LES MARCHÉS PUBLICS DE CYBERSÉCURITÉ

Assurez la conformité de vos marchés et sécurisez vos achats

1 JOUR, 7 HEURES

MARCHÉS ET PROCÉDURES SPÉCIFIQUES

CODE : APA47

Objectifs de la formation

Cerner les principales exigences réglementaires et techniques d'un marché public de cybersécurité

Intégrer les clauses spécifiques liées à la cybersécurité dans le cahier des charges de son marché

Appréhender les procédures de passation adaptée aux marchés publics de cybersécurité

Appréhender les modalités de l'exécution et de suivi du marché

Parmi nos formateurs

- **REMEUR Patrice**
  Expert cybersécurité : Directeur de l'Innovation & DPO,

Public concernés

- Acheteurs publics ; Agents en charge des achats pour la fonction publique d'Etat, la fonction publique hospitalière et les collectivités territoriales ; Directeurs du service marchés ; Responsables des cellules marchés ; Directeurs juridiques
- Toute personne souhaite acheter une solution ou service cybersécurité

Prérequis

- Aucun prérequis

Tarifs

- Tarif Session en classe virtuelle : 995,00 €HT
- Tarif Session en présentiel : 1 060,00 €HT

Les marchés publics de cybersécurité se distinguent par leur complexité et leur importance stratégique. Les acheteurs publics doivent prendre en compte les exigences techniques, respecter des normes et réglementations strictes et anticiper des menaces numériques, tout en garantissant la fiabilité et l'évolutivité des solutions adoptées.

Cette formation a été conçue pour vous guider dans la gestion des marchés publics de cybersécurité, depuis la définition des besoins jusqu'au suivi des prestations. Vous apprendrez à rédiger un cahier des charges adapté, à choisir des solutions efficaces et conformes, et à intégrer les enjeux de sécurité, de souveraineté et d'évolutivité.

A l'issue de cette formation, vous serez capable de piloter un marché public de cybersécurité avec confiance, en tenant compte des défis stratégiques, techniques et financiers pour garantir des résultats solides et durables.

Intégrer les spécificités d'un marché public de cybersécurité

- Appréhender les typologies des solutions cybersécurité
- Recueillir les besoins des différentes parties prenantes
- Quelles sont les attentes en termes de performance, de coûts, de niveaux de service et d'évolutivité
- Focus sur le rôle de l'acheteur public pour garantir une solution cyber conformes aux exigences techniques et réglementaires

---

ILLUSTRATION **Présentation des solutions cybersécurité existantes sur le marché**

S'approprier la méthodologie pour rédiger un cahier des charges cybersécurité

- Définir les exigences fonctionnelles et techniques
- Identifier des objectifs de sécurité : confidentialité, intégrité, disponibilité
- Quelles sont les clauses types de cybersécurité
- Appréhender les critères d'évaluation
- Prendre en compte la notion de souveraineté dans son marché
- Faire le point sur les pénalités de non-conformité en cas de défaillance du prestataire
- Garantir la mise à jour continue et l'adaptabilité des solutions proposées face aux nouvelles menaces

---

TRAVAIL DE GROUPE **Analyse d'un cahier des charges d'un marché de cybersécurité présenté par le formateur**

ATELIER **Avec l'appui du formateur, les stagiaires sont amenés à rédiger des clauses types de cybersécurité**

Appréhender les procédures et les modalités de passation de son marché

- Choisir la procédure de passation la plus adaptée à son marché
- Comment contrôler les certifications du prestataire
- Prendre en compte les coûts sur la durée du contrat : coûts directs, coûts indirects, coûts cachés
- Mettre en place une grille analyse des candidats : focus sur la sécurité des solutions proposées et leur conformité aux normes et réglementations

---

ATELIER **Analyse d'un marché de cybersécurité, avec présentation des différentes offres soumises et discussion des critères d'évaluation**

