Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DE L'ÉDUCATION NATIONALE ET DE LA JEUNESSE

Arrêté du 6 février 2023 portant création de la spécialité « cybersécurité » de mention complémentaire et fixant ses modalités de délivrance

NOR : *MENE2303765A*

Le ministre de l'éducation nationale et de la jeunesse,

Vu le code de l'éducation, notamment ses articles D. 337-139 à D. 337-160 ;

Vu l'arrêté du 15 janvier 2019 relatif aux diplômes professionnels délivrés par le ministre de l'éducation nationale et de la jeunesse et aux brevets de techniciens supérieurs permettant la délivrance de l'autorisation d'intervention à proximité des réseaux (AIPR) ;

Vu l'arrêté du 17 juin 2020 modifié fixant les conditions d'habilitation à mettre en œuvre le contrôle en cours de formation en vue de la délivrance du certificat d'aptitude professionnelle, du baccalauréat professionnel, du brevet professionnel, de la mention complémentaire, du brevet des métiers d'art et du brevet de technicien supérieur ;

Vu l'avis du Conseil supérieur de l'éducation en date du 15 décembre 2022 ;

Vu l'avis conforme de la commission professionnelle consultative « Industrie » en date du 6 janvier 2023,

Arrête :

Art. 1er. – Il est créé la spécialité « cybersécurité » de mention complémentaire dont la définition et les conditions de délivrance sont fixées conformément aux dispositions du présent arrêté.

Ce diplôme est classé au niveau 4 du cadre national des certifications professionnelles.

La présentation du diplôme figure en annexe I du présent arrêté.

Art. 2. – Le référentiel des activités professionnelles est défini en annexe II, et le référentiel de compétences est défini en annexe III.

Art. 2 *bis*. – Les compétences relatives à l'intervention à proximité des réseaux définies en annexe II de l'arrêté du 15 janvier 2019 relatif aux diplômes professionnels délivrés par le ministre de l'éducation nationale et de la jeunesse et aux brevets de techniciens supérieurs permettant la délivrance de l'autorisation d'intervention à proximité des réseaux (AIPR) complètent les compétences définies en annexes du présent arrêté. Les compétences définies en annexe II de l'arrêté du 15 janvier 2019 précité sont évaluées au cours des épreuves professionnelles.

Art. 3. – Le référentiel d'évaluation est fixé en annexe IV qui comprend les parties IV-1 relative aux unités constitutives du diplôme, IV-2 relative au règlement d'examen, et IV-3 relative à la définition des épreuves sous la forme ponctuelle et sous la forme du contrôle en cours de formation.

Art. 4. – L'accès en formation à la spécialité « cybersécurité » de mention complémentaire est ouvert aux candidats titulaires des baccalauréats professionnels, des baccalauréats technologiques et des baccalauréats généraux.

Il est également ouvert sur décision du recteur prise après avis de l'équipe pédagogique de l'établissement de formation aux personnes remplissant les conditions fixées à l'article D. 337-144 du code de l'éducation.

Art. 5. – La durée minimale de la formation en milieu professionnel au titre de la préparation de la spécialité « cybersécurité » de mention complémentaire est de quatorze semaines. Les modalités, l'organisation et les objectifs de cette formation sont définis en annexe V.

Art. 6. – La spécialité « cybersécurité » de mention complémentaire est délivrée aux candidats ayant passé avec succès l'examen défini par le présent arrêté, selon les conditions de délivrance prévues aux articles D. 337-147 à D. 337-153 du code de l'éducation.

Art. 7. – La première session d'examen de la spécialité « cybersécurité » de mention complémentaire, organisée conformément aux dispositions du présent arrêté, aura lieu en 2024.

Art. 8. – Le directeur général de l'enseignement scolaire et les recteurs d'académie sont chargés, chacun en ce qui le concerne, de l'exécution du présent arrêté, qui sera publié au *Journal officiel* de la République française.

Fait le 6 février 2023.

Pour le ministre et par délégation :
La cheffe du service de l'instruction publique,
et de l'action pédagogique,
adjointe au directeur général,
R.-M. PRADEILLES-DUVAL

ANNEXES

MENTION COMPLÉMENTAIRE DE NIVEAU 4 « CYBERSÉCURITÉ »

Sommaire

ANNEXE I

PRÉSENTATION DU DIPLÔME

I-1. **Présentation**

La mention complémentaire « cybersécurité » est un diplôme de niveau 4 qui vise à donner une qualification spécialisée. La formation se caractérise par une forte alternance entre la formation en établissement et la formation en milieu professionnel.

Cette mention complémentaire vise à former des techniciennes et techniciens capables d'intervenir sur l'installation, l'exploitation et la maintenance des réseaux informatiques notamment dans un environnement industriel. Le technicien ou la technicienne participe à la sécurisation des données, des applications, des infrastructures numériques, des produits et des équipements. Il ou elle contribue à la gestion des incidents, à l'audit des installations et systèmes, ainsi qu'à la diffusion d'une culture d'hygiène informatique.

Véritable enjeu de souveraineté, ce diplôme s'inscrit dans un contexte de développement de la connectivité des produits avec des risques très élevés de cyberattaques.

I-2. **Tableau de synthèse**

Pôles d'activités	Blocs de compétences	Unités
MISE EN ŒUVRE DE RÉSEAUX INFORMATIQUES	**Bloc n° 1 – Mise en œuvre de réseaux informatiques** – Valider le fonctionnement d'un réseau – Coder – Installer une infrastructure réseau – Exploiter une installation réseau – Maintenir un réseau	**Unité U1** **Mise en œuvre de réseaux informatiques**
CYBERSÉCURITÉ	**Bloc n° 2 – Cybersécurité** – Communiquer en situation professionnelle (français/anglais) – Analyser une installation réseau – Organiser une intervention – Gérer un projet	**Unité U2** **Cybersécurité**

ANNEXE II

RÉFÉRENTIEL DES ACTIVITÉS PROFESSIONNELLES

II-1. **Insertion professionnelle visée**

II-1.1. *Secteurs d'activités*

Le ou la titulaire de la mention complémentaire « cybersécurité » intervient dans les secteurs suivants :

– informatique industrielle ;
– télécommunications ;
– centres de services ;
– activités de conseils ;
– santé…

Toutes les tailles de structures sont susceptibles d'accueillir le titulaire du diplôme : grandes entreprises, sociétés de conseils et de services informatique et numériques, PME et start-up.

II-1.2. *Types d'emploi accessibles*

Les métiers concernés par la gestion de la cybersécurité peuvent se retrouver dans les domaines suivants :

– la cybersécurité industrielle ;
– le domaine des objets connectés (véhicules, IoT, systèmes embarqués, etc.).

