Certification PECB - Fondamentaux de la cyber sécurité

CATEGORIE : B

Vue d'ensemble

Domaine(s) d'activité professionnel dans lequel(s) est utilisé la certification :

Transverse :
- **Tous secteurs d'activité**

Code(s) NAF : **62.02A**
Code(s) NSF : **326**
Code(s) ROME : **M1805**, **M1801**
Formacode : **31006**

Date de création de la certification : **01/03/2014**
Mots clés : **Cyber attaques**, **Systèmes d'information**, **Sécurité**, **Cyber sécurité**

Identification

Identifiant : **4316**
Version du : **19/12/2018**

Références

Consensus, reconnaissance ou recommandation :
Formalisé :
- **Livre blanc défense et sécurité nationale Mission confiée par le Président de la République à Jean-Marie GUEHENNO, Conseiller maître à la Cour des Comptes - 2013**

Non formalisé :
- **Agence nationale de la sécurité des systèmes d'information (ANSSI) Bonnes pratiques / 2009-2018**

Norme(s) associée(s) :
- https://www.iso.org/-files/live/sites/isoorg/files/-store/fr/PUB100427_fr.pdf

Descriptif

Objectifs de l'habilitation/certification

Adossée à la norme ISO 27032, la certification recouvre les compétences essentielles en matière de cyber sécurité. Elle vise à permettre une approche méthodique de la sécurité de l'information, de la sécurité des réseaux et de l'Internet et de la protection des infrastructures d'information essentielles.

Lien avec les certifications professionnelles ou les CQP enregistrés au RNCP

- Aucun

Descriptif général des compétences constituant la certification

La certification recouvre cinq compétences-clés :

Analyser le système d'information de l'entreprise, afin de repérer ses points de faiblesse au regard des menaces d'intrusion et de perte de données inhérentes au cyberespace.
Etablir le cahier des charges de cyber sécurité de son entreprise conformément à la norme ISO 27032, afin de répondre aux impératifs

Public visé par la certification

Tous publics

de protection de l'activité dans le cadre du budget disponible.
Elaborer les parades adaptées aux menaces d'intrusion et de pertes de données inhérentes au cyberespace, conformément au cahier des charges et au budget imparti.
Etablir le schéma général de cyber sécurité à l'intention des responsables de l'entreprise, en vue de préparer un plan de communication vers l'ensemble du personnel.
Concevoir un plan de formation des personnels aux bonnes pratiques en matière de cyber sécurité conformes à la norme ISO 27032, afin d'assurer leur implication à tous les niveaux de l'entreprise.

Modalités générales

La formation conduisant à la certification est proposée en quatre journées (28 heures), en présentiel.

Cette formation est basée sur les meilleures pratiques en matière de cyber sécurité.

Les cours théoriques sont ponctués par de la mise en application. La répartition théorique et pratique est de 40-60%.

Les exercices pratiques sont panachés de travaux dirigés et guidés par l'apprenant et d'exercices en pleine autonomie, afin d'assurer une assimilation des savoir-faire requis.

Liens avec le développement durable

Aucun

Valeur ajoutée pour la mobilité professionnelle et l'emploi

Pour l'individu

La certification permet aux individus de :

Disposer des compétences nécessaires à la définition et à la mise en œuvre d'un programme de cyber sécurité : elle fournit une solution réaliste aux individus dans la protection de leurs données privées et pour la protection des données des organisations contre les escroqueries de phishing, les cyber attaques, le piratage informatique et autres menaces cybernétiques.
Appartenir au réseau de formateurs et certifiés PECB sollicités pour leurs compétences auprès des clients à l'international.
Répondre aux exigences de postes correspondant à ces caractéristiques : RSSI, responsable de la gestion des risques en sécurité de l'information, consultant en cyber sécurité.

Pour l'entité utilisatrice

La certification fournit des lignes directrices concernant la protection et la viabilité à long terme des processus d'affaires dans un contexte de cyber sécurité. Elle permet aux professionnels d'élaborer un cadre identifiant les processus les plus vulnérables aux cyber attaques.

La certification permet aux entités utilisatrices de :

Faciliter la gestion des compétences et le recrutement en s'appuyant sur une certification reconnue.
Favoriser la collaboration inter-organisationnelle en partageant un langage et des processus communs.
Garantir aux parties prenantes de l'organisation un certain standard de qualité.
Le maintien dans le temps de la certification garantit la tranférabilité des compétences d'une entité utilisatrice à une autre.

Evaluation / certification

Pré-requis

Pas de prérequis.

Centre(s) de passage/certification

Compétences évaluées

Evaluation de la totalité des cinq compétences-clés :

Analyser le système d'information de l'entreprise, afin de repérer ses points de faiblesse au regard des menaces d'intrusion et de perte de données inhérentes au cyberespace.
Etablir le cahier des charges de cyber sécurité de son entreprise conformément à la norme ISO 27032, afin de répondre aux impératifs de protection de l'activité dans le cadre du budget disponible.
Elaborer les parades adaptées aux menaces d'intrusion et de pertes de données inhérentes au cyberespace, conformément au cahier des charges et au budget imparti.
Etablir le schéma général de cyber sécurité à l'intention des responsables de l'entreprise, en vue de préparer un plan de communication vers l'ensemble du personnel.
Concevoir un plan de formation des personnels aux bonnes pratiques en matière de cyber sécurité conformes à la norme ISO 27032, afin d'assurer leur implication à tous les niveaux de l'entreprise.

Niveaux délivrés le cas échéant (hors nomenclature des niveaux de formation de 1969)

Pas de niveau.

- Adenium (Paris)
- Devoteam (Paris – Bruxelles – Luxembourg)
- Fidens (Paris – Lyon)
- Global Knowledge (Rueil Malmaison)
- HTS Experts (Valencienne)
- It-Gnosis (Paris)
- Orsys (Paris–Bruxelles–Luxembourg–Genève)
- Provadys (Paris)
- SCASSI (Toulouse – Paris – Madrid)
- Sekoia (Paris)
- Sodifrance (Rennes - Nantes)
- Sysdream (Paris)

La validité est Temporaire

La certification est valable 3 années.
Possibilité de certification partielle : non
Matérialisation officielle de la certification :
Remise d'un certificat de compétences PECB sous accréditation IAS (ISO 17024)

Plus d'informations

Statistiques

80 certificats sont délivrés en moyenne annuelle.

Autres sources d'information

https://pecb.com/fr/education-and-certification-for-individuals/iso-iec-27032