Le Répertoire National des Certifications Professionnelles (RNCP)

Résumé descriptif de la certification **Code RNCP : 27836**

Intitulé

Expert(e) en sécurité digitale

AUTORITÉ RESPONSABLE DE LA CERTIFICATION	QUALITÉ DU(ES) SIGNATAIRE(S) DE LA CERTIFICATION
ASTON Institut	Directrice

Niveau et/ou domaine d'activité

I (Nomenclature de 1969)

7 (Nomenclature Europe)

Convention(s) :

Code(s) NSF :

326 Informatique, traitement de l'information, réseaux de transmission

Formacode(s) :

Résumé du référentiel d'emploi ou éléments de compétence acquis

L'expert en sécurité digitale est responsable de la conception et de la sécurisation du système d'information de l'organisme. Interlocuteur privilégié de la DSI ou de la DG, il est chargé de mettre en place un système de management de la sécurité de l'information, dont il s'assure qu'il est d'une part en adéquation avec les objectifs généraux de l'entreprise et d'autre part compris et approprié par les équipes techniques et par les acteurs de la structure. Pour cela, il développe une vision globale du système de management de la sécurité de l'information, prenant en compte les impacts économiques, organisationnels, humains, techniques et juridiques pour le système cible. Polyvalent, l'expert en sécurité digitale est donc à la fois compétent sur les questions techniques, managériales et stratégiques.

Ainsi, l'expert en sécurité digitale accomplit toutes les activités en lien avec la conception, la mise en application et la gestion de la sécurité de l'information pour un système cible. Il est susceptible de réaliser chacune des étapes de la mise en œuvre d'un SMSI : définition des objectifs, organisation générale de la structure, mise en œuvre de la politique de défense, évaluation du niveau de sécurité, évaluation des impacts, définition des objectifs de sécurité, animation des équipes, conseil auprès des décideurs, suivi des budgets…

1) Conception d'un plan stratégique de sécurité pour un système cible

L'expert en sécurité digitale analyse les besoins d'un système cible donné et formalise un plan stratégique de sécurité. Pour cela il prend en compte l'ensemble des facteurs contraignants internes et externes, et s'intéresse notamment au positionnement business de l'entreprise, afin de formaliser un schéma directeur des Systèmes de Sécurité de l'Information et d'émettre des préconisations à destination des donneurs d'ordres.

2) Structuration d'une solution technique et organisationnelle répondant aux besoins de sécurité du système cible

En accord avec le schéma directeur SSI préalablement défini, ce professionnel structure des solutions adaptées aux besoins et aux contraintes du système cible. Pour cela, il est amené réaliser des études de marché concernant les technologies, les architectures et les prestataires susceptibles de contribuer à la structuration de la solution. Il est également chargé d'implémenter un SMSI (système de management de la sécurité de l'information) et les indicateurs de pilotage stratégiques, fonctionnels et opérationnels qui lui sont inhérents.

3) Conduite d'un audit de sécurité des systèmes d'information

Une fois la solution de sécurité implémentée dans un système cible, l'expert en sécurité digitale réalise des audits de sécurité afin d'en vérifier l'opérationnalité. Il prépare et réalise l'ensemble des phases de l'audit suite à quoi il rédige des préconisations d'améliorations ou de corrections à apporter. Il est également susceptible de réaliser, d'une part, des pentest ou test d'intrusion dans le système cible, c'est-à-dire tenter de trouver les failles du système en simulant une attaque. Et d'autre part, il peut réaliser des forensics ou investigations numériques légales, c'est-à-dire recueillir des preuves numériques d'un acte de cyber-criminalité.

4) Maintien en condition opérationnelle de la sécurité de l'information

Les préconisations suite aux audits de sécurité permettent le maintien en condition opérationnelle de la sécurité de l'information. Des modifications sont apportées à la gestion du système de sécurité notamment concernant la révision des indicateurs de suivi (de nouveaux indicateurs peuvent être créés, ou le niveau d'alerte concernant ces indicateurs peut être revu). Des modifications sont également apportées aux dispositifs techniques ou organisationnels en place. L'expert en sécurité digitale est garant, d'une part, du maintien des objectifs budgétaires liés à ce maintien en condition opérationnel, et d'autre part, du respect de la stratégie de l'entreprise.