Les emplois pouvant être exercés par le ou la titulaire de la mention complémentaire « cybersécurité » sont dès le début de carrière :

– intégrateur ou intégratrice de solutions de sécurité ;
– opérateur ou opératrice en cybersécurité ;
– technicien ou technicienne de maintenance en informatique ;
– installateur ou installatrice de réseaux informatiques ;
– etc.

Avec une expérience (5 ans environ), les perspectives d'évolution possibles se situent vers les emplois suivants :

– évaluateur ou évaluatrice de la sécurité des technologies de l'information ;
– analyste en cybersécurité ;
– technicien ou technicienne d'exploitation informatique ;
– etc.

II-2. **Description des activités professionnelles**

II-2.1. *Présentation des pôles d'activités*

Pôles d'activités	Activités professionnelles
MISE EN ŒUVRE DE RÉSEAUX INFORMATIQUES	Activité A1 – Installation et qualification
	Activité A2 – Exploitation et maintien en condition opérationnelle
	Activité A3 – Gestion de projet et d'équipe
	Activité A4 – Accompagnement du client
	Activité A5 – Maintenance des réseaux informatiques
CYBERSÉCURITÉ	Activité A6 – Élaboration et appropriation d'un cahier des charges
	Activité A7 – Audit de l'installation ou du système
	Activité A8 – Gestion d'incidents

II-2.2. *Définition des activités professionnelles*

Chaque activité professionnelle est décrite de la manière suivante :

– un intitulé et un identifiant (R1, R2, etc.) permettant de repérer l'activité ;
– un ensemble de tâches élémentaires permettant de décrire les différentes étapes nécessaires à la réalisation de l'activité ;
– des conditions d'exercice qui décrivent le contexte en termes de moyens et ressources à disposition, autonomie attendue (éventuellement différent pour chaque tâche) et résultats attendus.

Les niveaux d'autonomie sont spécifiés sous forme d'une autonomie partielle (la tâche est réalisée sous la supervision d'un supérieur hiérarchique) ou complète (la tâche est réalisée en totale autonomie et le supérieur hiérarchique n'intervient que lors du contrôle des résultats attendus).

Pôle « MISE EN ŒUVRE DE RÉSEAUX INFORMATIQUES »	
Activité A1 – Installation et qualification	
Tâches associées T1 : Prise en compte de la demande du client T2 : Vérification du dossier d'exécution et interprétation des plans T3 : Préparation du chantier en fonction de l'intervention souhaitée T4 : Réalisation des opérations avec, en particulier, intégration des contraintes client et contrôle matériel et logiciel de l'installation T5 : Recettage de l'installation	
Conditions d'exercice	*Moyens et ressources* – Le cahier des clauses techniques particulières (CCTP) et le périmètre contractuel de la demande – Les modèles documentaires nécessaires et correspondant à l'existant – Le dossier d'exécution dans son ensemble dont l'architecture réseau – Les contacts clients et prestataires, la localisation du chantier, les contraintes (matérielles, humaines, géographiques, structurelles etc.) – La liste des matériels (types et versions logiciels), les paramétrages existants – Les équipements de sécurité, d'accès au chantier, et de contrôle – Le PV de livraison (recette)
	Autonomie : partielle

	Résultats attendus
	– Les tests de validation, les documents de mise en œuvre sont produits
	– Les achats nécessaires (matériels) et les ressources humaines sont identifiées, la relation client est maîtrisée
	– Les alertes sur manquements de pièces, l'interprétation des plans d'exécution face à la réalité du terrain sont effectuées
	– La validation des informations nécessaires et adaptées à l'intervention est effectuée sur :
	  – la constitution de l'équipe (compétences et disponibilités)
	– les matériels et logiciels (types, versions etc.)
	– les paramétrages existants (à réinjecter ou adapter)
	– les calendaires (selon la disponibilité du client)
	– les éléments climatiques
	  – les états structurels et géographiques
	– Les éléments de preuve d'avancement quotidien (photos etc.), les signalements et alertes sur évolution et problèmes in situ (risques réglementaires, structurels, climatiques, etc.) sont apportés
	– Le cahier de recette (PV de livraison) est rempli et validé par le client
	– L'envoi éventuel des justificatifs de pénalités de report est effectué

Pôle « MISE EN ŒUVRE DE RÉSEAUX INFORMATIQUES »	
Activité A2 – Exploitation et maintien en condition opérationnelle	
Tâches associées T1 : Suivi de l'exploitation technique T2 : Contact avec les supports techniques externes T3 : Supervision de l'état du réseau dans son périmètre T4 : Réalisation d'un diagnostic de premier niveau T5 : Configuration matérielle et logicielle des équipements T6 : Intégration de nouveaux équipements T7 : Mise à jour des équipements	
Conditions d'exercice	*Moyens et ressources* – La liste des équipements disponibles (modèles et versions logicielles), l'architecture des réseaux, les plans, les schémas – Les contacts techniques et support des supports techniques externes – Les outils de conception de diagrammes et de supervision de réseau – La procédure de fonctionnement nominal – Les procédures de retour à un fonctionnement nominal – La procédure d'alerte – La documentation utilisateur – La documentation des paramétrages spécifiques des équipements opérationnels – Les documents de validation pour la nouvelle configuration, la documentation des nouveaux équipements – Le paramétrage des équipements existants
	Autonomie : partielle
	Résultats attendus – L'installation fonctionne nominalement – Les comptes rendus des échanges avec les contacts (support) des opérateurs sont produits – Les alertes suite aux anomalies détectées sont remontées – Le défaut est identifié, corrigé, le PV d'anomalie est rédigé, la documentation relative à l'installation est éventuellement mise à jour – Les documents de configuration sont mis à jour (matériels et logiciels) – Le cahier de recette suite à l'intégration des nouveaux équipements est complété – Le cahier de recette suite à la mise à jour des équipements est complété

Pôle « MISE EN ŒUVRE DE RÉSEAUX INFORMATIQUES »	
Activité A3 – Gestion de projet et d'équipe	
Tâches associées T1 : Identification de toutes les étapes du projet jusqu'à la réception des travaux T2 : Identification des ressources humaines et matérielles T3 : Interactions avec les acteurs externes au projet	
Conditions d'exercice	*Moyens et ressources* – La liste des matériels disponibles ou non (à commander) nécessaires – Le planning de tous les intervenants : collaborateurs, équipes, sous-traitants, etc. – La liste des prestataires impliqués dans le projet, les contacts avec les entreprises prestataires
	Autonomie : partielle
	Résultats attendus – Le reporting régulier (quotidien/hebdomadaire) de l'avancement des travaux à la hiérarchie et au client est effectué – Le suivi d'avancement, points d'étape, alertes sont effectués – Les documents sont renseignés

