IFALP
Institut Français des Achats et de la Logistique Publics
GIP CEI - Etablissement Public

CNA CONSEIL NATIONAL DES ACHATS

FRANCE 2030 | GOUVERNEMENT Liberté Égalité Fraternité | BANQUE des TERRITOIRES

Soutenu par l'Etat dans le cadre de l'AMI «Compétences et Métiers d'Avenir» du Programme France 2030, opéré par la Caisse des Dépôts.

# CYBERSÉCURITÉ DES ACHATS PUBLICS

*Certificat IFALP*

FORMATION CONTINUE
1 JOUR

**LIEUX DE FORMATION**
**En distanciel**

EXECUTIVE EDUCATION

# OBJECTIFS

Cette formation permet aux acteurs des achats publics de comprendre les risques cyber liés aux fournisseurs et à la chaîne d'approvisionnement numérique, d'identifier les obligations réglementaires applicables, d'intégrer des exigences de sécurité dans les marchés et de dialoguer efficacement avec les RSSI, DSI et prestataires.

**À l'issue de la formation, les participants seront capables de :**

- Comprendre les principaux risques cyber dans les achats publics
- Identifier les obligations réglementaires applicables
- Intégrer des exigences de cybersécurité dans les marchés publics
- Évaluer la maturité cyber d'un fournisseur
- Sécuriser la chaîne d'approvisionnement numérique
- Rédiger des clauses cyber adaptées aux consultations
- Gérer les incidents et obligations contractuelles liées à la cybersécurité
- Dialoguer efficacement avec les RSSI, DSI et prestataires

# PROGRAMME (PRÉVISIONNEL)

| | |
|---|---|
| **Module 1**<br>**Pourquoi les achats publics sont devenus une cible cyber ?**<br>45min | - Comprendre les enjeux stratégiques<br>- Mesurer les impacts d'un achat non sécurisé |
| **Module 2**<br>**Fondamentaux de cybersécurité pour non-techniciens**<br>1h | - Acquérir un vocabulaire commun<br>- Comprendre les concepts essentiels |
| **Module 3**<br>**Cadre juridique et réglementaire des achats publics**<br>1h15 | - Identifier les obligations réglementaires<br>- Traduire les exigences dans les marchés |
| **Module 4**<br>**Intégrer la cybersécurité dans le cycle achat**<br>1h15 | - Intégrer la sécurité à chaque étape du cycle achat |
| **Module 5**<br>**Rédaction des clauses cybersécurité**<br>1h15 | - Savoir rédiger des clauses adaptéesaux consultations |
| **Module 6**<br>**Risques fournisseurs et supply chain cyber**<br>45min | - Comprendre le risque de chaîne d'approvisionnement |
| **Module 7**<br>**Mise en situation finale & conclusion**<br>1h | - Mobiliser les acquis en équipe<br>- Évaluer la montée en compétence |

# PROFILS CONCERNÉS

- Acheteurs publics
- Responsables marchés publics
- Approvisionneurs
- Juristes commande publique
- Prescripteurs techniques
- Responsables achats SI / numérique
- Agents de collectivités, administrations, établissements publics, hôpitaux, universités

# NIVEAU & FORMAT

**Niveau :** Débutant à intermédiaire - aucune compétence technique approfondie requise
**Durée :** 1 journée (7 heures effectives hors pauses)

**Format pédagogique :**
- Exposés interactifs
- Études de cas réels
- Ateliers de rédaction de clauses
- Exercices d'analyse de risques fournisseurs
- Quiz et mises en situation
- Supports : fiches pratiques, modèles de clauses, grille d'évaluation fournisseur

