

Référent cybersécurité en TPE/PME

RS3818 · RS · Publiée

L'essentiel

Code(s) NSF	326p
Type d'enregistrement	Enregistrement sur demande
Date d'échéance	31/12/2021

Certificateur(s)

CCI FRANCE · SIRET : 18750002000073

Partenaires habilités

15 organismes habilités, d'après la liste publiée par France compétences : 15 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
AS FO BEARN SOULE BIGORRE	7823554080002 5	Former et organiser l'évaluation
CCIT ALSACE EUROMETROPOLE	1300226760001 4	Former et organiser l'évaluation
CCIT BORDEAUX GIRONDE	1300228580001 8	Former et organiser l'évaluation
CHAMB COMMERCE ET INDUSTRIE HAUTES ALPES	1805000190001 3	Former et organiser l'évaluation
CHAMBRE COMMERCE ET INDUSTRIE GRENOBLE	1838300170001 2	Former et organiser l'évaluation
CHAMBRE COMMERCE INDUSTRIE DE LA DROME	1826300120001 7	Former et organiser l'évaluation
CHAMBRE COMMERCE INDUSTRIE MAINE LOIRE	1300046090001 7	Former et organiser l'évaluation
CHAMBRE DE COMMERCE ET D INDUSTRIE	1879000140001 5	Former et organiser l'évaluation
CHAMBRE DE COMMERCE ET D'INDUSTRIE	1877091830023 5	Former et organiser l'évaluation
CHAMBRE DE COMMERCE ET D'INDUSTRIE DE REGION BRETAGNE	1835000400031 0	Former et organiser l'évaluation

Liste complète des 15 partenaires habilités : <https://data.aktaconseil.fr/certifications/rs3818-referent-cybersecurite-en-tpe-pme/partenaires>

Résumé de la certification

OBJECTIFS ET CONTEXTE

Les Très petites entreprises (TPE) et les Petites et moyennes entreprises (PME) représentent une source importante d'emplois et d'innovations. Elles évoluent aujourd'hui dans un environnement de plus en plus numérique, qui favorise incontestablement leur compétitivité et leur croissance. Pour autant, les nouvelles technologies de l'information et de la communication lorsqu'elles sont mal maîtrisées, peuvent être à l'origine de vulnérabilités et faciliter les attaques sur l'entreprise.

Pour y faire face, les TPE/PME n'ont pas toujours la possibilité de recruter des profils dédiés à la sécurité informatique. Qui plus est, l'approche qu'elles ont de la gestion des infrastructures informatiques varie en fonction de l'utilisation qui en est faite, de leur taille, du secteur économique et du budget qui y est consacré. De fait, à l'exception de certains secteurs très spécifiques, le niveau de perception et de prise en charge du cyber-risque dans les TPE/PME est aujourd'hui faible.

Afin de promouvoir un environnement favorable au développement économique et de préserver le patrimoine immatériel de ces entreprises, il convient aujourd'hui, dans une démarche d'intelligence économique, de mettre en place des solutions humaines et techniques adaptées aux spécificités des TPE/PME.

COMPÉTENCES ATTESTÉES

- Dans une perspective de veille sur l'intelligence et la sécurité économiques identifier et analyser des problèmes de cybersécurité.
- Prendre en compte les multiples aspects de la sécurité au sein d'une organisation.
- Dans une perspective de sécurisation, identifier les menaces liées à l'utilisation de l'informatique et des réseaux internet, réseaux privés d'entreprises, réseaux publics.
- Adopter les notions d'hygiène de base de la cybersécurité pour les organisations et les individus.
- En utilisant les outils informatiques et les services inhérents, protéger le patrimoine immatériel de l'entreprise.
- Respecter les obligations et prendre en compte les responsabilités juridiques de la cybersécurité.
- Pour faire face aux attaques, présenter les précautions techniques et juridiques, en sensibilisant les utilisateurs sur les enjeux associés.
- Mettre en place un protocole de gestion des incidents informatiques, de la détection à la gestion de crise.
- Afin de prendre en compte un contexte global d'intelligence et de sécurité économiques, identifier et analyser les problèmes de cybersécurité.
- Afin de protéger l'entreprise, délimiter le patrimoine immatériel de l'entreprise rentrant dans les enjeux de la cybersécurité.
- Pour une meilleure prévention, identifier les menaces liées à l'utilisation de l'outil informatique (internet, réseau entreprise, réseau public...).
- Pour déterminer les actions à mettre en œuvre, identifier les profils des collaborateurs à sensibiliser.
- Afin de mettre en place une démarche de prévention, définir les actions à réaliser et les types de support de sensibilisation à déployer.
- Afin de mettre en place les process de protection adaptés, caractériser les différents types d'attaques.
- Afin de respecter les cadres contractuels, identifier les responsabilités juridiques de l'entreprise.

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

Pas de prérequis.

Base légale

Date d'échéance de l'enregistrement 31/12/2021

Liens avec d'autres certifications

NOUVELLE(S) CERTIFICATION(S)

RS5568

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rs/3818/>

Demande CPF — formations engagées

Dossiers CPF engagés	254
Montant total engagé	353 460 €
Coût moyen par dossier	1 392 €
Durée moyenne	21 h
Période	01/2020 – 01/2022
France compétences	95 %
France Travail	3 %
Reste à charge titulaire	2 %
Entreprise	0 %
Compte d'engagement citoyen	0 %
Régions	0 %

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