Pôle « MISE EN ŒUVRE DE RÉSEAUX INFORMATIQUES »	
Activité A4 – Accompagnement du client	
Tâches associées T1 : Prise en compte des besoins du client T2 : Réception de l'installation avec le client T3 : Informations au client	
Conditions d'exercice	*Moyens et ressources* – La demande d'intervention du client – Les documents contractuels – Les équipements nécessaires à la validation – Les documents et logiciels de l'entreprise – Les modalités d'intervention normalisée – La documentation mise à disposition par l'entreprise
	Autonomie : partielle (sous le contrôle du manager)
	Résultats attendus – La demande du client est prise en compte ou transférée aux services compétents – Les performances de l'installation sont validées avec le client conformément à ses prescriptions. Les documents et les données contractuels de l'installation sont remis au client. Les opérations nécessaires à la levée de réserves éventuelles sont effectuées. – Le client est autonome dans la mise en œuvre de son installation – Les réponses aux questions du client et les conseils sont apportés – Les informations sont correctement transmises, de manière concise et précise aux intéressés

Pôle « MISE EN ŒUVRE DE RÉSEAUX INFORMATIQUES »	
Activité A5 – Maintenance des réseaux informatiques	
Tâches associées T1 : Suivi des interventions jusqu'à la fin de l'incident T2 : Réalisation de diagnostics et d'interventions de maintenance curative T3 : Réparation des liaisons, changement de cartes ou d'équipements T4 : Sauvegarde et restauration des configurations T5 : Rédaction de comptes rendus d'intervention	
Conditions d'exercice	*Moyens et ressources* – Les procédures de maintenance de l'entreprise – Les outils de reporting et le protocole propre à l'entreprise – Les outils de diagnostic, les outils nécessaires à l'intervention – Les dossiers techniques relatifs à l'intervention, les outils nécessaires à la réparation, les équipements de rechange – Les modèles de comptes rendus de l'entreprise
	Autonomie : partielle (restreinte à la complexité du réseau) sauf T5 en autonomie complète
	Résultats attendus – Les reportings sont effectués et archivés – La localisation de l'équipement en panne est réalisée. – L'identification de la cause de défaillance est effectuée. – La durée du diagnostic est optimale – Le réseau est opérationnel – Les documents sont complétés et conformes

Pôle « CYBERSÉCURITÉ »	
Activité 6 – Élaboration et appropriation d'un cahier des charges	
Tâches associées T1 : Collecte des informations T2 : Analyse des informations T3 : Interprétation du cahier des charges T4 : Formalisation du cahier des charges	
Conditions d'exercice	*Moyens et ressources* – Le dossier préliminaire du projet (expression du besoin, étude de marché etc.) – La documentation des équipements de l'entreprise (infrastructures matérielles et logicielles etc.) – Les moyens d'accès à Internet – Les outils logiciels (bureautique, modélisation, média, planification etc.) – Les contacts des intervenants sur le projet (internes, sous-traitants, clients, etc.)
	Autonomie : partielle
	Résultats attendus – Le cahier des charges préliminaire est complété ou rédigé – Les ressources permettant de réaliser le cahier des charges sont définies – Le planning prévisionnel est établi – Les tâches sont attribuées aux divers intervenants dans le planning prévisionnel

Pôle « CYBERSÉCURITÉ »	
Activité 7 – Audit de l'installation ou du système	
Tâches associées T1 : Évaluation des biens et moyens dans le périmètre de l'audit T2 : Évaluation de la configuration T3 : Évaluation du contrôle d'accès T4 : Évaluation de la gestion de compte T5 : Évaluation de la sécurité	
Conditions d'exercice	*Moyens et ressources* – Les outils logiciels d'évaluation (scan de vulnérabilité, de réseaux etc.) – La documentation des équipements à auditer (infrastructures matérielles, logicielles etc.) – Les infrastructures à auditer – Les utilisateurs et les exploitants – Les documents réglementaires, normatifs adoptés au sein de l'entreprise et du secteur de la sécurité des systèmes d'information – Le contrat de prestation de service – Les documentations et procédures d'audit (support de rapport d'audit, procédures techniques des outils d'audit)
	Autonomie : partielle
	Résultats attendus – L'ensemble des équipements matériels et logiciels du système d'information est identifié – Les outils logiciels sont mis en œuvre selon les spécifications et le cahier d'audit – Les vulnérabilités sont identifiées et hiérarchisées – Le rapport d'intervention est produit avec les résultats de l'audit – Des solutions sont proposées – Des recommandations de sécurité sont proposées

Pôle « CYBERSÉCURITÉ »	
Activité 8 – Gestion d'incidents	
Tâches associées T1 : Ouverture et catégorisation des tickets par niveau de criticité T2 : Traitement des tickets T3 : Remédiation des incidents T4 : Élaboration des rapports d'incidents T5 : Transmission de l'information (escalade)	
Conditions d'exercice	*Moyens et ressources* – Les outils logiciels (traçabilité de l'information, de tests, d'analyse et traitement de l'incident etc.) – Les documentations et procédures de traitement des incidents (support de rapport d'incidents etc.) – Les expertises et prestataires métiers (fournisseurs de services en nuage, d'équipements informatiques etc.) – L'outillage d'intervention sur les infrastructures matérielles – Les accès physiques nécessaires – Les contacts nécessaires (annuaire, liste de contacts) chez les clients et pour escalade – Les fiches réflexes de sensibilisation
	Autonomie : complète

	Résultats attendus – L'incident est résolu dans le périmètre de ses compétences – Le rapport d'incident est établi selon les procédures de traitement de l'incident – L'incident est correctement qualifié et transmis (escalade) – Le client est correctement informé et conseillé quant aux mesures de prévention possibles

ANNEXE III

RÉFÉRENTIEL DE COMPÉTENCES

III-1. **Définition des blocs de compétences**

III-1.1. *Liste des compétences*

C01	COMMUNIQUER EN SITUATION PROFESSIONNELLE (FRANÇAIS/ANGLAIS)
C02	ORGANISER UNE INTERVENTION
C03	ANALYSER UNE INSTALLATION RÉSEAU
C04	VALIDER LE FONCTIONNEMENT D'UN RÉSEAU
C05	CODER
C06	INSTALLER UNE INFRASTRUCTURE RÉSEAU
C07	EXPLOITER UNE INSTALLATION RÉSEAU
C08	MAINTENIR UN RÉSEAU
C09	GÉRER UN PROJET

III-1.2. *Blocs de compétences*

		C01	C02	C03	C04	C05	C06	C07	C08	C09
Pôle « MISE EN ŒUVRE DE RÉSEAUX INFORMATIQUES »	A1 : Installation et qualification				X	X	X	X		
	A2 : Exploitation et maintien en condition opérationnelle				X	X	X	X	X	
	A3 : Gestion de projet et d'équipe	X	X							X
	A4 : Accompagnement du client	X		X						
	A5 : Maintenance des réseaux informatiques			X	X	X		X	X	
Pôle « CYBERSÉCURITÉ »	A6 : Élaboration et appropriation d'un cahier des charges	X	X	X						X
	A7 : Audit de l'installation ou du système	X		X				X		X
	A8 : Gestion d'incidents			X	X	X		X		

Unités certificatives

U1				X	X	X	X	X	
U2	X	X	X						X

III-2. **Définition des compétences et connaissances associés**

Les compétences sont définies à l'aide des tableaux suivants qui rappellent les principales activités professionnelles mobilisant la compétence, et précisent ensuite les principales connaissances qui lui sont associées et les critères qui permettent de l'évaluer au travers des dimensions savoir, savoir-faire et savoir-être.

