Développer une conscience critique des savoirs dans un domaine et/ou à l'interface de plusieurs domaines
- Résoudre des problèmes pour développer de nouveaux savoirs et de nouvelles procédures et intégrer les savoirs de différents domaines
- Apporter des contributions novatrices dans le cadre d'échanges de haut niveau, et dans des contextes internationaux
- Conduire une analyse réflexive et distanciée prenant en compte les enjeux, les problématiques et la complexité d'une demande ou d'une situation afin de proposer des solutions adaptées et/ou innovantes en respect des évolutions de la réglementation

MODALITÉS D'ÉVALUATION

Chaque certificateur accrédité met en œuvre les modalités qu'il juge adaptées : rendu de travaux, mise en situation, évaluation de projet, etc.

Ces modalités d'évaluation peuvent être adaptées en fonction de la voie d'accès à la certification.

RNCP39495BC03 — Mettre en œuvre une communication spécialisée pour le transfert de connaissances

LISTE DE COMPÉTENCES

- Identifier, sélectionner et analyser avec esprit critique diverses ressources spécialisées pour documenter un sujet et synthétiser ces données en vue de leur exploitation
- Communiquer à des fins de formation ou de transfert de connaissances, par oral et par écrit, en français et dans au moins une langue étrangère

MODALITÉS D'ÉVALUATION

Chaque certificateur accrédité met en œuvre les modalités qu'il juge adaptées : rendu de travaux, mise en situation, évaluation de projet, etc.

Ces modalités d'évaluation peuvent être adaptées en fonction de la voie d'accès à la certification.

RNCP39495BC04 — Contribuer à la transformation en contexte professionnel

LISTE DE COMPÉTENCES

- Gérer des contextes professionnels ou d'études complexes, imprévisibles et qui nécessitent des approches stratégiques nouvelles
- Prendre des responsabilités pour contribuer aux savoirs et aux pratiques professionnelles et/ou pour réviser la performance stratégique d'une équipe
- Conduire un projet (conception, pilotage, coordination d'équipe, mise en œuvre et gestion, évaluation, diffusion) pouvant mobiliser des compétences pluridisciplinaires dans un cadre collaboratif
- Analyser ses actions en situation professionnelle, s'autoévaluer pour améliorer sa pratique dans le cadre d'une démarche qualité
- Respecter les principes d'éthique, de déontologie et de responsabilité sociale et environnementale
- Prendre en compte la problématique du handicap et de l'accessibilité dans chacune de ses actions professionnelles

MODALITÉS D'ÉVALUATION

Chaque certificateur accrédité met en œuvre les modalités qu'il juge adaptées : rendu de travaux, mise en situation, évaluation de projet, etc.

Ces modalités d'évaluation peuvent être adaptées en fonction de la voie d'accès à la certification.

RNCP39495BC05 — Piloter la sécurité des systèmes d'information

LISTE DE COMPÉTENCES

- Réaliser un état des lieux de l'organisation en cybersécurité et conduire une analyse des risques en utilisant la méthodologie la mieux adaptée
- Définir la Politique Sécurité des Systèmes d'Information (PSSI) et la traduire en procédures et bonnes pratiques
- Identifier les ressources nécessaires à la mise en œuvre et au maintien de la PSSI (humaines, techniques et financières)
- Communiquer, sensibiliser et/ou former les employés de l'organisation au respect de la Politique Sécurité
- Définir et/ou déployer les plans de reprise ou de continuité d'activités en fonction des menaces potentielles et de leurs impacts
- Manager une équipe et/ou collaborer au sein d'une équipe autour de projets communs en y intégrant les préoccupations sociales, environnementales et éthiques
- Rendre compte à la Direction de l'organisation et aux autorités compétentes du niveau de maturité de l'organisation en cybersécurité et des solutions mises en œuvre
- Assurer une veille technique, réglementaire sur les nouvelles vulnérabilités et menaces émergentes ainsi qu'une veille des incidents géopolitiques
- Veiller au respect des normes, de la réglementation française, européenne et internationale en vigueur, et des interfaces avec la CNIL (Commission Nationale de l'Informatique et Libertés), du CERT-FR (Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques) et CSIRT (équipe spécialisée dans la gestion des incidents de sécurité informatique)

MODALITÉS D'ÉVALUATION

Chaque certificateur accrédité met en œuvre les modalités qu'il juge adaptées : rendu de travaux, mise en situation, évaluation de projet, etc.

Ces modalités d'évaluation peuvent être adaptées en fonction de la voie d'accès à la certification.

RNCP39495BC06 — Concevoir, développer et maintenir des solutions de cybersécurité SI, systèmes embarqués et applications

LISTE DE COMPÉTENCES

- Gérer et/ou suivre un projet de sécurisation des infrastructures à partir d'un cahier des charges et d'un budget défini et en appliquant la méthodologie de projet la plus adéquate
- Analyser la sécurité d'un SI ou Système et évaluer les risques de potentielles attaques et de nouvelles vulnérabilités
- Concevoir, développer et intégrer des solutions sécurisées en respectant les normes et bonnes pratiques en vigueur
- Choisir et implémenter des protocoles de sécurité
- Choisir et intégrer un système de chiffrement adapté à un contexte donné
- Utiliser et développer des outils d'analyse de code et de rétro-ingénierie
- Rendre compte de l'avancée des projets et évaluer régulièrement l'efficacité des solutions mises en place afin d'implémenter les actions d'amélioration nécessaires

MODALITÉS D'ÉVALUATION

Chaque certificateur accrédité met en œuvre les modalités qu'il juge adaptées : rendu de travaux, mise en situation, évaluation de projet, etc.

Ces modalités d'évaluation peuvent être adaptées en fonction de la voie d'accès à la certification.

