SCIENCES PO GRENOBLE

FORMATION CONTINUE

CERTIFICAT
ENJEUX DE SÉCURITÉ : INNOVATIONS TECHNIQUES ET STRATÉGIQUES

Dans le cadre du développement de son offre de formation dans le champ de la gestion des risques et de la sécurité, Sciences Po Grenoble propose un nouveau certificat intitulé "Enjeux de sécurité : innovations techniques et stratégiques".
Ce certificat est construit sur la complémentarité de trois séminaires de deux jours chacun qui peuvent être soit suivis indépendamment les uns des autres, soit de façon combinée. Dans ce dernier cas ils donnent lieu à la délivrance d'un certificat sous certaines modalités. Les trois séminaires proposés portent sur les thématiques suivantes :

Séminaire 1 → Intelligence de politique locale de sécurité

Séminaire 2 → Cybercriminalité : anticiper, déceler, réagir à une attaque informatique

Séminaire 3 → Profiling

Basé sur une architecture modulaire, ce certificat vise à faciliter l'approfondissement des compétences de professionnels en activité ou de personnes en reconversion se destinant aux métiers de la sécurité.

INTELLIGENCE DE POLITIQUE LOCALE DE SÉCURITÉ

JEUDI 24 / VENDREDI 25 JANVIER 2019

L'intelligence de politique de sécurité est une méthode de réflexion stratégique qui a pour but d'aider les acteurs locaux de la sécurité publique à élaborer et à conduire des stratégies territoriales de sécurité. Les chances de réussite de telles stratégies dépendent de la qualité du travail d'information et de connaissance qui prépare leur mise en place et accompagne leur mise en œuvre.

Les enjeux de ce travail d'intelligence sont multiples. Il doit identifier les sources d'insécurité dans le territoire et déterminer celles qui méritent un traitement prioritaire. Il doit analyser de façon méthodique les menaces et problèmes ciblés, afin de mettre au point une réponse sur mesure. Il doit s'inscrire dans un cadre partenarial qui suppose partage des informations, coproduction des diagnostics, co-construction des solutions et copilotage de l'action publique de sécurité. Enfin, il doit évaluer avec rigueur et objectivité l'efficacité et l'impact des stratégies qui ont été déployées.

OBJECTIFS

- Mieux appréhender le contexte sociopolitique et le cadre institutionnel des politiques locales de sécurité en France, en ayant des éléments de comparaison avec d'autres pays.
- Connaître les étapes et les points-clés de la démarche d'élaboration d'une stratégie territoriale de sécurité.
- Avoir un aperçu des instruments et méthodes d'information et d'analyse pouvant être mobilisés pour la conception, le suivi et l'évaluation de l'action publique de sécurité.
- Comprendre la logique du travail en réseau dans le domaine de la sécurité et être capable de jouer un rôle moteur dans l'organisation et le fonctionnement des dispositifs partenariaux en charge de questions de sécurité.

PARTICIPANTS

Ce séminaire s'adresse aux :

- Elus et cadres territoriaux (coordinateurs CLSPD notamment) en charge de la prévention, de la tranquillité et de la sécurité
- Responsables de police municipale
- Cadres de la police et de la gendarmerie participant à des activités partenariales (chefs de circonscription territoriale, membres des états-majors, chefs de SIAP, commandants d'unités territoriales, responsables de service prévention et partenariat, délégués à la cohésion police population...)
- Responsables préfectoraux en charge des politiques de sécurité (délégués du préfet...)
- Responsables des questions de sécurité dans l'éducation nationale, les offices HLM, les sociétés de transport en commun

INTERVENANTS

Thierry DELPEUCH, *Chercheur CNRS en Sociologie et Science Politique, PACTE - Sciences Po Grenoble - Communauté Université Grenoble Alpes*

Didier JOUBERT, *Commissaire général et conseiller du Directeur central de la Police Nationale*

Jean-Marc JAFFRÉ, *membre du Centre de Recherche de l'Ecole des Officiers Gendarmerie Nationale*

JEUDI 24 JANVIER 2019 — 9H30-17H00

Connaître et conduire les politiques locales de sécurité

- L'action publique de sécurité en France : les perceptions de l'insécurité, les demandes de sécurité, les cadres institutionnels et professionnels de l'action publique de sécurité, les débats scientifiques autour des réponses publiques aux problèmes de sécurité.
- Comment bien travailler en réseau pour résoudre les problèmes de sécurité : concertation, coordination, animation, gouvernance, influence et leadership, règles du jeu à respecter...