Chaque compétence mobilise des connaissances. Pour chaque connaissance, un niveau taxonomique est indiqué permettant de préciser les limites de connaissances attendues.

Les niveaux taxonomiques utilisent une échelle à quatre niveaux :

– niveau 1 : niveau d'information ;
– niveau 2 : niveau d'expression ;
– niveau 3 : niveau de maîtrise d'outils ;
– niveau 4 : niveau de maîtrise méthodologique (ce niveau n'est pas utilisé en mention complémentaire).

Les critères d'évaluation relevant de savoirs-être sont indiqués en *italique*.

C01	COMMUNIQUER EN SITUATION PROFESSIONNELLE
Principales activités mettant en œuvre la compétence : A3 – Gestion de projet et d'équipe A4 – Accompagnement du client A6 – Élaboration et appropriation d'un cahier des charges A7 – Audit de l'installation ou du système	
Connaissances associées (et niveaux taxonomiques)	
– Technologies de l'information et de la communication (Internet, suite bureautique, outils collaboratifs, etc.)	*Niveau 3*
– Techniques de communication écrite et orale (s'adapter à son interlocuteur dans la forme et le contenu, faire passer un message, les règles de rédaction, de communication verbale, etc.)	*Niveau 3*
– Anglais technique	*Niveau 2*
– Politique de sécurité et risques pour chaque niveau de criticité	*Niveau 2*
– Termes d'un contrat de prestation	*Niveau 2*
Critères d'évaluation de la compétence	
– La présentation écrite (typographie, orthographe, illustration, lisibilité) est pertinente et soignée – La présentation orale (support et expression) est de qualité et claire – Les informations sont collectées, formalisées et présentées sous la forme la plus adaptée – Le technicien tient compte des éventuelles situations de handicap des personnes avec lesquelles il interagit – Les outils et moyens de communication sont mis en œuvre dans le respect de la politique de sécurité et de prévention des risques (hygiène informatique) – Le rapport d'intervention est produit, des solutions et des recommandations sont proposées – *Le style, le ton et la terminologie utilisés sont adaptés à la personne et aux circonstances* – *Le maintien général, les comportements et le langage adoptés sont conformes aux règles de la profession, la réaction est adaptée au contexte*	

C02	ORGANISER UNE INTERVENTION
Principales activités mettant en œuvre la compétence : A3 – Gestion de projet et d'équipe A6 – Élaboration et appropriation d'un cahier des charges	
Connaissances associées (et niveaux taxonomiques)	
– Diagramme de Gantt	*Niveau 2*
– Langages de modélisation : UML/SysML	*Niveau 2*
– Contrat de prestation de service : contraintes en termes de sécurisation	*Niveau 2*
– Différents acteurs du projet : sous-traitants, clients, maître d'œuvre, maître d'ouvrage, utilisateurs, exploitants etc.	*Niveau 3*
– Infrastructures matérielles et logicielles centralisées, décentralisées ou réparties	*Niveau 3*
– Documents d'architecture métiers (synoptiques réseaux, matrice de flux, schéma de câblage, etc.)	*Niveau 3*
Critères d'évaluation de la compétence	
– Les différents interlocuteurs et ressources sont identifiés – Le cahier des charges préliminaire est complété et les ressources permettant de réaliser le cahier des charges sont décrites – Le planning prévisionnel est interprété – *Face à un ensemble de faits, des actions appropriées à poser sont décidées* – *De façon à poser des actions au moment opportun dans un contexte déterminé, la prise en charge est adaptée selon les responsabilités* – *Le travail est préparé de façon à satisfaire les exigences de qualité, d'efficacité et d'échéancier*	

C03	ANALYSER UNE INSTALLATION RÉSEAU
Principales activités mettant en œuvre la compétence : A4 – Accompagnement du client A5 – Maintenance des réseaux informatique A6 – Élaboration et appropriation d'un cahier des charges A7 – Audit de l'installation ou du système A8 – Gestion d'incidents	
Connaissances associées (et niveaux taxonomiques)	
– Infrastructures matérielles et logicielles centralisées, décentralisées ou réparties	*Niveau 3*
– Outils de description d'architecture métiers (synoptiques réseaux, matrice de flux, schéma de câblage, etc.)	*Niveau 3*

C03	ANALYSER UNE INSTALLATION RÉSEAU	
– Langages de modélisation (UML, SysML, MLD/MCD)		*Niveau 2*
– Acteurs d'un projet : sous-traitants, clients, maître d'œuvre, maître d'ouvrage, utilisateurs, exploitants, etc.		*Niveau 2*
– Acteurs de l'écosystème réglementaire, normatif et de référence des bonnes pratiques : CNIL, ANSSI / NIS, Cybermalveillance.gouv.fr		*Niveau 2*
– Métriques des équipements réseaux		*Niveau 3*
– Outils et techniques de recherche et d'analyse de documentation y compris en anglais		*Niveau 3*
Critères d'évaluation de la compétence		
– Les spécifications du cahier des charges sont extraites – L'organisation structurelle des sous-ensembles est conforme aux exigences fonctionnelles – La structure de la solution technique est critiquée – Les algorithmes sont critiqués – *Le travail est préparé de façon à satisfaire les exigences de qualité, d'efficacité et d'échéancier* – *Le calme est conservé de façon constante dans des situations particulières, tout en persévérant dans la tâche jusqu'à l'atteinte du résultat sans se décourager* – *Face à un ensemble de faits, des actions appropriées à poser sont décidées*		