RNCP39495BC07 — Anticiper, gérer et remédier aux incidents et aux crises cybersécurité

LISTE DE COMPÉTENCES

- Anticiper, détecter les attaques et investiguer leur impact afin de mettre en place les mesures adéquates de remédiation
- Identifier les partenaires internes et/ou externes pour réaliser des audits techniques de sécurité, des attaques et pentest (tests d'intrusion) du système d'information et des applications selon les normes en vigueur
- Rédiger les rapports d'audits, d'incidents et des tests et les communiquer à l'organisation et aux autorités compétentes
- Mettre en place une cellule de crise en mobilisant des ressources (humaines, techniques, financières), en définissant le périmètre d'actions, les règles de fonctionnement et les modes de réaction à adopter en cas de crise
- Mettre en œuvre le plan de continuité d'activité ou de reprise d'activités en cas de crise majeure
- Définir et mettre en place tout axe d'amélioration nécessaire en fonction de l'évolution des attaques et des nouvelles vulnérabilités

MODALITÉS D'ÉVALUATION

Chaque certificateur accrédité met en œuvre les modalités qu'il juge adaptées : rendu de travaux, mise en situation, évaluation de projet, etc.

Ces modalités d'évaluation peuvent être adaptées en fonction de la voie d'accès à la certification.

RNCP39495BC08 — Apporter une expertise en terme de conseil et de recherche

LISTE DE COMPÉTENCES

- Etablir les enjeux de sécurité des systèmes d'information (SI) des différents secteurs d'activités et profils d'organisation
- Alerter la Direction d'une organisation tierce sur les risques encourus en matière de cybersécurité et préconiser les solutions à mettre en œuvre
- Communiquer, conseiller et apporter une assistance technique aux utilisateurs afin que ceux-ci s'approprient les outils et respectent la stratégie définie en matière de sécurité
- Réaliser des travaux de recherche et prospection en cybersécurité dans les domaines techniques, scientifiques et réglementaires

MODALITÉS D'ÉVALUATION

Chaque certificateur accrédité met en œuvre les modalités qu'il juge adaptées : rendu de travaux, mise en situation, évaluation de projet, etc.

Ces modalités d'évaluation peuvent être adaptées en fonction de la voie d'accès à la certification.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

- 62.01 Programmation informatique
- 62.02 Conseil en informatique
- 63.11 Traitement de données, hébergement et activités connexes

Le diplômé du Master mention Cybersécurité peut exercer ses activités dans les domaines de l'informatique, les télécommunications, l'industrie aéronautique et spatiale/ défense, les banques / assurance / finances, etc...dans de grandes entreprises, des PME ou des start-up.

TYPE D'EMPLOIS ACCESSIBLES

- Ingénieur Cybersécurité Système d'information (SI)
- Architecte réseaux et sécurité
- Consultant en Cybersécurité
- Responsable SSI (Sécurité des Système d'Information)
- Analyste Cybersécurité
- Administrateur sécurité
- Cryptologue
- Evalueur de la sécurité
- Auditeur Cybersécurité
- Surveillance d'intrusion (Blue Teamer) / Testeur d'intrusion (Red Teamer)
- Analyste de criticité (Pentester)
- Assistant expert en informatique légale (Analyste Forensic)
- Développeur et intégrateur de solutions de sécurité (DevSecOps)
- Ingénieur Cybersécurité logiciel / Ingénieur Cybersécurité systèmes embarqués
- Gestionnaire de crise en cybersécurité
- Délégué à la protection des données (DPO)
- Ingénieur R&D en cybersécurité

Marché du travail

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

Tension de recrutement (DARES 2024)	Élevée (4/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 3 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible, Lien formation-emploi
Salaire médian (mensuel)	2 781 €
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) 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)	41 765
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 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

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

Leur composition comprend :

- une moitié d'enseignants-chercheurs, d'enseignants ou de chercheurs participant à la formation
- des professionnels qualifiés ayant contribué aux enseignements
- des professionnels qualifiés n'ayant pas contribué aux enseignements

COMPOSITION DU JURY — VAE

Articles L6411-1 à L6423-3 du Code du travail

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	9 295 €
Selon la branche	7 700 € – 10 000 €
Prise en charge	Branches concernées
9 295 €	Valeur par défaut · 178 branches
10 000 €	CPNE Casinos, CPNE Travail Temporaire, CPNE de l'édition de livres, de l'édition phonographique et de l'édition de musique, CPNE des Télécoms, CPNE des industries de santé (CPNEIS)
8 450 €	CPNE des MFR, CPNE des Métiers de la Transformation des Grains, CPNE des Vins et Spiritueux, CPNE des centres de gestion agréés et habilités agricoles, CPNEFP Transformation Laitière
9 556 €	CPNEFP Grands Magasins/ Magasins Populaires, CPNEFP du Négoce de l'ameublement
9 500 €	CPNE Branche Caisse d'Epargne, CPNE de la branche Banque Populaire
9 992 €	CPNEFP Mutualité
9 300 €	CPNEFP des industries électriques et gazières
9 055 €	CPNEFP Habillement succursaliste
9 000 €	CPNE chimie
8 775 €	CPNEFP de la branche des entreprises du bureau et du numérique (commerces et services)
8 750 €	CPNEFP Commerce à distance
8 711 €	CPNEFP Professions de la Photographie
8 500 €	CPNEFP de la métallurgie

8 400 €	CPNEFP de la branche des prestataires de services du secteur tertiaire
---------	--

7 700 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager
---------	---

Base légale

Date d'échéance de l'enregistrement	31/08/2029
-------------------------------------	------------

Date de dernière délivrance possible	31/08/2032
--------------------------------------	------------

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://www.ensicaen.fr/>

<https://www.univ-rennes.fr/>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/39495/>