# LIVRABLES PÉDAGOGIQUES

**Support participant :**
- Slides complets
- Glossaire cyber
- Fiches réflexes

**Outils pratiques :**
- Questionnaire fournisseur cyber
- Grille d'évaluation
- Clauses types
- Matrice de criticité

**Ressources :**
- Guides ANSSI
- Modèles CNIL
- Référentiels ISO
- Documentation NIS2

# COMPÉTENCES VISÉES

**Savoirs :**
- Comprendre le risque cyber achat
- Connaître les obligations réglementaires

**Savoir-faire :**
- Évaluer un fournisseur
- Rédiger des clauses adaptées
- Participer à une analyse de risque

**Savoir-être :**
- Culture sécurité
- Vigilance contractuelle
- Coopération intermétiers

## LES RESPONSABLES SCIENTIFIQUES DE L'IFALP

**Irène FOGLIERINI**
**Responsable académique**
**Campus Cachan**
**Professeure Associée, Phd.**
ifoglierini@gip-cei.com

**Dr Thierry SAUVAGE**
**Directeur de recherche en Achats et Supply Chain, PhD, HDR**
tsauvage@gip-cei.com

## VOTRE RESPONSABLE FORMATION

**Sylvia DÉSIGNÉ**
**Responsable Formation Continue**
sdesigne@gip-cei.com

## MEMBRES DU COMITÉ DE LABELLISATION

- Direction des Achats de l'Etat
- France Travail
- Conseil National des Achats
- Ministère de l'Intérieur
- Ministère des Armées
- Direction des Achats de l'AP-HP
- Département des Hauts-de-Seine

# CONDITIONS D'ADMISSION ET PRÉREQUIS

Expérience professionnelle dans les achats publics.

# CANDIDATURES

**ADMISSION SUR DOSSIER ET ENTRETIENS**

Dossier à compléter en ligne sur : **www.gip-cei.com**

Formation accessible aux personnes en situation de handicap, contacter le Pôle handicap du GIP CEI : handicap@gip-cei.com

# COÛT

**LE PRIX DE LA FORMATION EST DE 600€***

- Plan de développement des compétences
- Plan de formation continue
- Financement personnel
- Compte Personnel de Formation (CPF)

** les membres du consortium sont invités à prendre contact avec l'IFALP*

# MÉTHODES ET MOYENS MOBILISÉS

- Pédagogie participative et pragmatique centrée sur la pratique
- Études de cas réels d'attaques fournisseurs et supply chain
- Ateliers de rédaction de clauses et d'analyse de risques fournisseurs
- Quiz, mises en situation et grille d'évaluation fournisseur
- Corps professoral : enseignants académiques et experts cyber

# DATES IMPORTANTES

Dates - Ouverture des candidatures : toute l'année

Durée - 1 jour

Modalités d'évaluation :
- QCM final
- Auto-évaluation de montée en compétence

Le GIP CEI / ESLI – ESTI a obtenu, le 12 juillet 2021, la certification du référentiel national de qualité Qualiopi.

Qualiopi processus certifié
RÉPUBLIQUE FRANÇAISE

La certification qualité a été délivrée au titre des catégories d'actions suivantes :
ACTIONS DE FORMATION
ACTIONS PERMETTANT DE VALIDER LES ACQUIS DE L'EXPÉRIENCE
ACTIONS DE FORMATION PAR APPRENTISSAGE

**CONTACT POUR LA FORMATION CONTINUE**

06 10 10 63 24
sdesigne@gip-cei.com

www.gip-cei.com

IFALP
Institut Français des Achats et de la Logistique Publics
GIP CEI - Etablissement Public

# CYBERSÉCURITÉ DES ACHATS PUBLICS

**FORMATION CONTINUE**

**1 JOURNÉE**

## OBJECTIF

Cette formation permet aux acteurs des achats publics de comprendre les risques cyber liés aux fournisseurs et à la chaîne d'approvisionnement numérique, d'identifier les obligations réglementaires applicables, d'intégrer des exigences de sécurité dans les marchés et de dialoguer efficacement avec les RSSI, DSI et prestataires.

## CIBLE

Acheteurs publics, Responsables marchés publics, Approvisionneurs, Juristes commande publique, Prescripteurs techniques, Responsables achats SI / numérique, Agents de collectivités, administrations, établissements publics, hôpitaux, universités

## DURÉE

1 journée en distanciel

## NIVEAU

Débutant à intermédiaire — aucune compétence technique approfondie requise

## FORMAT PÉDAGOGIQUE

- Exposés interactifs
- Études de cas réels
- Ateliers de rédaction de clauses
- Exercices d'analyse de risques fournisseurs
- Quiz et mises en situation
- Supports : fiches pratiques, modèles de clauses, grille d'évaluation fournisseur

## PROGRAMME

### MODULE 1 : POURQUOI LES ACHATS PUBLICS SONT DEVENUS UNE CIBLE CYBER

- **Panorama de la menace :** ransomware, compromission fournisseur, phishing attaque supply chain, fuite de données
- **Cibles publiques :** collectivités, hôpitaux, universités, ministères, opérateurs publics
- **Le fournisseur, porte d'entrée :** sous-traitance, SaaS / cloud, maintenance distante
- **Impacts :** interruption de service, responsabilité contractuelle, réputation, coûts, sanctions