5) Accompagnement de la mise en œuvre de la politique de sécurité SI d'un système cible

Enfin, les modifications apportées à la gestion de la sécurité doivent être mises en œuvre de manière homogène à tous les niveaux de l'entreprise. Pour cela, l'expert en sécurité digitale accompagne la direction dans la mise en place des outils de déploiement de la politique, notamment en termes de recrutements, de sensibilisation ou de formation des collaborateurs. Il s'assure également de la mise en œuvre d'une charte informatique conforme à la stratégie de sécurisation digitale de l'entreprise.

Les capacités attestées renvoient à cinq grands domaines de compétences couvrant l'ensemble de la conception et de la mise en œuvre de la sécurité d'un système cible :

BLOC 1 : Concevoir un plan stratégique de sécurité pour un système cible

C1. Identifier l'ensemble des enjeux (techniques, humains, organisationnels, financiers et juridiques) liés aux besoins de sécurité d'un système cible afin de rédiger un schéma directeur SSI

C2.Mener une analyse de risques, auquel est exposé un système d'information afin de formaliser des objectifs de sécurité de l'organisation

C3. Conceptualiser et formaliser des préconisations adaptées au système cible en tenant compte du principe de sécurité en profondeur, du R.O.I (Return On Investment) et du B.I.A. (Business Impact Analysis), afin de convaincre des donneurs d'ordre.

BLOC 2 : Structurer une solution technique et organisationnelle répondant aux besoins de sécurité du système cible

C4 Concevoir un cahier des charges fonctionnel et technique dans le but de diffuser un appel d'offres

C5.Formaliser une proposition technique et organisationnelle complète, en en réalisant un benchmark des produits ou dispositifs de sécurité dans le but de convaincre des décideurs
C6. Extrapoler une politique de sécurité des systèmes d'information basée sur une analyse de risques.
C7. Concevoir des indicateurs de différents niveaux (stratégiques, fonctionnels et opérationnels) liés à la sécurité de l'information
BLOC 3 : Conduire un audit de sécurité des systèmes d'information
C8. Piloter l'audit d'un système d'information en préparant les différentes phases afin d'estimer ou de faire estimer le niveau de sécurité d'un SI
C9. Réaliser une ou plusieurs phases de l'audit en effectuant des tests de vulnérabilité et d'intrusion afin d'identifier les failles de sécurité du système
C10. Réaliser une investigation numérique légale (Forensic) en appliquant des protocoles d'investigation numérique respectant les procédures légales afin d'apporter des preuves d'un acte malveillant
C11.Formaliser les résultats de l'audit de sécurité afin d'émettre des préconisations techniques et organisationnelles
BLOC 4 : Maintenir en condition opérationnelle de la sécurité de l'information
C.12 Gérer les incidents de sécurité en apportant des réponses adaptées à chaque incident grâce à la lecture des indicateurs afin de maintenir le niveau de sécurité en accord avec la stratégie de l'entreprise.
C13. Analyser le dépassement des indicateurs de pilotage et de contrôle en relevant des incidents et en vérifiant la pertinence des alertes afin de garantir l'opérationnalité de la protection
C14. Garantir le suivi des risques de façon constant en réalisant une veille sur les nouvelles menaces, sur les solutions de sécurité, afin de prévenir les failles du système
C15. Assurer le suivi des budgets liés à la sécurité de l'information d'une organisation. afin de maintenir les objectifs fixés
BLOC 5 : Accompagner la mise en œuvre de la politique de sécurité d'un système cible
C16. Conseiller les décideurs en identifiant les profils d'agent impactés par la sécurité du SI pour l'ensemble des services de la structure, et en identifiant les résistances, afin de fluidifier la mise en œuvre sur le terrain
C17. Sensibiliser et former les équipes en rédigeant, en diffusant et en mettant en application des documents liés à la SSI afin de susciter l'adhésion des acteurs quant aux règles de sécurité
C18. Piloter la formation et le recrutement des équipes techniques, en s'assurant de la montée en compétence en interne afin d'atteindre une maturité de l'entreprise sur les questions de sécurité

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

Secteurs d'activité

Les fonctions exercées par l'expert-e- en sécurité digitale peuvent concerner toute structure disposant d'un système d'information et susceptible de mettre en œuvre un système de management de la sécurité de l'information. Elles sont donc transversales à tout secteur d'activité.
L'expert-e- en sécurité digitale peut exercer dans toute entreprise de grande taille, tout secteur d'activité confondu (industrie, énergie, télécommunications, banques, services...). Il peut aussi exercer ses fonctions dans le SI d'une institution publique de grande taille.
Il peut également intégrer une PME en informatique, spécialisée en sécurité digitale ou délivrant des prestations de service auprès de grands comptes. Des cabinets de conseil spécialisés en informatique sont aussi intéressés par des profils experts en sécurité digitale.