Appréhender les modalités de l'exécution et de suivi du marché

- Mettre en place un plan de suivi et de contrôle des prestations
- Gérer les incidents de sécurité et procédures de notification
- Assurer l'évaluation continue de la conformité du prestataire aux exigences de sécurité
- Gestion des évolutions et des mises à jour de sécurité

ATELIER Élaboration d'un plan de suivi de marché en cybersécurité en définissant des indicateurs clés de performance (KPI) et des mécanismes de contrôle adaptés

Evaluation des acquis de la formation

Dates

Classe virtuelle	Paris
04/12/2026	04/12/2026
11/06/2027	
14/09/2027	
17/12/2027	

Modalités pédagogiques, d'évaluation et techniques

- **Modalités pédagogiques:**

Pour les formations synchrones-présentiel ou classes virtuelles (formations à distance, en direct), les stages sont limités, dans la mesure du possible, à une douzaine de participants, et cherchent à respecter un équilibre entre théorie et pratique. Chaque fois que cela est possible et pertinent, des études de cas, des mises en pratique ou en situation, des exercices sont proposées aux stagiaires, permettant ainsi de valider les acquis au cours de la formation. Les stagiaires peuvent interagir avec le formateur ou les autres participants tout au long de la formation, y compris sur les classes virtuelles durant lesquelles le formateur, comme en présentiel peut distribuer des documents tout au long de la formation via la plateforme. Un questionnaire préalable dit 'questionnaire pédagogique' est envoyé aux participants pour recueillir leurs besoins et attentes spécifiques. Il est transmis aux intervenant(e)s avant la formation, leur permettant de s'adapter aux publics. Pour les formations en E-learning (formations à distance, asynchrones), le stagiaire peut suivre la formation à son rythme, quand il le souhaite. L'expérience alterne des vidéos de contenu et des activités pédagogiques de type quizz permettant de tester et de valider ses acquis tout au long du parcours. Des fiches mémos reprenant l'essentiel de la formation sont téléchargeables. La présence d'un forum de discussion permet un accompagnement pédagogique personnalisé. Un quizz de validation des acquis clôture chaque parcours. Enfin, le blended-learning est un parcours alternant présentiel, classes virtuelles et/ou e-learning.

- **Modalités d'évaluation:**

Toute formation se clôture par une évaluation à chaud de la satisfaction du stagiaire sur le déroulement, l'organisation et les activités pédagogiques de la formation. Les intervenant(e)s évaluent également la session. La validation des acquis se fait en contrôle continu tout au long des parcours, via les exercices proposés. Sur certaines formations, une validation formelle des acquis peut se faire via un examen ou un QCM en fin de parcours. Une auto-évaluation des acquis pré et post formation est effectuée en ligne afin de permettre à chaque participant de mesurer sa progression à l'issue de la formation. Une évaluation à froid systématique sera effectuée à 6 mois et 12 mois pour s'assurer de l'ancrage des acquis et du transfert de compétences en situation professionnelle, soit par téléphone soit par questionnaire en ligne.

- **Modalités techniques FOAD:**

Les parcours sont accessibles depuis un simple lien web, envoyé par Email aux stagiaires. L'accès au module de E-learning se fait via la plateforme 360Learning. La durée d'accès au module se déclenche à partir de la réception de l'invitation de connexion. L'accès aux classes virtuelles se fait via la plateforme Teams. Le(a) stagiaire reçoit une invitation en amont de la session lui permettant de se connecter via un lien. Pour une bonne utilisation des fonctionnalités multimédia, vous devez disposer d'un poste informatique équipé d'une carte son et d'un dispositif vous permettant d'écouter du son (enceintes ou casque). En ce qui concerne la classe virtuelle, d'un microphone (éventuellement intégré au casque audio ou à la webcam), et éventuellement d'une webcam qui permettra aux autres participants et au formateur de vous voir. En cas de difficulté technique, le(a) stagiaire pourra contacter la hotline au 01 70 72 25 81, entre 9h et 17h ou par mail au logistiqueformations@infopro-digital.com et la prise en compte de la demande se fera dans les 48h.