

# CYBERSÉCURITÉ OPÉRATIONNELLE LOGISTIQUE ET ACHATS

Certificat IFALP - Module spécialisé en sécurité de la Supply Chain



## LIEUX DE FORMATION

L'IFALP - Institut Français des Achats et de la Logistique Publics  
55, avenue du Président Wilson, 94230 CACHAN

EXECUTIVE EDUCATION

# MODULE SPÉCIALISÉ – CYBERSÉCURITÉ DES ACHATS ET DE LA LOGISTIQUE



## OBJECTIFS

Le programme cible les acheteurs publics, responsables logistiques et managers de la supply chain qui souhaitent acquérir une maîtrise opérationnelle des risques cyber sur leurs flux physiques, contractuels et numériques. Dans un contexte où la supply chain est devenue une cible privilégiée (rançongiciels, compromission de fournisseurs, fraudes au virement, atteintes à la souveraineté des données), le participant apprendra à identifier, évaluer et traiter les menaces qui pèsent sur ses achats et sa logistique. La formation lui apportera une vision écosystémique couvrant la gouvernance, l'analyse de risques fournisseurs, la sécurisation des systèmes d'informations logistiques (WMS, TMS, ERP) et la conduite d'incidents.



## PROGRAMME (PRÉVISIONNEL)

Le programme de formation est conçu selon une hybridation des meilleures pratiques en cybersécurité issues des secteurs public et privé. Les apprenants acquièrent une double compétence opérationnelle et stratégique.

|                                                  | Fondamentaux                                                                                                                                                                                                            | Approche opérationnelle                                                                                                                                                                               |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>GOVERNANCE &amp; CADRE RÉGLEMENTAIRE</b>      | <ul style="list-style-type: none"><li>- Cadre juridique : RGPD, NIS2, LPM, DORA</li><li>- Réglementation des achats publics et clauses de cybersécurité</li><li>- Référentiels ANSSI, ISO 27001, ISO 28000</li></ul>    | <ul style="list-style-type: none"><li>- Politique de sécurité achats / supply chain</li><li>- Rôles RSSI / DPO / acheteur / Risk Manager</li><li>- Souveraineté numérique et achats publics</li></ul> |
| <b>ANALYSE DES RISQUES FOURNISSEURS</b>          | <ul style="list-style-type: none"><li>- Méthode EBIOS Risk Manager appliquée aux achats</li><li>- Cartographie des dépendances et tiers critiques</li><li>- Évaluation cyber des fournisseurs</li></ul>                 | <ul style="list-style-type: none"><li>- Audits et questionnaires sécurité (SIG, VSA)</li><li>- Notation et scoring fournisseurs</li><li>- Traitement des non-conformités</li></ul>                    |
| <b>SÉCURISATION DES SI LOGISTIQUES</b>           | <ul style="list-style-type: none"><li>- Sécurité des SI achats (e-procurement, SI marchés)</li><li>- Sécurité des SI logistiques (WMS, TMS, ERP)</li><li>- Échanges EDI/API et chiffrement des flux</li></ul>           | <ul style="list-style-type: none"><li>- IAM et gestion des accès dans la chaîne</li><li>- Sécurité du cloud et des SaaS achats</li><li>- Traçabilité et intégrité des données</li></ul>               |
| <b>MENACES &amp; FRAUDES SUR LA SUPPLY CHAIN</b> | <ul style="list-style-type: none"><li>- Rançongiciels et attaques sur la chaîne logistique</li><li>- Fraudes au président, FOVI, faux RIB</li><li>- Compromission via les fournisseurs (supply chain attacks)</li></ul> | <ul style="list-style-type: none"><li>- Contrefaçon et traçabilité des composants</li><li>- Risques liés à l'IA et aux objets connectés (IoT)</li><li>- Veille sur les menaces sectorielles</li></ul> |
| <b>CONTRACTUALISATION &amp; CONTINUITÉ</b>       | <ul style="list-style-type: none"><li>- Clauses cyber dans les marchés publics</li><li>- PAS, PSSI, audits contractuels, droit d'audit</li><li>- Réversibilité, sortie de contrat</li></ul>                             | <ul style="list-style-type: none"><li>- SLA et indicateurs sécurité</li><li>- Notification d'incident et gouvernance crise</li><li>- Assurance cyber et transfert de risque</li></ul>                 |
| <b>GESTION DE CRISE &amp; CONTINUITÉ</b>         | <ul style="list-style-type: none"><li>- Plan de continuité d'activité supply chain</li><li>- Exercices de crise et retours d'expérience</li><li>- Communication de crise interne / fournisseurs</li></ul>               | <ul style="list-style-type: none"><li>- Cellule de crise et chaîne de décision</li><li>- Reprise d'activité et alternatives fournisseurs</li><li>- Mesure de la résilience opérationnelle</li></ul>   |

## COMPÉTENCES CIBLÉES

- Définir une politique de cybersécurité des achats
- Évaluer la maturité cyber des fournisseurs
- Sécuriser les SI achats et logistiques
- Rédiger des clauses cyber dans les marchés
- Manager les incidents et les crises cyber
- Assurer la conformité (NIS2, RGPD, LPM)
- Mesurer et piloter la performance cyber
- Sensibiliser les acteurs internes / externes



## PROFILS CONCERNÉS

- Acheteurs publics et responsables marchés
- Responsables logistique et supply chain
- RSSI, correspondants SSI, Risk Managers
- Directeurs achats et chefs de projet transformation

### LES RESPONSABLES SCIENTIFIQUES DE L'IFALP



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



**Hind ABOUSSIKINE**  
Ingénieur, Phd, responsable  
de la filière Cybersécurité  
Industrielle, GIP CEI  
haboussikine@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'APHP
- Département des Hauts-de-Seine



## **CONDITIONS D'ADMISSION ET PRÉREQUIS**

Validation du parcours académique et expérience dans la fonction achats, logistique, supply chain ou sécurité des SI.

### **CANDIDATURES**

#### **ADMISSION SUR DOSSIER ET ENTRETIENS**

Dossier à compléter en ligne sur : [www.gip-cei.com](http://www.gip-cei.com)

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

### **MÉTHODES ET MOYENS MOBILISÉS**

- Pédagogie centrée sur une approche participative (études de cas, mises en situation, war games cyber)
- Travaux pratiques en laboratoire (analyse d'incident, audit fournisseur)
- Corps professoral composé de professeurs académiques et experts achats / cybersécurité
- Campus en région parisienne et séances en immersion en administration

### **DATES IMPORTANTES**

Ouverture des candidatures : toute l'année  
Rentrée : janvier 2027

### **DURÉE**

10 jours répartis sur une année (5 sessions de 2 jours).

### **COÛT**

Le prix de la formation est de 5 500 €\*.

- 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*

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



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  
[sdesigner@gip-cei.com](mailto:sdesigner@gip-cei.com)



[www.gip-cei.com](http://www.gip-cei.com)