Enfin, il peut intégrer une agence publique pour la sécurité telle que l'ANSSI (Agence Nationale pour la Sécurité des Systèmes d'Information) ou la DCPJ (Direction Centrale de Police Judiciaire).

Type emplois accessibles

Expert en sécurité digitale - Expert en cyberdéfense - Expert en cybersécurité - Consultant en sécurité des systèmes d'information - Chef de projet en sécurité des systèmes d'information - Pentester - Auditeur en sécurité des systèmes d'information - Architecte en sécurité des systèmes d'information - Assistant RSSI - IT Risk Manager (Junior) - Administrateur système réseau et sécurité

Codes des fiches ROME les plus proches :

M1801 : Administration de systèmes d'information
M1802 : Expertise et support en systèmes d'information
M1803 : Direction des systèmes d'information
M1806 : Conseil et maîtrise d'ouvrage en systèmes d'information

Modalités d'accès à cette certification

Descriptif des composantes de la certification :

La certification comporte deux composantes liées aux cinq capacités énumérées ci-dessus :

1. Cas pratique en groupe :

a. Elaboration et restitution d'une analyse de risques SSI (sécurité des systèmes d'information) :
b. Réalisation et présentation d'un test d'intrusion :
c. Réalisation d'une investigation Forensic
d. Etude de cas sur le SMSI (Système de Management des systèmes d'information)
e. Présentation d'une veille en lien avec un sujet technologique actuel
f. Présentation d'un cahier des charges fonctionnel

2. Mémoire professionnel final & soutenance :

Structuration du mémoire :

- Introduction (description du contexte professionnel)
- Description du SI de l'entreprise (dans le respect de la confidentialité imposée par l'entreprise)
- Description des missions effectuées pendant la période en entreprise

- Rapport d’une partie d’un audit réalisé dans l’entreprise
- Plan de sensibilisation et/ou de formation des collaborateurs de l’entreprise

Bloc de compétence :

INTITULÉ	DESCRIPTIF ET MODALITÉS D'ÉVALUATION
Bloc de compétence n°1 de la fiche n° 27836 - Accompagner la mise en œuvre de la politique de sécurité d’un système cible	**Descriptif :** •Conseiller les décideurs en identifiant les profils d’agent impactés par la sécurité du SI pour l’ensemble des services de la structure, et en identifiant les résistances, afin de fluidifier la mise en œuvre sur le terrain •Sensibiliser et former les équipes en rédigeant, en diffusant et en mettant en application des documents liés à la SSI afin de susciter l’adhésion des acteurs quant aux règles de sécurité •Piloter la formation et le recrutement des équipes techniques, en s’assurant de la montée en compétence en interne afin d’atteindre une maturité de l’entreprise sur les questions de sécurité **Modalités d'évaluation :** Modalité II : Mémoire professionnel Partie consacrée au plan de sensibilisation ou de formation
Bloc de compétence n°2 de la fiche n° 27836 - Concevoir un plan stratégique de sécurité pour un système cible	**Descriptif :** •Identifier l’ensemble des enjeux (techniques, humains, organisationnels, financiers et juridiques) liés aux besoins de sécurité d’un système cible afin de rédiger un schéma directeur SSI •Mener une analyse de risques, auquel est exposé un système d’information afin de formaliser des objectifs de sécurité de l'organisation •Conceptualiser et formaliser des préconisations adaptées au système cible en tenant compte du principe de sécurité en profondeur, du R.O.I (Return On Investment) et du B.I.A. (Business Impact Analysis), afin de convaincre des donneurs d’ordre. **Modalités d'évalauation :** Modalité I.a : Elaboration et restitution d’une analyse de risques SSI
Bloc de compétence n°3 de la fiche n° 27836 - Structurer une solution technique et organisationnelle répondant aux besoins de sécurité du système cible	**Descriptif :** •Concevoir un cahier des charges fonctionnel et technique dans le but de diffuser un appel d'offres •Formaliser une proposition technique et organisationnelle complète, en en réalisant un benchmark des produits ou dispositifs de sécurité dans le but de convaincre des décideurs •Extrapoler une politique de sécurité des systèmes d'information basée sur une analyse de risques. •Concevoir des indicateurs de différents niveaux (stratégiques, fonctionnels et opérationnels) liés à la sécurité de l'information **Modalités d'évalauation :** Modalité I.f : Présentation d’un cahier des charges fonctionnel Modalité I.d : Etude de cas sur un SMSI

