

Manager de la cybersécurité

RNCP36595 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326n
Formacode(s)	31006
Code(s) ROME	M1802
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	01/07/2022
Date d'échéance	01/07/2025

Certificateur(s)

DE VINCI HIGHER EDUCATION (DVHE) · SIRET : 44087031900025

Partenaires habilités

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

Organisme	SIRET	Habilitation
ASSOCIATION LEONARD DE VINCI	40285022600018	Former et organiser l'évaluation
ISCOD	88877726500032	Former et organiser l'évaluation
OKTOGONE GROUP	84521063200012	Former et organiser l'évaluation
VISIPLUS	44321186700025	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

Le management de la sécurité des données numériques repose sur une analyse des risques auxquels sont confrontés les systèmes d'information et les réseaux. Le métier associe la conception d'architectures de sécurité à la mise en œuvre de solutions destinées à assurer une sûreté de fonctionnement maximale de ceux-ci et la protection des bases de données contre tous types d'intrusion à des fins de vol ou de destruction.

ACTIVITÉS VISÉES

Analyse stratégique des cyber-risque

Veille géopolitique sur les cyber-menaces et la cybercriminalité

Identification des risques d'intrusion dans les systèmes d'information de l'entreprise

Analyse des risques affectant les données numériques

Mise en œuvre de l'intelligence économique

Conception et organisation de la sécurité des systèmes d'information et des réseaux

Conception d'une architecture de sécurité adaptée au niveau de risques

Conduite d'un appel d'offres sur les architectures et solutions de sécurité

Choix des prestataires en cyber sécurité

Veille réglementaire

Déploiement de la sécurité des systèmes d'information et des réseaux

Sécurisation des réseaux et des services

Protection des données et du patrimoine immatériel de l'entreprise
Sécurisation des locaux et des infrastructures sensibles
Mise en place de la sûreté de fonctionnement
Management de la cyber sécurité dans l'entreprise
Elaboration du schéma organisationnel de la cyber sécurité
Formation et conseil aux services supports
Conduite de projet et conduite du changement
Anticipation de la gestion des crises
Gestion budgétaire et financière
Elaboration du budget prévisionnel et du plan de financement
Contrôle de gestion et pilotage budgétaire
Suivi et contrôle des sous-traitants

COMPÉTENCES ATTESTÉES

Analyser une situation géopolitique propice à la cyberguerre, en recensant les cyberattaques passées, dans le but de cartographier les menaces potentielles sur les systèmes d'information d'un pays ou d'une industrie.

Conduire un audit du système d'information et des réseaux de son entreprise, afin d'identifier leurs points de vulnérabilité au regard des menaces d'intrusion inhérentes au cyberspace.

Dresser un état des dommages potentiels devant résulter des attaques au système d'information de son entreprise, en caractérisant les atteintes possibles aux données numériques (altération, captation ou destruction) traitées ou stockées par celui-ci, en vue d'établir un cahier des charges de la cyber sécurité.

Se conformer à la norme ISO 27032, dans le cadre du budget disponible, afin de répondre aux impératifs de protection de l'activité et des données.

Organiser la surveillance de l'environnement concurrentiel de son entreprise, en collectant les informations économiques et stratégiques utiles, afin d'anticiper sur les intentions des concurrents sur le marché national et international.

Etablir le schéma général de la cyber sécurité dans son entreprise, en s'appuyant sur l'audit de vulnérabilité des systèmes d'information et des réseaux, afin de déterminer les caractéristiques d'une nouvelle architecture à mettre en place.

Traduire en spécifications techniques les attentes en matière d'architecture et de solutions de sécurité, en vue de la rédaction du cahier des charges d'un appel d'offres sur le marché des prestataires.

Coordonner la rédaction du cahier des charges et de l'appel d'offres, conformément au schéma général de la cyber sécurité préalablement établi, en vue de la sélection des prestataires et sous-traitants.

Analyser la situation économique et financière des répondants à l'appel d'offres, afin d'assurer la viabilité à long terme des solutions retenues.

Choisir une prestation de cyber sécurité, dans le respect du budget imparti et du cahier des charges, afin d'optimiser la couverture des risques.