DÉJEUNER

L'évaluation stratégique de l'environnement sécuritaire

- Réaliser un diagnostic territorial de sécurité
- Analyser un problème de sécurité

VENDREDI 25 JANVIER 2019 – 9H00 - 16H30

La méthode de raisonnement pour la conception et le suivi d'une stratégie territoriale de sécurité

- Principaux points clés à prendre en considération à l'étape de l'élaboration (présentation de la méthode de raisonnement stratégique)
- Exemples concrets de dispositifs d'intelligence au service d'une stratégie territoriale de sécurité
- L'adoption et l'appropriation de nouveaux instruments et de nouvelles méthodes d'intelligence : management de l'innovation et conduite du changement

DÉJEUNER

L'évaluation des stratégies territoriales de sécurité

- Les critères d'évaluation : effectivité, efficience, efficacité, qualité de service, satisfaction du public, impact, effets pervers...
- La démarche d'évaluation d'une action spécifique

CYBERCRIMINALITÉ : ANTICIPER, DÉCELER, RÉAGIR À UNE ATTAQUE INFORMATIQUE

JEUDI 11 / VENDREDI 12 AVRIL 2019

La croissance exponentielle et multiforme de la criminalité informatique concerne le secteur public qui détient nombre d'informations personnelles et sensibles dont il se doit d'assurer la sécurité. (État civil, urbanisme, marchés publics...).

L'ouverture des administrations locales à l'univers d'internet et la dématérialisation croissante des relations avec les usagers, fournisseurs, citoyens rend indispensable de se préparer concrètement à l'éventualité d'attaques cybercriminelles et prendre les dispositions pour améliorer les dispositifs de prévention existants.

OBJECTIFS

- Estimer les risques existants dans leur diversité
- Rappeler les bonnes pratiques de la sécurité de l'information
- Connaître les méthodes et les outils concrets permettant d'anticiper et de déceler une attaque informatique avec des tests d'intrusion
- Analyser les tentatives d'intrusion
- Réagir à l'intrusion au niveau informatique, juridique, administratif
- Savoir communiquer sur l'incident en interne et en externe

PARTICIPANTS

Ce séminaire s'adresse aux :

- Elus notamment ceux en charge de la sécurité
- Cadres responsables des systèmes d'information des collectivités et institution publiques
- DGS, DGA et cadres en charge de la gestion de données publiques

INTERVENANTS

Benjamin DUCOS, *Responsable du management des risques de l'information, AXA*

Emmanuel BRESSON, *Chargé de mission Cyber et Intelligence Artificielle au cabinet de la ministre des Armées*

Florent MION, *Commissaire Divisionnaire, chef de la division criminelle de la DIPJ de Lyon*

JEUDI 11 AVRIL 2019 — 9H30-17H00

Connaître la cybercriminalité

- Rétrospective de la cybercriminalité
- Les formes de la cybercriminalité
- Les cybercriminels : qui sont-ils, quelles sont leurs motivations, quels objectifs ?
- Les infractions : les destructions, le vol d'information, les « occupations sauvages », les détournements, la diffusion d'information confidentielle, le chantage....
- Les conséquences : matérielles, financières légales, politiques...

DÉJEUNER

Anticiper

- Organiser la sécurité dans ses différentes dimensions : Technique / Organisationnelle / Juridique
- Classifier les biens informationnels au regard de leur sensibilité à une attaque cybercriminelle et / ou de leur importance pour la collectivité
- Le statut particulier des informations nominatives et l'obligation légale de sécurité : rôle de la CNIL et cadre légal des informations

VENDREDI 12 AVRIL 2019 — 9H00 - 16H30

Gérer une situation d'attaque informatique

- Qualifier l'attaque et ses objectifs
- Comprendre ce qui est en train d'être fait / a été fait par les pirates
- Evaluer les impacts inhérents à l'attaque ainsi qualifiée
- Gestion de la crise - Check List des opérations à réaliser (techniques, administratives, judiciaires)
- Après la crise : revoir les processus de gestion de la sécurité et définir des indicateurs