C04	VALIDER LE FONCTIONNEMENT D'UN RÉSEAU	
Principales activités mettant en œuvre la compétence : A1 – Installation et qualification A2 – Exploitation et maintien en condition opérationnelle A5 – Maintenance des réseaux informatiques A8 – Gestion d'incidents		
Connaissances associées (et niveaux taxonomiques)		
– Réseaux informatiques (protocoles, équipements et outils usuels et industriels)		*Niveau 3*
– Sécurisation des réseaux (ACL, mots de passe, pare-feu etc.)		*Niveau 3*
– Modèle OSI en couches		*Niveau 2*
– Fiches de recette (scénario d'utilisation du logiciel, résultats attendus)		*Niveau 3*
– Usages et documents réglementaires, normatifs adoptés au sein de l'entreprise et du secteur de la sécurité des systèmes d'information : CNIL/RGPD/ISO.../ réglementation sectorielle		*Niveau 2*
– Outils logiciels d'évaluation, de traçabilité de l'information, de tests, d'analyse de traitement et de rapport de l'incident		*Niveau 3*
Critères d'évaluation de la compétence		
– Les exigences à valider sont identifiées dans le périmètre défini – Les procédures de test sont établies – Les résultats de tests sont synthétisés pour évaluer la conformité globale – Le document de recette est validé par le client et la recette est réalisée avec le client – *Le travail est préparé de façon à satisfaire les exigences de qualité, d'efficacité et d'échéancier* – *Le calme est conservé de façon constante dans des situations particulières, tout en persévérant dans la tâche jusqu'à l'atteinte du résultat sans se décourager* – *Face à un ensemble de faits, des actions appropriées à poser sont décidées*		

C05	CODER	
Principales activités mettant en œuvre la compétence : A1 – Installation et qualification A2 – Exploitation et maintien en condition opérationnelle A5 – Maintenance des réseaux informatiques A8 – Gestion d'incidents		
Connaissances associées (et niveaux taxonomiques)		
– Langages de Scripts (UNIX (bash/zsh), Powershell)		*Niveau 3*
– Principes fondamentaux de programmation (variables, alternatives, boucles et fonctions)		*Niveau 3*
– Interface de ligne de commande des systèmes d'exploitation		*Niveau 3*

C05	CODER
Critères d'évaluation de la compétence	
– Les environnements logiciels et matériels sont choisis et justifiés – Le code est commenté – La solution logicielle est intégrée et testée conformément aux spécifications du cahier des charges, des bonnes pratiques et des différentes politiques de sécurité et de protection des données personnelles – *La résolution d'un problème nouveau imprévu est réussie en utilisant ses propres moyens conformément aux règles de la fonction* – *Le travail est effectué selon les attentes exprimées de temps, de quantité ou de qualité* – *Le travail est préparé de façon à satisfaire les exigences de qualité, d'efficacité et d'échéancier*	

C06	INSTALLER UNE INFRASTRUCTURE RÉSEAU	
Principales activités mettant en œuvre la compétence : A1 – Installation et qualification A2 – Exploitation et maintien en condition opérationnelle		
Connaissances associées (et niveaux taxonomiques)		
– Modèle OSI en couches		*Niveau 2*
– Protocoles usuels IPv4, HTTP, HTTPS, TCP/IP, Ethernet		*Niveau 3*
– Protocoles (IPv6, SSH, DNS, SMTP, POP, IMAP, SIP, RTP, DHCP, SNMP, MQTT, NTP etc.)		*Niveau 2*
– Routage (NAT, PAT)		*Niveau 3*
– Commutation (VLAN incl.)		*Niveau 3*
– Pare Feu, ACL		*Niveau 3*
– Réseaux de terrain (Modbus overIP etc.)		*Niveau 3*
– Réseaux IoT (LPWAN, 802.15.4, Bluetooth)		*Niveau 3*
– WLAN		*Niveau 3*
– Systèmes d'exploitation (Windows, UNIX, virtualisations)		*Niveau 3*
– Architecture réseaux cellulaires		*Niveau 2*
– VPN		*Niveau 3*
Critères d'évaluation de la compétence		
– Les équipements nécessaires à la réponse au CDC (fourni par le client) sont identifiés – Une procédure de configuration ou d'installation est déterminée ainsi que les points critiques ; ces procédures sont soumises à validation si nécessaire – La ou les procédures choisie(s) est (sont) suivie(s) – Un compte-rendu du fonctionnement de l'installation est fourni (anomalies, difficultés et retours client(s) etc.) – *Le style, le ton et la terminologie utilisés sont adaptés à la personne et aux circonstances* – *Le travail est effectué selon les attentes exprimées de temps, de quantité ou de qualité* – *Le travail est préparé de façon à satisfaire les exigences de qualité, d'efficacité et d'échéancier*		

C07	EXPLOITER UNE INSTALLATION RÉSEAU	
Principales activités mettant en œuvre la compétence : A1– Installation et qualification A2– Exploitation et maintien en condition opérationnelle A5 – Maintenance des réseaux informatiques A7 – Audit de l'installation ou du système A8 – Gestion d'incidents		
Connaissances associées (et niveaux taxonomiques)		
– Interface ligne de commande d'équipements et OS		*Niveau 3*
– Connexion et prise en main à distance (protocoles et législation associée)		*Niveau 2*
– Logiciels de supervision (DashBoard Nagios, Centreon) et protocoles associés (SNMP (MIBs)		*Niveau 3*
– Outils logiciels d'évaluation, de traçabilité de l'information, de tests, d'analyse de traitement et de rapport de l'incident		*Niveau 3*
– Politique et outils de sauvegarde		*Niveau 3*

C07	EXPLOITER UNE INSTALLATION RÉSEAU
– Outils de mise à jour système et sécurité système (gestion des paquets logiciels, mise à jour de sécurité, script mise à jour automatique, etc.)	*Niveau 3*
– Infrastructures matérielles, logicielles : centralisées, décentralisées ou réparties, microservices : cloud, local, hybride, symboles de représentation	*Niveau 3*
– Usages et documents réglementaires, normatifs adoptés au sein de l'entreprise et du secteur de la sécurité des systèmes d'information : CNIL/RGPD/ISO etc./ réglementation sectorielle	*Niveau 2*
Critères d'évaluation de la compétence	
– Les différents éléments matériels et/ou logiciels sont identifiés à partir d'un schéma fourni – Le fonctionnement d'un équipement matériel et/ou logiciel est vérifié en tenant compte du contexte opérationnel – La mise à jour d'un matériel et/ou logiciel est proposée et justifiée – Les optimisations ou résolution d'incidents nécessaires sont effectuées – *La résolution d'un problème nouveau imprévu est réussie en utilisant ses propres moyens conformément aux règles de la fonction* – *Face à un ensemble de faits, des actions appropriées à poser sont décidées* – *Le travail est préparé de façon à satisfaire les exigences de qualité, d'efficacité et d'échéancier*	

