

Cybersécurité et Réseaux

RS5031 · RS · Publiée

L'essentiel

Code(s) NSF	326
Formacode(s)	31006
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	10/10/2019
Date d'échéance	10/10/2024

Certificateur(s)

CFA INSTA · SIRET : 50947289000029

Partenaires habilités

3 organismes habilités, d'après la liste publiée par France compétences : 1 à former et organiser l'évaluation et 2 à former.

Organisme	SIRET	Habilitation
AMBIENT IT	81227101300037	Former
AMBIENT IT	81227101300045	Former
SORBONNE UNIVERSITE	13002338500011	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

Cette certification offre les compétences de spécialisation nécessaires à la conduite d'audits en sécurité des systèmes informatiques et des réseaux. Elle permet d'acquérir les connaissances indispensables pour analyser le niveau de fiabilité et de sécurité d'un système d'information, d'en déceler les points de faiblesse et de dresser la cartographie des risques. Après rédaction d'un rapport d'audit, le certifié sera en mesure de rechercher et proposer des solutions, d'élaborer une politique générale de cybersécurité et de mettre en place des protocoles de sécurité ainsi qu'un système de détection, de traitement et de contrôle des anomalies.

COMPÉTENCES ATTESTÉES

Analyser les enjeux économiques et juridiques liés aux risques d'altération du système d'information.

Analyser la stratégie de cybersécurité de l'organisation et la politique de gestion des données et des traitements

Identifier et caractériser les menaces de dysfonctionnement du système d'information

Analyser la gestion des identités et des accès et les flux d'informations critiques de l'activité d'un système d'information

Synthétiser les analyses liées à la vulnérabilité du système d'information

Définir les indicateurs de fiabilité du système d'information

Rédiger le rapport d'audit de sécurité du système d'information

Exploiter le rapport d'audit de l'organisation pour identifier les axes correctifs à

rechercher et proposer des solutions de protection du système d'information.
 Caractériser les solutions et les outils du marché et élaborer la politique de sécurité du système d'information
 Evaluer les ressources humaines et matérielles à mobiliser et déployer les solutions techniques retenues
 Analyser les différents protocoles réseaux (IP, IMCP, UDP, TCP, ...) pour concevoir des architectures sécurisées.
 Mettre en place les pare-feux client/serveur des applications web
 Mettre en place les contrats de maintenance et de backup des matériels
 Concevoir les procédures en cas d'interruption de service pour organiser les plans de continuité l'activité et les services de l'organisation.
 Identifier un référent interne et expliciter ses missions pour garantir la bonne gestion de la politique de sécurité et accompagner l'organisation dans la durée.
 Mettre en place et animer les instances de pilotage pour superviser le déploiement
 Informer et sensibiliser l'ensemble des collaborateurs à la politique de sécurité de l'organisation
 Concevoir les protocoles d'audits internes et les planifier
 Mettre en place le système de contrôle et les procédures de traitement des incidents
 Concevoir des mises à l'épreuve de la politique de sécurité
 Mettre à jour les composants techniques du système pour intégrer les évolutions fonctionnelles et techniques
 Assurer une veille technologique sur l'évolution des cyber-risques

Secteur d'activité et type d'emploi

RÉGLEMENTATIONS D'ACTIVITÉ

Aucun

Voies d'accès

MODALITÉS D'ACCÈS

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

PRÉREQUIS À L'ENTRÉE EN FORMATION

Niveau 5 et des connaissances en réseau sont appréciées.

COMPOSITION DU JURY — FORMATION INITIALE

Trois personnes seront désignées pour représenter le jury de certification :

- Un responsable pédagogique référent
- Deux personnes extérieures à la formation appartenant à l'entreprise

Le

jury sera responsable de la remise de la certification.

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

Trois personnes

seront désignées pour représenter le jury de certification :

- Un responsable pédagogique référent
- Deux

personnes extérieures à la formation appartenant à l'entreprise

Le

jury sera responsable de la remise de la certification.

Base légale

Date de décision	10/10/2019
Durée de l'enregistrement	5 ans
Date d'échéance de l'enregistrement	10/10/2024

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rs/5031/>

Entrées et sorties de formation

Entrées en formation	41
Parcours menés à terme	43
Taux d'achèvement	105 %
Période	02/2022 – 11/2024

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

Demande CPF — formations engagées

Dossiers CPF engagés	57
Montant total engagé	278 009 €
Coût moyen par dossier	4 877 €
Durée moyenne	34 h
Période	09/2021 – 09/2024
France compétences	51 %
OPCO	36 %
France Travail	8 %
Reste à charge titulaire	4 %
Entreprise	1 %
Compte d'engagement citoyen	0 %

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