MAS
Maîtrise d'études avancées
Master of Advanced Studies

DAS
Diplôme de formation continue
Diploma of Advanced Studies

CAS
Certificat de formation continue
Certificate of Advanced Studies

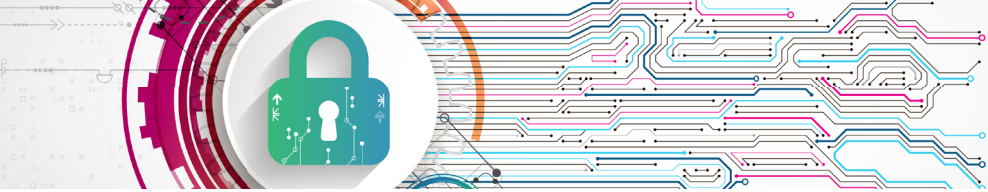
Sécurité de l'information

janvier 2024 > décembre 2025

Formation continue en cours d'emploi et modulaire

CENTRE UNIVERSITAIRE D'INFORMATIQUE | CUI

UNIVERSITÉ DE GENÈVE



Direction

- **Professeur Dimitri Konstantas**, Centre universitaire d'informatique, Université de Genève

Coordination

- **Philippe Doerks**, Centre universitaire d'informatique, Université de Genève

Comité directeur

- **Éric Choffat**, (MBA, CSSI, CISA, CISM, CISSP), Global Information Security & Risk Control Lead, JT International
- **Anastasija Collen**, Computer Scientist, Université de Genève
- **Professeur Dimitri Konstantas**, Centre universitaire d'informatique, Université de Genève
- **Professeur Jean-Henry Morin**, Université de Genève
- **Jean-Luc Pillet**, adjoint scientifique, Université de Genève
- **Jean-Pierre Therre**, Managing Partner, Corporate Resilience Advisors Sarl

Comité scientifique

Vous pouvez consulter le détail des membres du Comité scientifique aux adresses suivantes:

CAS: Cliquez ici

DAS: Cliquez ici

MAS: Cliquez ici

Intervenant-es

Vous pouvez consulter le détail des intervenant-es aux adresses suivantes:

CAS: Cliquez ici

DAS: Cliquez ici

MAS: Cliquez ici

Se former à la sécurité de l'information de manière multidisciplinaire pour répondre aux défis actuels et futurs

Les métiers dans le domaine de la sécurité de l'information sont multiples et se déploient dans un contexte en perpétuelles évolutions. Quelles sont les compétences requises? Quelles formations faut-il suivre? La personne responsable de la sécurité de l'information doit être compétente dans une diversité d'activités: communication, stratégie, audit, pédagogie, management, risque, juridique, gouvernance, et coordination.

Ces compétences nécessitent d'être en permanence renouvelées. Les personnes responsables de la sécurité de l'information doivent en effet non seulement être en mesure d'identifier les risques actuels et d'anticiper les risques futurs, mais aussi de planifier et d'assurer le suivi de la mise en place des mesures de prévention, détection et correction adéquates, et surtout de sensibiliser les collaborateurs et collaboratrices pour que chacun-e puisse acquérir les bons réflexes.

Pour assurer cette mission, ces personnes doivent se former dans les cinq dimensions clés de la sécurité de l'information et de la gestion du risque.

- **Managériale.** Cette dimension s'articule autour de l'évaluation et de la gestion des risques de l'information, la mise en place d'indicateurs et métriques, l'organisation de la sécurité et de plans de continuité d'activités, la conception d'une méthodologie d'audit, etc.
- **Organisationnelle et humaine**. Cette dimension s'articule autour de la conception et de la mise en œuvre de plans d'assurance qualité et de référentiels qualité, du management de projets, de la sensibilisation et motivation du personnel, etc.
- **Technologique**. Cette dimension s'articule autour de l'implémentation de nouvelles applications de l'informatique, de la refonte des systèmes d'information, de la sécurité des réseaux et des communications internet, des architectures de sécurité, etc.
- **Juridique**. Cette dimension s'articule autour de la mise en conformité avec les réglementations et les lois en vigueur.
- **Stratégique et de gouvernance**. Cette dimension s'articule autour de l'intégration de la sécurité de l'information au cœur de la direction d'entreprise.

