Fondamentaux de la cyber sécurité

CATEGORIE : C

Vue d'ensemble

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

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

Code(s) NAF : —
Code(s) NSF : **415z**, **310**
Code(s) ROME : **M1802**, **M1801**
Formacode : **31009**

Date de création de la certification : **01/02/2016**
Mots clés : **PREVENTION**, **RISQUE**, **SECURITE**, **Management**

Identification

Identifiant : **3628**
Version du : **28/06/2018**

Références

Consensus, reconnaissance ou recommandation :
Formalisé :
- **Rapport au gouvernement : La transformation numérique de l'économie française – Novembre 2014**

Non formalisé :
- **Programme gouvernemental « Transition-numérique » (lancé en 2012)**

Descriptif

Objectifs de l'habilitation/certification

La certification recouvre un ensemble de compétences permettant de protéger son matériel et les réseaux de l'entreprise contre les virus et les cyber attaques. Elle vise plus généralement à l'acquisition des bonnes pratiques de sécurité informatique.

Lien avec les certifications professionnelles ou les CQP enregistrés au RNCP

- Aucun

Descriptif général des compétences constituant la certification

La certification recouvre neuf compétences-clés :

Mettre à jour son ordinateur et ses logiciels afin de préserver l'étanchéité des pare-feux
Sécuriser le cloud et les mots de passe en accord avec l'organisation de l'entreprise
Sauvegarder les données et fichiers en observation des règles de sécurité
Protéger sa boite-mail contre tous types de dangers d'intrusion
Adopter les gestes de premier secours en cas d'attaque informatique
Evaluer les dégâts d'une attaque informatique de façon exhaustive
Utiliser la mise en quarantaine pour limiter la propagation d'une attaque
Décontaminer son ordinateur à la suite d'une attaque informatique
Capitaliser l'expérience d'une attaque informatique en vue d'améliorer

Public visé par la certification

Tous publics

le plan de prévention

Modalités générales

La formation conduisant à la certification est entièrement digitalisée. Le parcours, équivalent à 20 heures de contenu en formation classique, est étalé sur quatre semaines et comprend :

Des vidéos pédagogiques
Des activités de mise en pratique et simulations
Des ressources complémentaires (articles, outils, modèles, ...)
Des forums de discussion
Des classes virtuelles avec l'expert
Les outils d'évaluation
Les participants ont des occasions très régulières d'échanger avec l'expert UNOW, par écrit ou en direct grâce aux classes virtuelles. Ils sont accompagnés dans leur montée en compétence, en contact étroit avec l'équipe pédagogique chargée d'animer la formation et de suivre leur progression.

Liens avec le développement durable

niveau 2 : certifications et métiers pour lesquels des compétences évoluent en intégrant la dimension du développement durable

Valeur ajoutée pour la mobilité professionnelle et l'emploi

Pour l'individu

Les compétences acquises permettent aux certifiés de protéger leurs outils numériques contre les virus, les attaques et tous types d'intrusions dans le système d'information. Ceci permet d'éviter des pertes de temps importantes, voire des pertes d'informations, et constitue un facteur important de diminution du stress professionnel.

Pour l'entité utilisatrice

Les cyber attaques présentent des risques importants pour les entreprises. Leur prévention repose sur la compétence de l'ensemble des collaborateurs en matière de cyber sécurité. La certification des salariés revêt ainsi un caractère stratégique. La certification est délivrée à l'issue de sessions de formation en ligne qui peuvent être suivies sur le temps de travail.

Evaluation / certification

Pré-requis

Pas de pré-requis.

Compétences évaluées

Evaluation de la totalité des neuf compétences-clés :

Mettre à jour son ordinateur et ses logiciels afin de préserver l'étanchéité des pare-feux
Sécuriser le cloud et les mots de passe en accord avec l'organisation de l'entreprise
Sauvegarder les données et fichiers en observation des règles de sécurité
Protéger sa boite-mail contre tous types de dangers d'intrusion
Adopter les gestes de premier secours en cas d'attaque informatique
Evaluer les dégâts d'une attaque informatique de façon exhaustive

Centre(s) de passage/certification

- UNOW 22, rue Chapon 75003 PARIS

Utiliser la mise en quarantaine pour limiter la propagation d'une attaque
Décontaminer son ordinateur à la suite d'une attaque informatique
Capitaliser l'expérience d'une attaque informatique en vue d'améliorer le plan de prévention

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

Pas de niveau.

La validité est Permanente

Possibilité de certification partielle : non
Matérialisation officielle de la certification :
Certificat de compétences

Plus d'informations

Statistiques

Moyenne de 120 certifiés par an.

Autres sources d'information

https://www.unow.fr