Concevoir et utiliser un système de veille sur l'actualité des contraintes légales et réglementaires, à l'aide des outils numériques de recherche sur les sites des organismes spécialisés en matière de cyber sécurité et les bases de données juridiques du domaine, afin d'assurer la conformité légale des dispositifs de sécurité mis en place.

Identifier les emplacements des pare-feux et alertes les mieux adaptés à la prévention des intrusions, afin d'optimiser les temps de détection et de réponse.

Installer les dispositifs de remplacement des réseaux infectés, dans le but d'assurer la continuité des services aux utilisateurs.

Protéger l'accès aux espaces de stockage et aux données par des systèmes de codes d'accès et de cryptage adaptés aux menaces, afin d'assurer la conservation du patrimoine immatériel de l'entreprise.

Identifier les risques d'atteinte aux infrastructures physiques en vue de placer les alertes et protections à même d'anticiper sur toutes tentatives d'intrusion dans les locaux.

Optimiser les solutions de fourniture d'énergie et les dispositifs de secours en cas de défaillance, afin d'assurer l'alimentation permanente des systèmes d'information et des réseaux de l'entreprise.

Etablir le schéma général de la sûreté de fonctionnement à l'intention des services internes à l'entreprise, en vue de garantir la continuité de l'activité quelles que soient les attaques sur le système d'information.

Sur la base des audits de risques cyber sur les systèmes et réseaux, les données et les infrastructures, conduire une analyse systémique de l'organisation de son entreprise en vue de répartir les responsabilités dans un organigramme général de la cyber sécurité.

Analyser les compétences du personnel de son entreprise en matière de cyber sécurité, au moyen de questionnaires et d'entretiens, en vue de concevoir et mettre en place un plan de formation des personnels et de conseil aux services supports.

Prendre en compte le référentiel général d'amélioration de l'accessibilité (RGAA) et les recommandations de la norme internationale WCAG 2.1 (Web Content Accessibility Guidelines) à un niveau aaa, dans le but d'adapter le management interne de la cyber sécurité aux personnes handicapées.

Prendre en compte la multiculturalité des personnels de son organisation, dans le but d'adapter le management interne de la cyber sécurité aux modes particuliers d'appréhension des directives.

Utiliser une méthode de gestion de projet pour la mise en place d'une nouvelle organisation de la cyber sécurité dans l'entreprise.

Accompagner le changement nécessité par les dispositions locales et internationales en matière de cyber sécurité, au plus près des postes de travail, afin d'assurer le bon fonctionnement de l'organisation mise en place.

Concevoir et déployer dans l'entreprise une communication destinée à anticiper sur la gestion des crises occasionnées par les tentatives d'intrusion cyber.

Estimer les investissements (coûts et calendrier), afin de déterminer les besoins de financement.

Négocier les conditions de financement en tenant compte des évolutions probables des technologies de la cyber sécurité, en vue de construire un budget fiable à moyen terme.

Choisir des indicateurs de suivi budgétaire adaptés au contexte de la cyber sécurité, en vue de constituer les tableaux de bord de gestion conformes aux principes de son entreprise.

Analyser en continu les écarts budgétaires, afin de décider la mise en place des mesures correctives et d'assurer la réalisation des projets dans le cadre imparti.

Assurer le suivi des contrats de sous-traitance en vérifiant régulièrement la solidité des garanties financières, afin d'éviter les ruptures dans la fourniture et la maintenance des systèmes de sécurité mis en place.

Blocs de compétences

RNCP36595BC01 — Mener une analyse stratégique des risques cyber

LISTE DE COMPÉTENCES

Analyser une situation géopolitique propice à la cyberguerre, en recensant les cyberattaques passées, dans le but de cartographier les menaces potentielles sur les systèmes d'information d'un pays ou d'une industrie.

Conduire un audit du système d'information et des réseaux de son entreprise, afin d'identifier leurs points de vulnérabilité au regard des menaces d'intrusion inhérentes au cyberspace.

Dresser un état des dommages potentiels devant résulter des attaques au système d'information de son entreprise, en caractérisant les atteintes possibles aux données numériques (altération, captation ou destruction) traitées ou stockées par celui-ci, en vue d'établir un cahier des charges de la cyber sécurité.