Public

- Responsables de la sécurité de l'information et du Risk Management
- Responsables des systèmes d'information
- Responsables sécurité
- Responsables des politiques de sécurité et Compliance
- Chef-fes de projets de la sécurité de l'information
- Conseiller-es à la protection des données
- Auditeurs/trices des systèmes d'information
- Juristes chargé-es de sécurité et de conformité de l'information
- Toute personne qui veut en savoir plus sur la Cybersécurité

Objectifs

- Se former aux concepts Cyber et apporter des compétences à la gouvernance de la sécurité de l'information
- Identifier les risques nouveaux dans des domaines tel que:
  - Le «nuage»
  - L'intelligence artificielle
  - L'intelligence économique
  - Loi sur la protection des données nLPD, RGPD, Cloud Act, etc.
- Planifier et assurer le suivi de la mise en place des mesures de prévention de détection et de correction adéquates pour y faire face
- Sensibiliser les collaborateurs/trices de manière que chacun-e puisse acquérir les bons réflexes

Compétences visées

- Anticiper la communication et faire face aux médias lors d'une situation de crise
- Comprendre les gestions d'identité et les contrôles d'accès avec les solutions d'aujourd'hui et de demain
- Comprendre les mécanismes de la cybercriminalité et mettre en œuvre les principaux moyens de défense pour s'en protéger

- Connaître les différentes stratégies et processus de réponse aux incidents, autant sur le plan technique (incident response) que sur le plan organisationnel (incident handling)
- Élaborer et mettre en œuvre une stratégie de protection du patrimoine informationnel et cognitif de l'entreprise
- Élaborer et mettre en œuvre une stratégie de veille active (y compris threat intelligence)
- Élaborer une politique de sécurité de l'information et la décliner en des standards et procédures visant en la mise en place de mesures organisationnelles et techniques justifiées et applicables en compte leur impact sur l'organisation et leur efficacité
- Identifier et élaborer des stratégies, des scénarios et des plans adaptés de continuité des activités des affaires. Appliquer les différents processus d'anticipation, de sauvegarde, de contingentement et de relance des activités de l'entreprise
- Identifier les enjeux et les techniques du renseignement offensif, concurrentiel ou institutionnel, ainsi que les possibles mesures de contre-renseignement
- Maîtriser les principes généraux de la protection des données personnelles
- Maîtriser les processus d'analyse forensiques ainsi que les pièges à éviter
- Mettre en place une stratégie de réponse aux incidents comprenant les méthodologies, les outils et les ressources nécessaires
- Planifier et réaliser une mission d'audit des systèmes d'information
- Produire des indicateurs et des tableaux de bord adaptés à chaque partie prenante
- Protéger proactivement son entreprise dans le monde virtuel
- Surveiller la conformité des règles en vigueur et rapporter à la direction
- Utiliser des modèles, outils et bonnes pratiques de la gouvernance sécurité

Modalités et méthodes pédagogiques

- Le programme est animé par des universitaires et des professionnelles, toutes et tous spécialistes des domaines relatifs à la sécurité de l'information et des systèmes d'information. La diversité des compétences des enseignant-es assure la pluridisciplinarité de cette formation.
- Les méthodes pédagogiques utilisées offrent un environnement propice aux échanges d'idées et d'expériences et encouragent la constitution d'un «réseau de compétences» entre les participant-es d'une volée et des volées précédentes.
- L'enseignement donné de manière didactique fait appel à des études de cas et à des exercices pratiques dédiés à la sécurité de l'information. Un site web sécurisé est mis à disposition pendant la durée de la formation.