INTITULÉ	DESCRIPTIF ET MODALITÉS D'ÉVALUATION
Bloc de compétence n°4 de la fiche n° 27836 - Conduire d'un audit de sécurité des systèmes d'information	**Descriptif :** •Piloter l'audit d'un système d'information en préparant les différentes phases afin d'estimer ou de faire estimer le niveau de sécurité d'un SI •Réaliser une ou plusieurs phases de l'audit en effectuant des tests de vulnérabilité et d'intrusion afin d'identifier les failles de sécurité du système •Réaliser une investigation numérique légale (Forensic) en appliquant des protocoles d'investigation numérique respectant les procédures légales afin d'apporter des preuves d'un acte malveillant •Formaliser les résultats de l'audit de sécurité afin d'émettre des préconisations techniques et organisationnelles **Modalités d'évaluation :** Modalité II : Mémoire professionnel Partie consacrée à l'audit de sécurité d'un SI Modalité I.b : Réalisation et présentation d'un test d'intrusion Modalité I.c : Réalisation d'une investigation numérique légale (Forensic)
Bloc de compétence n°5 de la fiche n° 27836 - Maintenir en condition opérationnelle de la sécurité de l'information	**Descriptif :** •Gérer les incidents de sécurité en apportant des réponses adaptées à chaque incident grâce à la lecture des indicateurs afin de maintenir le niveau de sécurité en accord avec la stratégie de l'entreprise. •Analyser le dépassement des indicateurs de pilotage et de contrôle en relevant des incidents et en vérifiant la pertinence des alertes afin de garantir l'opérationnalité de la protection •Garantir le suivi des risques de façon constant en réalisant une veille sur les nouvelles menaces, sur les solutions de sécurité, afin de prévenir les failles du système •Assurer le suivi des budgets liés à la sécurité de l'information d'une organisation. afin de maintenir les objectifs fixés **Modalités d'évaluation :** Modalité I.d : Présentation d'une gestion d'incidents au sein d'un SMSI Modalité I.d : Etude de cas sur un SMSI Modalité I.e : Veille technologique

Validité des composantes acquises : illimitée

CONDITIONS D'INSCRIPTION À LA CERTIFICATION	OUI	NON	COMPOSITION DES JURYS
Après un parcours de formation sous statut d'élève ou d'étudiant	X		5 personnes composent le jury : •2 membres ASTON •3 professionnels externes à ASTON
En contrat d'apprentissage		X	
Après un parcours de formation continue	X		5 personnes composent le jury : •2 membres ASTON •3 professionnels externes à ASTON
En contrat de professionnalisation	X		5 personnes composent le jury : •2 membres ASTON •3 professionnels externes à ASTON
Par candidature individuelle	X		5 personnes composent le jury : •2 membres ASTON •3 professionnels externes à ASTON

Par expérience dispositif VAE prévu en 2013	X		5 personnes composent le jury : •2 membres ASTON •3 professionnels externes à ASTON

	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 23 février 2017 publié au Journal Officiel du 03 mars 2017 portant enregistrement au répertoire national des certifications professionnelles. Enregistrement pour cinq ans, au niveau I, sous l'intitulé "Expert(e) en sécurité digitale" avec effet au 06 décembre 2013, jusqu'au 03 mars 2022.

Référence du décret et/ou arrêté VAE :

Références autres :

Pour plus d'informations

Statistiques :

10 titulaires de la certification par an en moyenne

Autres sources d'information :

alternance@aston-ecole.com

http://www.aston-ecole.com/esd

Lieu(x) de certification :

ASTON Institut : Île-de-France - Val-de-Marne (94) [ARCUEIL]

ASTON Institut : Nord-Pas-de-Calais Picardie - Nord (59) [LILLE]

47 - 49 avenue Edouard Vaillant - 92100 Boulogne Billancourt

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

19-21 rue du 8 mai 1945 - 94110 ARCUEIL

163 bis avenue de Bretagne Hall B - 59000 LILLE

Historique de la certification :