Se conformer à la norme ISO 27032, dans le cadre du budget disponible, afin de répondre aux impératifs de protection de l'activité et des données.

Organiser la surveillance de l'environnement concurrentiel de son entreprise, en collectant les informations économiques et stratégiques utiles, afin d'anticiper sur les intentions des concurrents sur le marché national et international.

MODALITÉS D'ÉVALUATION

Travaux écrits

Etude de cas

Mise en situation professionnelle

Présentation orale devant le jury

RNCP36595BC02 — Concevoir et organiser la sécurité des SI et des réseaux

LISTE DE COMPÉTENCES

Etablir le schéma général de la cyber sécurité dans son entreprise, en s'appuyant sur l'audit de vulnérabilité des systèmes d'information et des réseaux, afin de déterminer les caractéristiques d'une nouvelle architecture à mettre en place.

Traduire en spécifications techniques les attentes en matière d'architecture et de solutions de sécurité, en vue de la rédaction du cahier des charges d'un appel d'offres sur le marché des prestataires.

Coordonner la rédaction du cahier des charges et de l'appel d'offres, conformément au schéma général de la cyber

sécurité préalablement établi, en vue de la sélection des prestataires et sous-traitants.

Analyser la situation économique et financière des répondants à l'appel d'offres, afin d'assurer la viabilité à long terme des solutions retenues.

Choisir une prestation de cyber sécurité, dans le respect du budget imparti et du cahier des charges, afin d'optimiser la couverture des risques.

Concevoir et utiliser un système de veille sur l'actualité des contraintes légales et réglementaires, à l'aide des outils numériques de recherche sur les sites des organismes spécialisés en matière de cyber sécurité et les bases de données juridiques du domaine, afin d'assurer la conformité légale des dispositifs de sécurité mis en place.

MODALITÉS D'ÉVALUATION

Questionnaire

Travaux écrits

Mise en situation professionnelle

Présentation orale devant le jury

RNCP36595BC03 — Déployer la sécurité des SI et des réseaux

LISTE DE COMPÉTENCES

Identifier les emplacements des pare-feux et alertes les mieux adaptés à la prévention des intrusions, afin d'optimiser les temps de détection et de réponse.

Installer les dispositifs de remplacement des réseaux infectés, dans le but d'assurer la continuité des services aux utilisateurs.

Protéger l'accès aux espaces de stockage et aux données par des systèmes de codes d'accès et de cryptage adaptés aux menaces, afin d'assurer la conservation du patrimoine immatériel de l'entreprise.

Identifier les risques d'atteinte aux infrastructures physiques en vue de placer les alertes et protections à même d'anticiper sur toutes tentatives d'intrusion dans les locaux.

Optimiser les solutions de fourniture d'énergie et les dispositifs de secours en cas de défaillance, afin d'assurer l'alimentation permanente des systèmes d'information et des réseaux de l'entreprise.

Etablir le schéma général de la sûreté de fonctionnement à l'intention des services internes à l'entreprise, en vue de garantir la continuité de l'activité quelles que soient les attaques sur le système d'information.

MODALITÉS D'ÉVALUATION

Travaux écrits

Mise en situation professionnelle

Présentation orale devant le jury

RNCP36595BC04 — Manager la cyber sécurité dans l'entreprise

LISTE DE COMPÉTENCES

Sur la base des audits de risques cyber sur les systèmes et réseaux, les données et les infrastructures, conduire une analyse systémique de l'organisation de son entreprise en vue de répartir les responsabilités dans un organigramme général de la cyber sécurité.

Analyser les compétences du personnel de son entreprise en matière de cyber sécurité, au moyen de questionnaires et d'entretiens, en vue de concevoir et mettre en place un plan de formation des personnels et de conseil aux services supports.

Prendre en compte le référentiel général d'amélioration de l'accessibilité (RGAA) et les recommandations de la norme internationale WCAG 2.1 (Web Content Accessibility Guidelines) à un niveau aaa, dans le but d'adapter le management interne de la cyber sécurité aux personnes handicapées.

Prendre en compte la multiculturalité des personnels de son organisation, dans le but d'adapter le management interne de la cyber sécurité aux modes particuliers d'appréhension des directives.

Utiliser une méthode de gestion de projet pour la mise en place d'une nouvelle organisation de la cyber sécurité dans l'entreprise.