Structure des formations

Les formations en Sécurité de l'information de l'Université de Genève répondent à ces impératifs et permettent l'acquisition de connaissances et compétences de manière modulaire. Elles s'articulent en trois niveaux:

- Certificat de formation continue (CAS) en Sécurité de l'Information
- Diplôme de formation continue (DAS) en Sécurité de l'Information
- Maîtrise universitaire d'études avancées (MAS) en Sécurité de l'Information

La formation de niveau CAS permet aux personnes relativement novices dans le domaine de la sécurité de l'information d'acquérir les fondamentaux du domaine. Trois parcours sont proposés pour la formation de niveau CAS:

- Parcours 1: «Protection de l'information: technologies et services»
- Parcours 2: «Gouvernance de la sécurité de l'information dans les entreprises»
- Parcours 3: «Gestion de la sécurité dans un contexte global»

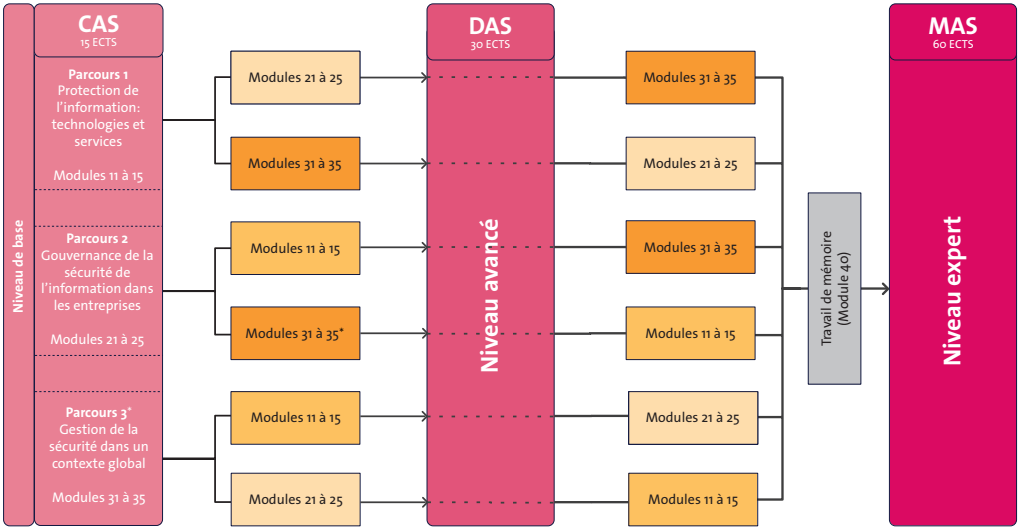
La formation de niveau DAS permet d'approfondir ces fondamentaux et de les compléter par de nouvelles compétences sur des aspects de gouvernance.

La formation de niveau MAS permet de former des expert-es, à même de naviguer au travers de toutes les dimensions de la sécurité de l'information.

Les modules qui constituent chaque niveau de la formation peuvent également être suivis «à la carte» et de manière indépendante. Si un nombre suffisant de crédits ECTS sont acquis par une combinaison de plusieurs modules, il est alors possible d'obtenir un CAS ou un DAS «personnalisé», sous réserve de l'évaluation ad hoc par le Comité directeur, qui statue, le cas échéant, sur l'obtention du titre.

Chaque module se compose de 24 heures d'enseignement chacun, y compris le contrôle des connaissances et équivaut à 3 crédits ECTS. Le travail de mémoire représente 15 crédits ECTS.

Les formations sont articulées de manière à pouvoir progresser à travers ces différents niveaux.



*Des prérequis peuvent être nécessaires, veuillez consulter le programme détaillé des modules

Chaque module se compose de 24 heures d'enseignement chacun, y compris le contrôle des connaissances et équivaut à 3 crédits ECTS. Le travail de mémoire représente 15 crédits ECTS.

- La durée des études pour le CAS est d'un semestre (15 crédits ECTS).
- La durée des études pour le DAS est de deux semestres (30 crédits ECTS).
- La durée des études pour le MAS est de quatre semestres (60 crédits ECTS).