DÉJEUNER

Retour d'expérience de cas concrets

- Nature et déroulement de l'attaque
- Conséquences de l'attaque
- Précautions prises depuis l'attaque
- Exemples de cyber attaques : WannaCry / NSA ; Petya / NotPetya ; Deloitte ; Uber

Etude de cas sous forme de mise en situation

PROFILING

JEUDI 13 / VENDREDI 14 JUIN 2019

Le terrorisme, les actes criminels, les intrusions et la criminalité économique, mais aussi la détection de situations de crise et des comportements à risque, constituent des domaines pertinents où l'anticipation, la lecture des signaux faibles, la collecte et l'exploitation de données de différentes natures constituent un atout majeur dans la gestion des situations de crise.

OBJECTIFS

- Définir les bases scientifiques du profiling
- S'initier aux techniques du profiling
- Connaitre les domaines d'application, les méthodologies et les situer dans la boite à outils de l'anticipation et de la gestion des risques

PARTICIPANTS

Ce séminaire s'adresse aux :

- Professionnels de la sécurité, risk-managers, acteurs de la sécurité dans les entreprises
- Responsables des ressources humaines dans les entreprises et les collectivités

INTERVENANTS

Eric LENFANT, *Docteur, Directeur Médiform Consult*

Christian PERALDI, *Général de division (2s)*

Taoufik BOURGOU, *Maitre de Conférences HDR en science Politique, Université de Lyon & Sciences Po Lyon, Chercheur au CERDAP2 - Sciences Po Grenoble*

Capitaine JANDOT, *Gendarmerie Nationale, Département des Sciences de l'Analyse Criminelle*

Chef d'Escadron BRUNEL-DUPIN, *Gendarmerie Nationale, Département des Sciences du Comportement*

Samuel DEMARCHI, *Maitre de conférences Psychologie Sociale, Paris VIII*

JEUDI 13 JUIN 2019 — 9H30-17H00

Introduction aux bases scientifiques du profiling

Profilage du comportement criminel (Criminal Behavior, Profiling)

Profilage d'investigation (Investigative Profiling) et spécifique (déduction d'un profil personnalisé)

DÉJEUNER

Profilage géographique et hotspot mapping

VENDREDI 14 JUIN 2019 — 9H30-17H00

Profilage prédictif et signaux faibles

Mission de sécurité des pouvoirs publics, innovations technologiques

DÉJEUNER

Limites du profilage, perspectives et évolutions

RENSEIGNEMENTS ET INSCRIPTIONS

Le cadre pédagogique du certificat n'exige aucun prérequis formel.

Chaque séminaire s'articule autour d'une alternance d'exposés présentés par des intervenants spécialistes des questions traitées et de discussions avec les participants.

Les participants peuvent s'inscrire pour l'ensemble du certificat (3 séminaires) ou pour un des séminaires au choix.

Sciences Po Grenoble est agréé pour la formation des élus.

Tarif : 3000 euros pour le certificat complet ou 1000 euros par séminaire.
Ce coût est exempté de TVA.

La validation du certificat se fait sur la base :

→ de l'attestation par le responsable pédagogique du suivi assidu par le candidat de chacun des modules qui composent le certificat

→ de la validation par le responsable pédagogique de la production par le candidat d'un document synthétique d'un format de 3 à 5 pages explicitant ses acquis, notamment par la mise en regard de ses expériences en situation professionnelle et de ses pratiques avec les enseignements et interrogations tirées de la formation suivie.

RESPONSABLE PÉDAGOGIQUE

Jean Charles FROMENT
Directeur de Sciences Po Grenoble, Professeur de droit public

Pour toutes informations complémentaires et obtenir le bulletin d'inscription, contactez :

RESPONSABLE ADMINISTRATIVE

Stéphanie MARTIN
Chargée de développement de la Formation Continue
stephanie.martin@sciencespo-grenoble.fr
Tél. 04 76 82 60 13

Sciences Po Grenoble
Institut d'études politiques de Grenoble
1030 av. centrale - Domaine Universitaire
38400 Saint-Martin-d'Hères

→ **www.sciencespo-grenoble.fr**