**Icebreaker -** « Où se situe le risque cyber dans votre processus achat ? »

### MODULE 2 : FONDAMENTAUX DE CYBERSÉCURITÉ POUR NON-TECHNICIENS

- **Principes :** confidentialité, intégrité, disponibilité
- **Actifs sensibles :** données personnelles / santé, données financières, données classifiées, services critiques
- **Concepts clés :** authentification / MFA, chiffrement, sauvegarde, journalisation, cloud, VPN, SOC / CERT
- **Architectures fournisseur :** SaaS, IaaS, hébergement externe, infogérance, sous-traitance

**Quiz interactif -** Reconnaître les risques cyber dans un scénario achat

### MODULE 3 : CADRE JURIDIQUE ET RÉGLEMENTAIRE DES ACHATS PUBLICS

- **Commande publique :** besoin fonctionnel et sécurité, cyber = exigence de performance
- **RGPD & achats :** sous-traitant RGPD, clauses obligatoires, localisation des données, DPA, violations
- **Référentiels :** ISO 27001/27002, SecNumCloud, HDS, guides ANSSI, NIS2, DORA, eIDAS
- **Obligations secteur public :** homologation, PSSI, continuité d'activité, archivage & souveraineté
- **Responsabilités :** acheteur, juriste, RSSI, DPO, prescripteur, titulaire

**Étude de cas -** Analyse d'un marché public réel - identifier les lacunes cyber

# RESPONSABLES DE PROGRAMME

## Dr Thierry SAUVAGE

- Directeur de recherche en Achats et Supply Chain, PhD, HDR

## Irène FOGLIERINI

- Docteur en Sciences de la Gestion - PhD
- Master of Public Administration – MPA
- Professeure Associée, responsable académique et qualité du Campus Cachan
- Présidente de la Commission des Contrats Publics de l'APHP
- Directrice des formations achats (privée et publique) dans les grandes écoles de commerce
- Directrice des achats dans les secteurs automobiles et santé
- Auteure de plusieurs livres et articles

## MODULE 4 : INTÉGRER LA CYBERSÉCURITÉDANS LE CYCLE ACHAT

- **Définition du besoin :** données manipulées, cartographie des risques, criticité exigences minimales
- **Sourçage & consultation :** questions cyber fournisseurs, évaluation de maturité, certifications, due diligence
- **Analyse des offres :** pondération cyber, critères techniques, valeur technique vs prix, offres à risque
- **Exécution :** pilotage sécurité, audits, gestion des incidents, réversibilité, sous-traitance
- **Fin de contrat :** restitution des données, effacement sécurisé, réversibilité cloud, continuité

**Atelier pratique -** Construire une grille d'évaluation cyber fournisseur

## MODULE 5 : RÉDACTION DES CLAUSES CYBERSÉCURITÉ

- **Clauses techniques :** MFA, chiffrement, sauvegarde, hébergement, gestion des accès
- **Clauses organisationnelles :** sensibilisation, politique sécurité, habilitations, notification d'incident
- **Clauses sensibles :** auditabilité, droit de contrôle, réversibilité, localisation, SLA sécurité
- **Gestion d'incident :** délais de notification, escalade, coordination de crise, preuve & traçabilité
- **Pénalité & responsabilité :** limitation de responsabilité, assurance cyber, pénalités, résiliation

**Atelier rédactionnel -** Clause de notification d'incident · clause de réversibilité, questionnaire fournisseur

## MODULE 6 : RISQUES FOURNISSEURS ET SUPPLY CHAIN CYBER

- **Le risque supply chain :** prestataires critiques, dépendances invisibles, logiciels tiers, open source
- **Cartographie :** criticité métier, sensibilité des données, interconnexions SI
- **Évaluation continue :** audit, KPI sécurité, revues périodiques, surveillance fournisseur
- **Crise fournisseur :** fournisseur compromis, continuité de service, plans de secours

**Étude de cas -** Analyse d'une attaque supply chain célèbre - chronologie,failles, leçons achat

## MODULE 7 : MISE EN SITUATION FINALE & CONCLUSION

- **Mise en situation :** échanges, quiz et correction
- **Synthèse :** les 10 réflexes cyber de l'acheteur public, checklist opérationnelle
- **Évaluation :** QCM final, auto-évaluation

**Remise des supports -** Modèles de clauses, guide d'analyse fournisseur, bibliographie & veille