Accompagner le changement nécessité par les dispositions locales et internationales en matière de cyber sécurité, au plus près des postes de travail, afin d'assurer le bon fonctionnement de l'organisation mise en place.

Concevoir et déployer dans l'entreprise une communication destinée à anticiper sur la gestion des crises occasionnées par les tentatives d'intrusion cyber.

MODALITÉS D'ÉVALUATION

Travaux écrits

Mise en situation professionnelle
Présentation orale devant le jury

RNCP36595BC05 — Gérer les aspects budgétaires et financiers de la cyber sécurité

LISTE DE COMPÉTENCES

Estimer les investissements (coûts et calendrier), afin de déterminer les besoins de financement.

Négocier les conditions de financement en tenant compte des évolutions probables des technologies de la cyber sécurité, en vue de construire un budget fiable à moyen terme.

Choisir des indicateurs de suivi budgétaire adaptés au contexte de la cyber sécurité, en vue de constituer les tableaux de bord de gestion conformes aux principes de son entreprise.

Analyser en continu les écarts budgétaires, afin de décider la mise en place des mesures correctives et d'assurer la réalisation des projets dans le cadre imparti.

Assurer le suivi des contrats de sous-traitance en vérifiant régulièrement la solidité des garanties financières, afin d'éviter les ruptures dans la fourniture et la maintenance des systèmes de sécurité mis en place.

MODALITÉS D'ÉVALUATION

Travaux écrits

Mise en situation professionnelle

Présentation orale devant le jury

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Toutes entreprises et institutions publiques et privées dotées de systèmes d'informations.

Toutes entreprises de services numériques et organismes spécialisés en cyber sécurité.

TYPE D'EMPLOIS ACCESSIBLES

Le manager de la cyber sécurité occupe généralement les fonctions suivantes :

- Manager de la cyber sécurité · Expert(e) en sécurité des SI
- Responsable de la sécurité des systèmes d'information et des réseaux (RSSI)
- Responsable de la sécurité des systèmes d'information
- Ingénieur cyber sécurité

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)
Facteurs principaux	Lien formation-emploi, Manque de main-d'œuvre disponible
Salaire médian (mensuel)	3 115 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (35 % des actifs en emploi)
Familles professionnelles (FAP)	M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	4 758
Jugés difficiles à recruter	45 %
Emplois saisonniers	0 %
Familles professionnelles (FAP)	M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

Etre titulaire d'un diplôme ou titre de niveau 6.

Ou d'un diplôme ou titre de niveau 5, après validation du dossier par la Commission d'autorisation de candidature (CAC).

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

Le jury de certification est constitué de cinq personnes dont trois professionnels extérieurs à l'autorité de certification.

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	7 748 €
Selon la branche	7 748 € – 8 273 €
Prise en charge	Branches concernées
7 748 €	Valeur par défaut · 204 branches
8 273 €	CPNE de l'ingénierie, des services informatiques et du conseil, CPNEFP ICGV entreprises de la viande, CPNEFP de la Mutualité Sociale Agricole
8 088 €	CPNE Branche Caoutchouc, CPNE des industries de santé (CPNEIS), CPNEFP de la métallurgie
8 245 €	CPNE des Télécoms
8 108 €	CPNE de l'édition de livres, de l'édition phonographique et de l'édition de musique
8 062 €	CPNEFP dans les établissements d'enseignement privés sous contrat

Base légale

Date de décision	01/07/2022
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	01/07/2025

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2020	15	0	87 %	91 %
2019	11	0	91 %	72 %
2018	3	0	100 %	100 %

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP32025

NOUVELLE(S) CERTIFICATION(S)

RNCP40246

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<http://www.ilv.fr>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/36595/>

Entrées et sorties de formation

Entrées en formation	10
Parcours menés à terme	7
Taux d'achèvement	70 %
Période	11/2022 – 06/2026

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

Demande CPF — formations engagées

Dossiers CPF engagés	11
Montant total engagé	50 088 €
Coût moyen par dossier	4 553 €
Durée moyenne	602 h
Période	09/2022 – 04/2025
France compétences	72 %
OPCO	16 %
Reste à charge titulaire	12 %

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