Le parcours à la carte et personnalisé (optionnel)

Pour des personnes qui ne désirent pas suivre l'intégralité d'une formation, il est possible de s'inscrire à un ou plusieurs modules isolés. Dans le cas où le/la participant-e valide 15 crédits ECTS, il/elle obtient un CAS personnalisé sans thème. Si 30 crédits ECTS sont validés, il est possible d'obtenir un DAS personnalisé sans thème. Les modalités pratiques et divers détails concernant cette inscription personnalisée devront être approuvés par le Comité scientifique.

Programme

Module 11 | **Fondements de la sécurité de l'information (3 ECTS)**

Présentation des fondamentaux des systèmes d'information et leur relation avec la sécurité de l'information.

Module 12 | **Gestion des risques de l'information (3 ECTS)**

Présentation des standards, normes et méthodes utilisées pour l'analyse des risques liés aux systèmes d'information (ISO 2700x, Ebios, Bâle II). Mise en perspective de ces standards sectoriels dans un cadre d'Entreprise wide Risk Management supporté par un standard global (ISO 31000, COSO II).

Module 13 | **Continuité des activités, gestion de crise et sécurité physique (3 ECTS)**

Les enjeux réels pour l'entreprise des situations à hauts risques ou de crise. Cadre réglementaire, normatif et bonnes pratiques de la gestion de la continuité des activités (BCM). La méthodologie et les constituants essentiels de la continuité des activités: la gouvernance, la stratégie, les scénarios, les plans, les mesures et les tests. L'analyse d'impact (BIA): une étape clé pour assurer l'identification des processus métiers et des ressources opérationnelles les plus critiques pour l'entreprise. L'orchestration et la maîtrise des phases de veille, de crise, de contingence et de relance. La validation et la maintenance des solutions de continuité des activités. Stratégies de protection physique pour les ressources (humaines, matérielles et immatérielles) de l'information. Mise en place de solutions de réduction de risques adaptées dans le domaine de la sécurité incendie, anti-intrusion, le contrôle des accès et la vidéosurveillance.

Module optionnel | **Système d'exploitation, composants réseaux et protocoles internet**

Fonctionnement de Windows. Autorisations NTFS. Modèle en couche des protocoles internet. Gouvernance internet. Réseau local Ethernet, internetworking et configuration dynamique. Analyse des protocoles DNS et http. Arborescence DNS et mécanismes Web (cache, cookie, logs). Proxy http.

Module 14 | **Bonnes pratiques des dispositifs de sécurité logique (3 ECTS)**

Défense périmétrique. Chiffrements et signature numérique. Infrastructure à clé publique. Identités numériques et technologies d'authentification. Réseaux privés virtuels. Réseau sans fil. Attaques et menaces applicatives (messagerie et web). Virtualisation et Cloud Computing. Tests de pénétration. Prérequis: connaissances réseau. Le module optionnel peut aider à cette préparation.

Module 15 | **Veille et tendances technologiques en sécurité de l'information (3 ECTS)**

Les nouvelles tendances des TIC (p. ex. mobilité, VoIP, nouvelles applications Internet, biométrie,...) qui ont un impact significatif en sécurité de l'information. Analyse des risques et opportunités que ces nouvelles tendances peuvent induire dans une société. Prérequis: module 14

Module 21 | **Aspects juridiques, éthiques et sécuritaires liés à la digitalisation de la société (3 ECTS)**

L'impact sociétal lié à la transformation numérique concerne non seulement les entreprises, mais également l'individu et le citoyen. Les objets interconnectés, les voitures autonomes et les Smart Cities, les cybermonnaies sont aujourd'hui incontournables et vont façonner notre mode de vie. Dans ce contexte, ce module a pour but

d'aborder les aspects sécuritaires et légaux de cette évolution digitale, mais également d'en étudier les aspects réglementaires et contractuels.

