

Le Répertoire National des Certifications Professionnelles (RNCP)

Résumé descriptif de la certification **Code RNCP : 32025**

Intitulé

Manager de la sécurité des données numériques

AUTORITÉ RESPONSABLE DE LA CERTIFICATION

Institut Léonard de Vinci

QUALITÉ DU(ES) SIGNATAIRE(S) DE LA CERTIFICATION

Président

Niveau et/ou domaine d'activité

I (Nomenclature de 1969)

7 (Nomenclature Europe)

Convention(s) :

Code(s) NSF :

326n Analyse informatique, conception d'architecture de réseaux

Formacode(s) :

Résumé du référentiel d'emploi ou éléments de compétence acquis

Les activités du (de la) manager de la sécurité des données numériques se répartissent en trois ensembles :

Analyse des risques

Analyse des risques inhérents au système d'information
Identification des risques d'intrusion et d'interruption des services
Analyse des risques affectant les données numériques
Choix d'un modèle de politique de sécurité

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

Conception d'une architecture de sécurité
Réponse à un appel d'offres sur les architectures de sécurité
Identification et choix des solutions de sécurité disponibles sur le marché
Respect de la réglementation
Réponse aux alertes et mise en place des solutions adaptées

Déploiement, management et audit de la sécurité des systèmes d'information et des réseaux

Sécurisation des réseaux et des services
Sécurisation des systèmes d'exploitation
Sécurisation des bases de données
Sûreté de fonctionnement
Audit de la sécurité du système d'information et des réseaux
Le (la) titulaire est capable de :
Réaliser un audit du système d'information de l'entreprise
Caractériser les atteintes possibles aux données numériques
Exercer une veille technologique sur les dispositifs de sécurité des systèmes d'information
Choisir et justifier le choix d'un modèle de politique de sécurité
Choisir une architecture de sécurité
Choisir les parades les mieux adaptées aux risques de cyber attaque
Accéder aux bases de données juridiques en matière de sécurité des données numériques
Assurer la conformité des solutions retenues avec la réglementation en cours.
Choisir les technologies de protection contre les cyber attaques (système d'exploitation, bases de données, réseaux) à même d'assurer le fonctionnement des services.

Superviser la mise en place des solutions de sécurité et organiser les programmes de tests.

Réaliser un audit technique

Réaliser un audit de sécurité

Secteurs d'activité ou types d'emplois accessibles par le détenteur de ce diplôme, ce titre ou ce certificat

Toutes entreprises et organisations publiques et privées dotées d'un système d'information. Toutes entreprises de services numériques et organismes spécialisés en cyber sécurité.

La protection des données numériques est un enjeu majeur des entreprises et des Etats, dont la complexité requiert des compétences d'autant plus pointues que la variété des menaces s'accroît. 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.

Le(la) manager de la sécurité des données numérique occupe généralement les fonctions suivantes :

Manager de la cyber sécurité

Expert(e) en sécurité des SI

Expert(e) en cyberdéfense

Responsable de la sécurité des systèmes d'information

Ingénieur cyber sécurité

Consultant(e) en sécurité des SI

Codes des fiches ROME les plus proches :

M1802 : Expertise et support en systèmes d'information

Réglementation d'activités :

Néant

Modalités d'accès à cette certification

Descriptif des composantes de la certification :

La validation des trois blocs de compétences est obligatoire pour la validation du titre :

1. Analyser les risques inhérents au système d'information d'une entreprise
2. Concevoir et organiser la sécurité des systèmes d'information et des réseaux
3. Déployer, manager et auditer la sécurité des systèmes d'information et des réseaux

Bloc de compétence :

INTITULÉ	DESCRIPTIF ET MODALITÉS D'ÉVALUATION
Bloc de compétence n°1 de la fiche n° 32025 - Analyser les risques inhérents au système d'information d'une entreprise	<p>Descriptif</p> <ul style="list-style-type: none">• Réaliser un audit du système d'information de l'entreprise• Caractériser les atteintes possibles aux données numériques• Exercer une veille technologique sur les dispositifs de sécurité des systèmes d'information• Choisir et justifier le choix d'un modèle de politique de sécurité <p>Modalités d'évaluation et de certification</p> <ul style="list-style-type: none">• Evaluation sur étude de cas donnant lieu à rapport individuel écrit et soutenance devant un jury composé de formateurs et professionnels de la sécurité informatique. <p>Obtention du titre</p> <ul style="list-style-type: none">• Bloc de compétences capitalisable.• Un certificat des compétences attestées selon les modalités d'évaluation décrites sera délivré à chaque candidat/e à l'issue de la validation du bloc de compétences n°1.