C08	MAINTENIR UN RÉSEAU
Principales activités mettant en œuvre la compétence : A2 – Exploitation et maintien en condition opérationnelle A5 – Maintenance des réseaux informatiques	
Connaissances associées (et niveaux taxonomiques)	
– Outils logiciels d'évaluation, de traçabilité de l'information, de tests, d'analyse de traitement	*Niveau 3*
– Outillage nécessaire au diagnostic, à la réparation et les équipements de rechange	*Niveau 3*
– Infrastructures matérielles, logicielles : centralisées, décentralisées ou réparties, microservices : cloud, local, hybride, symboles de représentation	*Niveau 3*
– Documents d'exploitation et de pilotage (procédures internes, contacts et niveau de criticité)	*Niveau 2*
– Les droits d'accès et contacts nécessaires	*Niveau 2*
Critères d'évaluation de la compétence	
– Les outils logiciels et matériels permettant d'effectuer les tests et l'analyse du système d'information sont identifiés et mis en œuvre selon les spécifications – Les résultats de tests et d'analyse sont interprétés de manière pertinente et les causes de l'incident sont localisées – Le service est opérationnel – Le client est correctement informé et conseillé quant aux mesures de prévention possibles – *Le style, le ton et la terminologie utilisés sont adaptés à la personne et aux circonstances* – *Le déroulement des tâches de travail est observé avec attention et de façon soutenue de façon à en contrôler le résultat attendu* – *Face à un ensemble de faits, des actions appropriées à poser sont décidées*	

C09	GÉRER UN PROJET
Principales activités mettant en œuvre la compétence : A3 – Gestion de projet et d'équipe A6 – Élaboration et appropriation d'un cahier des charges A7 – Audit de l'installation ou du système	
Connaissances associées (et niveaux taxonomiques)	
– Conduite de projet (Cycle en V, méthodes Agile (Scrum, Kanban))	*Niveau 2*
– Langages de modélisation : UML, SysML, MCD	*Niveau 2*
– Techniques de conduite de réunion de projet	*Niveau 2*
– Outils de gestion de projet	*Niveau 3*
– Notions de complexités techniques et de criticités	*Niveau 3*
– Moyens, outils et méthodes de veille technologique	*Niveau 2*
– Cartographie des acteurs du projet : sous-traitants, clients, maître d'œuvre, maître d'ouvrage, utilisateurs, exploitants etc.	*Niveau 2*

C09	GÉRER UN PROJET
Critères d'évaluation de la compétence	
– Les tâches sont réparties en tenant compte des compétences, les documents sont renseignés, un planning prévisionnel est proposé – Le cas échéant, les besoins spécifiques des personnes en situation de handicap sont pris en compte – L'adéquation des ressources humaines et des ressources matérielles pour mener le projet est validée – L'équipe projet communique correctement et gère les retards et les aléas – Les travaux sont réalisés et livrés avec la documentation en concordance avec les besoins du client – *Le travail est préparé de façon à satisfaire les exigences de qualité, d'efficacité et d'échéancier* – *La résolution d'un problème nouveau imprévu est réussie en utilisant ses propres moyens conformément aux règles de la fonction* – *Le travail en équipe est conduit de manière solidaire en contribuant par des idées et des efforts*	

ANNEXE IV

RÉFÉRENTIEL D'ÉVALUATION

IV-1. **Unités constitutives**

Unité U1 – Mise en œuvre de réseaux informatiques

Le contenu sur lequel repose l'unité U1 correspond aux compétences du bloc n° 1 « Mise en œuvre de réseaux informatiques » défini dans l'annexe III « référentiel de compétences ».

Unité U2 – Cybersécurité

Le contenu sur lequel repose l'unité U2 correspond aux compétences du bloc n° 2 « Cybersécurité » défini dans l'annexe III « référentiel de compétences ».

IV-2. **Règlement d'examen**

Mention complémentaire de niveau 4 « Cybersécurité »			**Candidats**		
			Scolaires (établissement public ou privé sous contrat) **Apprentis** (CFA habilité ou en CFA porté par un EPLE, GRETA ou GIP-FCIP assurant toute la formation théorique) **Formation professionnelle continue** dans un établissement public	**Scolaires** (établissement privé hors contrat) **Apprentis** (CFA ou section d'apprentissage non habilité) **Formation professionnelle continue** en établissement privé **Candidats justifiant de 3 années d'activité professionnelle**. **Enseignement à distance**	
ÉPREUVES	Unité	Coef.	Mode	Mode	Durée
E1 – Mise en œuvre de réseaux informatiques	U1	2	CCF	Ponctuel pratique	4h
E2 – Cybersécurité	U2	3	CCF	Ponctuel pratique	4h

IV-3. **Définition des épreuves**

Epreuve E1 – Mise en œuvre de réseaux informatiques

Unité U1

Coefficient 2

Objectif de l'épreuve

L'épreuve a pour objectif l'évaluation des compétences associées au pôle « Mise en œuvre de réseaux informatiques » :

L'objectif de l'épreuve est d'évaluer les compétences suivantes :

– C04 : valider le fonctionnement d'un réseau ;
– C05 : coder ;
– C06 : installer une infrastructure réseau ;
– C07 : exploiter une installation réseau ;
– C08 : maintenir un réseau.

Les critères d'évaluation sont ceux définis dans le référentiel de compétences. L'évaluation des candidats sur ces critères s'appuie sur toutes les dimensions (savoirs, savoir-faire, savoir-être) de la compétence.

D'autres compétences peuvent être mobilisées mais ne sont pas évaluées dans le cadre de cette épreuve.

Contenu de l'épreuve

Les compétences sont évaluées dans un contexte professionnel conforme aux activités et tâches du pôle « Mise en œuvre de réseaux informatiques » décrites dans le référentiel des activités professionnelles.

Les moyens et ressources associés aux activités professionnelles seront mis à disposition des candidats.

Modalités d'évaluation

Contrôle en cours de formation :

L'évaluation s'appuie sur plusieurs activités permettant d'établir un suivi et un bilan des compétences visées par l'épreuve. Les activités sont menées en centre de formation et/ou en entreprise.

Le suivi de l'acquisition des compétences, les bilans intermédiaires et le bilan final sont établis :

– par l'équipe pédagogique du domaine professionnel dans le cas où l'activité est menée en centre de formation ;
– par l'équipe pédagogique du domaine professionnel, le tuteur ou maître d'apprentissage et le candidat dans le cas où l'activité est menée conjointement avec une entreprise.

Le suivi d'acquisition des compétences requiert l'utilisation d'un livret de suivi individualisé exploité par les enseignants assurant l'encadrement des candidats au cours de la formation. La fréquence des bilans intermédiaires est à l'initiative de l'équipe pédagogique.

Au cours du dernier trimestre de la formation, une commission d'évaluation composée par l'équipe pédagogique du domaine professionnel est réunie sous l'autorité du chef d'établissement. La commission d'évaluation arrête le positionnement de chaque candidat à son niveau de maîtrise des compétences sur la grille nationale d'évaluation de l'épreuve publiée dans la circulaire nationale d'organisation de l'examen.

A l'issue du positionnement, l'équipe pédagogique de l'établissement de formation constitue, pour chaque candidat, un dossier comprenant :

– le livret de suivi des compétences et les bilans intermédiaires ;
– la grille nationale d'évaluation renseignée ayant conduit à la proposition de note.