Module 22 | **Gouvernance de la sécurité et processus métiers (3 ECTS)**

Le processus Cobit ME4 fournir la gouvernance IT. Les piliers de la gouvernance. L'alignement stratégique et les expériences vécues. Les objectifs de contrôle de la gouvernance IT: concept / différences entre Gouvernance et Contrôle financier. La gestion des performances et les métriques.

Module 23 | **Audit des systèmes d'information (3 ECTS)**

Cobit, planification de mission. Audit des SI. Audit des applications et des accès logiques. Audit SDLC et de la gestion des changements. Comité d'audit et audit de la gestion des incidents.

Module 24 | **Séminaires sur la sécurité de l'information (3 ECTS)**

Obligation pour les participant-es de suivre 10 séminaires avec la rédaction d'une synthèse et d'une analyse critique pour chaque séminaire sur une période de 15 mois.

Module 25 | **La protection des données appliquées (3 ECTS)**

Les principes régissant le traitement des données personnelles, selon les législations suisse et européenne, sont expliqués et mis en œuvre dans des cas concrets. L'enseignement de ce module est réparti sur l'ensemble du DAS, de manière à mettre en lumière les aspects de protection des données personnelles lorsque la matière des autres modules, domaines englobés par la sécurité de l'information, le nécessite ou le justifie. L'objectif est de donner les outils permettant la création d'un système de gestion de la protection des données en entreprise.

Module 31 | **Intelligence économique (3 ECTS)**

Les enjeux de l'intelligence économique et stratégique dans l'entreprise d'aujourd'hui, de la multinationale à la PME/PMI. La protection du patrimoine informationnel et cognitif des entreprises et la recherche active d'informations pertinentes (marchés, cadre juridique et réglementaire, concurrents, produits, prestations, technologies, etc.). La méthodologie et les techniques de l'intelligence économique comme processus d'aide à la décision stratégique ainsi que comme outil de rétention des avantages concurrentiels. La conception et la mise en œuvre d'une structure de veille. Le développement d'une culture collective, éventuellement offensive, de l'information à l'interne et vers l'environnement de l'entreprise. Les changements induits par les initiatives et les pratiques d'intelligence économique. Étude de quelques cas pratiques.

Module 32 | **Le Big Data, intelligence artificielle et Cloud: enjeux sécuritaires (3 ECTS)**

Les concepts liés au Big Data: les algorithmes et machine learning, réseaux neuronaux et les ambitions de l'AI seront étudiés dans ce module en tenant compte des aspects sécuritaires. Une partie importante de ce module sera consacrée à l'évolution du Cloud, conséquente de l'accroissement massif du volume de données: gestion des données, méthodes d'intégration, moyens d'analyse et logiciels de qualité seront les éléments qui seront abordés dans ce contexte dans une perspective «sécurité».

Module 33 | **Développement et mise en œuvre d'une politique de sécurité de l'information (3 ECTS)**

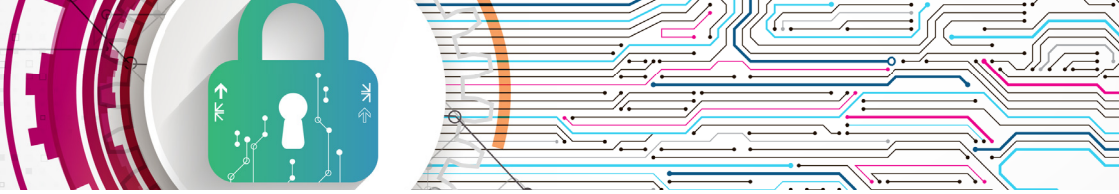
Définitions concernant les Politiques et Procédures (P&P) de l'entreprise. La rédaction des P&P suivant l'audience. Les P&P de Sécurité de l'information par domaines et leur intégration. L'adéquation au contexte d'affaires, légal et réglementaire et au style de gouvernance. L'utilisation de l'architecture d'entreprise pour le design des P&Ps. Coût de mise en œuvre vs bénéfices en termes de réduction des risques. «Auditabilité» et lien avec le cadre de conformité (ex. SOX, Basel II). Promotion et communication des P&P. Applicabilité aux tierces parties. L'éveil (awareness). Le suivi de conformité. Ce module est un module de synthèse utilisant la plupart des notions acquises dans les précédents modules (Risques, Conformité, Audit, Bonnes Pratiques, etc.). Il est basé sur une étude de cas. Prérequis: modules 11, 12, 23.