INTITULÉ**DESCRIPTIF ET MODALITÉS D'ÉVALUATION**

Bloc de compétence n°2 de la fiche n° 32025 - Concevoir et organiser la sécurité des systèmes d'information et des réseaux

Descriptif

- Choisir une architecture de sécurité
- Choisir les parades les mieux adaptées aux risques de cyber attaque
- Accéder aux bases de données juridiques en matière de sécurité des données numériques
- Assurer la conformité des solutions retenues avec la réglementation en cours

Modalités d'évaluation et de certification

- Evaluation sur étude de cas donnant lieu à rapport individuel écrit et soutenance devant un jury composé de formateurs et professionnels de la sécurité informatique.

Obtention du titre

- Bloc de compétences capitalisable.
- Un certificat des compétences attestées selon les modalités d'évaluation décrites sera délivré à chaque candidat/e à l'issue de la validation du bloc de compétences n°2.

INTITULÉ	DESCRIPTIF ET MODALITÉS D'ÉVALUATION
Bloc de compétence n°3 de la fiche n° 32025 - Déployer, manager et auditer la sécurité des systèmes d'information et des réseaux	<p>Descriptif</p> <ul style="list-style-type: none"> • Choisir les technologies de protection contre les cyber attaques (système d'exploitation, bases de données, réseaux) à même d'assurer le fonctionnement des services • Superviser la mise en place des solutions de sécurité et organiser les programmes de tests • Réaliser un audit technique • Réaliser un audit de sécurité <p>Modalités d'évaluation et de certification</p> <ul style="list-style-type: none"> • Evaluation sur étude de cas donnant lieu à rapport individuel écrit et soutenance devant un jury composé de formateurs et professionnels de la sécurité informatique. <p>Obtention du titre</p> <ul style="list-style-type: none"> • Bloc de compétences capitalisable. • Un certificat des compétences attestées selon les modalités d'évaluation décrites sera délivré à chaque candidat/e à l'issue de la validation du bloc de compétences n°3.

Validité des composantes acquises : illimitée

CONDITIONS D'INSCRIPTION À LA CERTIFICATION	OUINON	COMPOSITION DES JURYS
Après un parcours de formation sous statut d'élève ou d'étudiant	X	Président de jury : un représentant d'une entreprise partenaire Membres du jury : le directeur pédagogique, un membre du corps enseignant, deux professionnels extérieurs à l'organisme.
En contrat d'apprentissage	X	Président de jury : un représentant d'une entreprise partenaire Membres du jury : le directeur pédagogique, un membre du corps enseignant, deux professionnels extérieurs à l'organisme.
Après un parcours de formation continue	X	Président de jury : un représentant d'une entreprise partenaire Membres du jury : le directeur pédagogique, un membre du corps enseignant, deux professionnels extérieurs à l'organisme.
En contrat de professionnalisation	X	Président de jury : un représentant d'une entreprise partenaire Membres du jury : le directeur pédagogique, un membre du corps enseignant, deux professionnels extérieurs à l'organisme.

Par candidature individuelle		X	
Par expérience dispositif VAE prévu en 2013	X		Président de jury : un représentant d'une entreprise partenaire Membres du jury : le directeur pédagogique, un membre du corps enseignant, deux professionnels extérieurs à l'organisme.

	OUI	NON
Accessible en Nouvelle Calédonie		X
Accessible en Polynésie Française		X

LIENS AVEC D'AUTRES CERTIFICATIONS

ACCORDS EUROPÉENS OU INTERNATIONAUX

Base légale

Référence du décret général :

Référence arrêté création (ou date 1er arrêté enregistrement) :

Arrêté du 11 décembre 2018 publié au Journal Officiel du 18 décembre 2018 portant enregistrement au répertoire national des certifications professionnelles. Enregistrement pour 4 ans, au niveau I, avec effet au 16 septembre 2014, jusqu'au 18 décembre 2022.

Référence du décret et/ou arrêté VAE :

Références autres :

Pour plus d'informations

Statistiques :

Autres sources d'information :

www.ilv.fr

Lieu(x) de certification :

Institut Léonard de Vinci : Île-de-France - Hauts-de-Seine (92) [COURBEVOIE]

Institut Léonard de Vinci

Pôle Universitaire Léonard de Vinci – 92916 PARIS LA DEFENSE CEDEX

Lieu(x) de préparation à la certification déclarés par l'organisme certificateur :

Institut Léonard de Vinci

Pôle Universitaire Léonard de Vinci – 92916 PARIS LA DEFENSE CEDEX

Historique de la certification :