CYBERSÉCURITÉ : PRÉVENEZ LES RISQUES CYBER DANS VOS MARCHÉS PUBLICS

Intégrer la cybersécurité dans ses processus achats

1 JOUR, 7 HEURES

FORMATIONS MÉTIER DE L'ACHETEUR PUBLIC	CODE : APA38

Objectifs de la formation

Appréhender les enjeux de la cybersécurité appliquée aux marchés publics

Identifier les obligations de l'acheteur public en matière de cybersécurité

Identifier les procédures de détection et de signalement des incidents de cybersécurité

Identifier les exigences techniques et fonctionnelles d'un appel d'offres de cybersécurité

Parmi nos formateurs

- **REMEUR Patrice**
  Expert cybersécurité et communication de crise cyber,
  CABINET GOOD INFO CYBER

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

Critères d'admission

- Cette formation entre dans le champ d'application des dispositions relatives à la formation professionnelle continue car considérée comme une action d'adaptation et de développement des compétences des salariés.

Prérequis

- Aucun prérequis n'est nécessaire

Tarifs

- Tarif Session en présentiel : 790,00 €HT

Dans un monde de plus en plus interconnecté, où les données sensibles circulent à travers les réseaux numériques, la cybersécurité devient non seulement un impératif technique, mais aussi un enjeu stratégique et économique.

Les marchés publics représentent un domaine où la cybersécurité est d'une importance particulière. En effet, les marchés publics traitent une grande quantité de données sensibles et d'informations confidentielles. La protection de ces données contre les cyberattaques est alors une priorité absolue, pour garantir la confidentialité, l'intégrité et la disponibilité des informations et aussi pour préserver la

confiance du public dans leurs institutions.

La présente formation vise à doter les participants des connaissances, compétences et outils nécessaires en matière de cybersécurité dans leurs marchés publics.

Introduction à la Cybersécurité

- Définir les concepts de base de la cybersécurité
- Cerner les réglementations et normes applicables : RGPD (Règlement Général sur la Protection des Données), directives de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), NIS-2
- Faire le point sur la stratégie nationale de cybersécurité : acteurs clés et rôles

ATELIER Quiz : via une application interactive, les stagiaires testent leurs connaissances sur le cadre théorique de la cybersécurité

Identifier les enjeux de la cybersécurité appliquée aux marchés publics

- Quels sont les enjeux de la cybersécurité dans les marchés publics ?
- Appréhender les risques associés
- Repérer les menaces et vulnérabilités cyber des marchés publics
- Cerner les risques liés aux systèmes d'information : risques liés aux données, risques liés aux prestataires ou sécurité physique
- Cerner les conséquences d'une cyberattaque dans le cadre des marchés publics : financières, juridiques, de réputation

ILLUSTRATION Des exemples d'attaques récentes ayant ciblé des entités publiques sont présentés par le formateur

La gestion des risques et conformité réglementaire

- Evaluer les risques de la cybersécurité dans le processus achat
- La conformité : normes et réglementations en matière de cybersécurité
- Quelles sont les obligations de l'acheteur public en matière de cybersécurité
- Assurer la gestion des fournisseurs et l'évaluation de leur sécurité informatique

ATELIER Analyse de la conformité juridique d'un dossier présenté par le formateur

Les meilleures pratiques en cybersécurité pour les acheteurs publics

- Quelles sont les politiques de sécurité des informations et gestion des accès
- Sécuriser les systèmes de gestion des marchés publics
- Identifier les critères pour une évaluation des offres
- Intégrer les éléments à prendre en compte dans un cahier des charges cybersécurité

ATELIER Analyse d'un appel d'offres portant sur un marché de cybersécurité. Les stagiaires sont amenés identifier les exigences techniques et fonctionnelles du marché, ainsi que les critères de sélection

ATELIER Les participants analysent un cahier des charges intégrant la cybersécurité

Evaluation des acquis et débriefing final

Dates

Paris

27/11/2024

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.