Forme ponctuelle :

L'épreuve prend la forme d'une épreuve ponctuelle pratique d'une durée de 4h. Elle se déroule sur un plateau technique adapté au contexte professionnel associé à l'épreuve et défini dans le référentiel des activités professionnelles.

L'organisation de l'épreuve est définie dans la circulaire nationale d'organisation d'examen.

Les candidats sont positionnés à leur niveau de maîtrise des compétences sur la grille nationale d'évaluation de l'épreuve publiée dans la circulaire nationale d'organisation de l'examen.

Epreuve E2 – Cybersécurité

Unité U2

Coefficient 3

Objectif de l'épreuve

L'épreuve a pour objectif l'évaluation des compétences associées au pôle « Cybersécurité » :

– C01 : communiquer en situation professionnelle (français/anglais) ;
– C02 : organiser une intervention ;
– C03 : analyser une installation réseau ;
– C09 : gérer un projet.

Les critères d'évaluation sont ceux définis dans le référentiel de compétences. L'évaluation des candidats sur ces critères s'appuie sur toutes les dimensions (savoirs, savoir-faire, savoir-être) de la compétence.

D'autres compétences peuvent être mobilisées mais ne sont pas évaluées dans le cadre de cette épreuve.

Contenu de l'épreuve

Les compétences sont évaluées dans un contexte professionnel conforme aux activités et tâches du pôle « Cybersécurité » décrites dans le référentiel des activités professionnelles.

Les moyens et ressources associés aux activités professionnelles seront mises à disposition des candidats.

Modalités d'évaluation

Contrôle en cours de formation :

L'évaluation s'appuie sur plusieurs activités permettant d'établir un suivi et un bilan des compétences visées par l'épreuve. Les activités sont menées en centre de formation et/ou en entreprise.

Le suivi de l'acquisition des compétences, les bilans intermédiaires et le bilan final sont établis :

– par l'équipe pédagogique du domaine professionnel dans le cas où l'activité est menée en centre de formation ;

– par l'équipe pédagogique du domaine professionnel, le tuteur ou maître d'apprentissage et le candidat dans le cas où l'activité est menée conjointement avec une entreprise.

Le suivi des compétences requiert l'utilisation d'un livret de suivi individualisé exploité par les enseignants assurant l'encadrement des candidats au cours de la formation. La fréquence des bilans intermédiaires est à l'initiative de l'équipe pédagogique.

Au cours du dernier trimestre de la formation, une commission d'évaluation composée par l'équipe pédagogique est réunie sous l'autorité du chef d'établissement. La commission d'évaluation arrête le positionnement de chaque candidat à son niveau de maîtrise des compétences sur la grille nationale d'évaluation de l'épreuve publiée dans la circulaire nationale d'organisation de l'examen.

A l'issue du positionnement, l'équipe pédagogique de l'établissement de formation constitue, pour chaque candidat, un dossier comprenant :

– le livret de suivi des compétences et les bilans intermédiaires ;
– la grille nationale d'évaluation renseignée ayant conduit à la proposition de note.

Forme ponctuelle :

L'épreuve prend la forme d'une épreuve ponctuelle pratique d'une durée de 4h. Elle se déroule sur un plateau technique adapté au contexte professionnel associé à l'épreuve et défini dans le référentiel des activités professionnelles.

L'organisation de l'épreuve est définie dans la circulaire nationale d'organisation d'examen.

Les candidats sont positionnés à leur niveau de maîtrise des compétences sur la grille nationale d'évaluation de l'épreuve publiée dans la circulaire nationale d'organisation de l'examen.

ANNEXE V

PÉRIODE DE FORMATION EN MILIEU PROFESSIONNEL

V-1. **Présentation générale des périodes de formation en milieu professionnel**

Garantes de la qualité du diplôme et de sa cohérence avec les opportunités, évolutions et contraintes des métiers relevant de la cybersécurité, les périodes de formation en milieu professionnel constituent un gage d'insertion professionnelle et participent à la formation des candidats à la mention complémentaire « cybersécurité ».

Le cursus de formation de la mention complémentaire « cybersécurité » respecte le principe de l'alternance, sous tutorat pédagogique. La formation se déroule en centre de formation et au sein de l'organisation support des périodes de formation en milieu professionnel. La mise en œuvre d'une pédagogie de l'alternance réclame une liaison très étroite entre l'organisme de formation et ses formateurs, la structure d'alternance, la personne tutrice et l'élève stagiaire. Dans ce contexte, la structure d'alternance est, comme le centre de formation, l'un des lieux ressources de la construction de la compétence du stagiaire.

Ainsi, l'apprenant construit des compétences à partir des expériences acquises en centre de formation et en entreprise. La construction de ces compétences s'exprime par nature en situation et en action. Elles n'apparaissent donc jamais comme une simple application d'éléments de théorie ou de savoir-faire, acquis en centre de formation mais comme une adaptation à un contexte d'action précis. Les acquisitions effectives en centre de formation ou en entreprise sont de natures différentes mais ne peuvent se résumer à une application théorie/pratique, car on acquiert dans les deux lieux des éléments de théorie et des éléments de pratique. En conséquence, le rôle de l'alternance est de permettre l'adaptation des différents savoirs à la réalité concrète de leur mise en application. Organiser une formation en alternance permet de passer d'une logique d'enseignement à une logique de construction de connaissances et d'acquisition de compétences.

La qualité des périodes de formation en milieu professionnel repose sur un engagement de tous les partenaires de l'alternance dans le respect des principes pédagogiques suivants :

– l'implication du stagiaire dans le projet de la structure où son engagement est un élément moteur de la construction des compétences ;
– la mise en responsabilité progressive du stagiaire ;
– l'autonomie du stagiaire dans la maîtrise des compétences attendues par le référentiel comme un objectif à atteindre à l'issue de la période de formation en milieu professionnel ;
– l'expérimentation pédagogique essentielle comme une possibilité offerte d'explorer des champs nouveaux, utiles à l'élève stagiaire comme à la structure ;
– l'indispensable relation entre l'organisme de formation et la structure d'accueil permettant :
  – la cohérence entre la formation en centre et en structure : au-delà des outils de liaison, il est de la responsabilité de la personne tutrice de veiller à cette cohérence en sollicitant quand c'est nécessaire l'organisme de formation ;
  – la mise en adéquation des contraintes du centre de formation avec celles de l'organisation d'accueil.

V-2. **Modalités d'organisation des périodes de formation en milieu professionnel**

Les périodes de formation en milieu professionnel peuvent se dérouler dans plusieurs entreprises définies par le référentiel des activités professionnelles. La personne référente dans l'organisation d'accueil contribue à la formation du stagiaire en étroite collaboration avec l'équipe pédagogique de l'établissement de formation, qui veille à assurer la complémentarité des savoirs et des savoir-faire entre l'établissement de formation et la structure d'accueil.

Chaque période de PFMP donne lieu, à l'occasion d'une visite dans l'organisation d'accueil, à l'élaboration d'un bilan individuel établi conjointement par la personne tutrice et les membres de l'équipe pédagogique. Ce bilan indique la nature des activités réalisées en lien avec les compétences visées et négociées entre l'établissement de formation et l'organisation d'accueil. Il précise également la maîtrise atteinte des compétences visées

V-2.1. *Pour la voie scolaire*

Les périodes de formation en milieu professionnel sont obligatoires pour les candidats scolaires relevant d'une préparation en présentiel ou à distance.

Elles sont organisées avec le concours des milieux professionnels et l'équipe pédagogique participe à l'organisation et au suivi des périodes de formation en milieu professionnel conformément à la circulaire n° 2016-053 du 29 mars 2016 relative à l'encadrement des périodes en entreprise (*BO*EN du 31 mars 2016).

Il est préconisé que la durée des PFMP soit comprise entre quatorze et dix-huit semaines, quatorze semaines étant la durée minimale.

Le rythme de l'alternance et le choix des dates des périodes de PFMP relève de l'autonomie des établissements qui prendront en considération les contraintes du ou des milieux professionnels d'accueil des élèves.

La formation dispensée en milieu professionnel se déroule sous la responsabilité du chef ou de la cheffe d'établissement sur la base d'une convention, établie entre l'établissement d'enseignement et la structure d'accueil.

Dans le cas d'un prolongement sur la période de vacances scolaires, la convention avec la structure d'accueil en précise les modalités notamment celles relatives au suivi. Si la PFMP se déroule à l'étranger, la convention pourra être adaptée pour tenir compte des contraintes imposées par la législation du pays d'accueil.

L'annexe pédagogique de la convention est établie conjointement par l'équipe pédagogique et la ou les personnes tutrices : modes de relations à établir, types d'activités, objectifs et contenus de formation.

Pendant la PFMP, l'élève a obligatoirement la qualité de stagiaire et non de salarié. La présence continue de l'élève stagiaire dans l'organisation d'accueil est requise pendant toute la durée de la PFMP. En fin de PFMP, une attestation de PFMP lui est remise par la personne responsable de structure d'accueil. Elle permet de vérifier la conformité réglementaire de la formation en milieu professionnel en précisant au minimum les dates et la durée de la PFMP.

Pour chaque PFMP, la personne tutrice de la structure d'accueil, accompagne le stagiaire pour appréhender, mettre en œuvre et analyser les situations de travail rencontrées.

Afin d'en garantir son caractère formateur, la PFMP est placée sous la responsabilité de l'équipe pédagogique. Celle-ci définit les objectifs de la PFMP et sa mise en place, assure son suivi et l'exploitation qui en est faite et explicite aux responsables des organisations d'accueil les objectifs, et plus particulièrement les compétences, que la PFMP vise à développer.

Aux termes de la circulaire n° 2016-053 du 29 mars 2016 relative à l'encadrement des périodes en entreprise (*BO*EN du 31 mars 2016), la recherche et le choix des entreprises d'accueil relèvent de la responsabilité de l'équipe pédagogique de l'établissement de formation.

V-2.2. *Pour la voie de l'apprentissage*

La formation en milieu professionnel se déroule conformément aux dispositions du code du travail, dans le cadre de l'alternance propre au contrat d'apprentissage. Les dispositions du code du travail complètent les dispositions de l'article D. 3337-145 du code de l'éducation.

Elle s'articule avec la formation dispensée dans un centre de formation d'apprentis pour permettre l'acquisition des compétences définies dans le diplôme. Chaque visite dans l'entreprise donne lieu à l'élaboration d'un bilan individuel établi conjointement par le maître d'apprentissage et un ou des membres de l'équipe pédagogique. Ce bilan indique la nature des activités réalisées en lien avec les compétences visées et négociées entre le centre de formation et l'entreprise.

Afin d'assurer une cohérence dans la formation, l'équipe pédagogique du centre de formation d'apprentis doit veiller à informer les maîtres d'apprentissage des objectifs des différentes périodes au moyen d'un document de liaison, et plus particulièrement de leur importance dans les épreuves certificatives du diplôme.

La formation fait l'objet d'un contrat conclu entre l'apprenti et son employeur conformément aux dispositions en vigueur dans le code du travail. Si les diverses activités de la formation ne peuvent être réalisées dans l'entreprise, l'article R. 6223 -10 du code du travail doit être mis en œuvre (cf. accueil de l'apprenti dans d'autres entreprises que celle qui l'emploie).

Pour les apprentis, les attestations de formation en milieu professionnel sont remplacées par un certificat de travail de l'employeur confirmant le statut du candidat comme apprenti dans son entreprise ou organisme.

V-2.3. *Pour la voie de la formation continue*

Candidat en situation de première formation pour ce diplôme ou en reconversion

Il est préconisé que la durée des PFMP soit comprise entre quatorze et dix-huit semaines, quatorze semaines étant la durée minimale.

Elle s'ajoute aux durées de formation dispensées dans le cadre de la formation professionnelle continue par chaque organisme de formation.

Le stagiaire peut effectuer sa préparation dans le cadre d'un contrat de travail de type particulier tel qu'un contrat de professionnalisation. Dans ce cas, la durée de formation en milieu professionnel est incluse dans la période de formation dispensée en milieu professionnel où s'effectue le contrat si les activités exercées sont en cohérence avec les exigences du référentiel et conformes aux objectifs.

A l'issue de chaque période de formation en milieu professionnel, une attestation de présence doit être renseignée par l'organisme de formation et signée par son responsable. Elle précise la période, la structure d'accueil et le nombre de semaines effectuées.

Candidat en situation de perfectionnement

Le candidat doit avoir exercé des activités relevant du secteur professionnel de la mention complémentaire, en tant que salarié à temps plein, pendant six mois au moins au cours de l'année précédant l'examen

ou les a exercées à temps partiel pendant un an au cours des deux années précédant l'examen.

V-2.4. *Positionnement*

Pour les candidats positionnés par décision du recteur la durée minimale de la période en milieu professionnel est de :

– huit semaines pour les candidats de la voie scolaire (article D. 337-146 du code de l'éducation) ;
– six semaines pour les candidats issus de la voie de la formation professionnelle continue.

V-2.5. *Pour les candidats se présentant au titre de leur expérience professionnelle*

Le candidat n'effectue pas de stage, mais doit justifier de trois années d'expérience professionnelle dans un emploi qualifié correspondant à la finalité de la mention complémentaire à l'examen de laquelle il s'inscrit.

Le candidat produit ses certificats de travail pour l'inscription à l'examen.