Module 34 | **Cybercriminalité, recherche de preuves et cyber forensics (3 ECTS)**

Analyse de la criminalité et TIC. Traces numériques et investigations, Sciences forensiques Prérequis: modules 11, 12, 14, 15, 31

Module 35 | **Savoir communiquer en entreprise, y compris en cas de crise (3 ECTS)**

La communication écrite. La communication orale. Savoir adapter le discours en tenant compte du profil de l'interlocuteur. La culture d'entreprise. Les compétences spécifiques en communication en cas de crise. Les canaux à utiliser. Les procédures à mettre en œuvre. La stratégie avec les médias.



Module 40 | **Mémoire MAS-InfoSec (15 ECTS)**

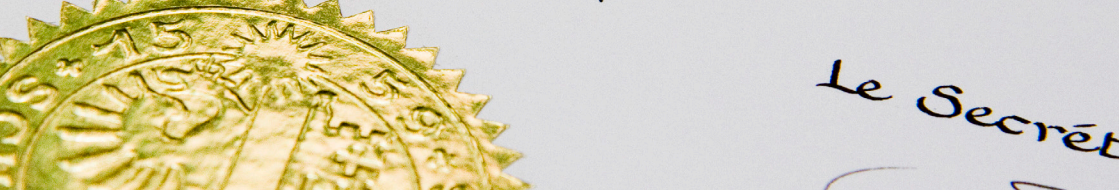
Ce travail doit permettre de démontrer que la personne est apte à gérer un projet académique et à analyser puis résoudre des problèmes concrets dans le domaine choisi. Les critères sont les suivants: pertinence du sujet, revue de la littérature avec références bibliographiques, méthodologie appliquée (standard et normes en sécurité de l'information), analyse effectuée au sein de l'entreprise, la faisabilité et les recommandations pratiques qui peuvent déboucher vers un projet. Le superviseur contrôlera le choix du sujet, la planification du projet, la collecte des données, les actions à effectuer et les recommandations qui en découlent. La Direction InfoSec validera la qualité du travail rendu.

Modalités d'évaluation

Chaque module est validé par un contrôle des connaissances (travail individuel et/ou travail de groupe) et/ou un examen. Le module 24 est validé par la remise de synthèses et d'analyses critiques des séminaires suivis.

Travail de fin d'études

Pour le MAS uniquement, le module 40 est validé lorsque le travail de mémoire est conforme aux exigences d'un mémoire MAS.



Titre obtenu

Les modalités d'évaluation des connaissances sont définies dans le règlement d'étude du programme remis aux participant-es en début de formation.

L'obtention du titre est conditionnée à la fréquentation assidue de tous les modules et à l'exécution de tous les travaux requis à la satisfaction des enseignants.

L'Université de Genève délivre les titres suivants aux participant-es ayant satisfait aux conditions d'évaluation des connaissances:

Le Certificat de formation continue en Sécurité de l'information (*Certificate of Advanced Studies in Information Security*) (15 crédits ECTS).

Le Diplôme de formation continue en Sécurité de l'Information (*Diploma of Advanced Studies in Information Security*) (30 crédits ECTS).

La Maîtrise universitaire d'études avancées en Sécurité de l'Information (*Master of Advanced Studies in Information Security*) (60 crédits ECTS).

Les personnes inscrites à un ou plusieurs modules isolés recevront une attestation de réussite si elles satisfont aux conditions d'attribution des crédits ECTS correspondants.

Renseignements pratiques

Conditions d'admission

- Titulaire d'une maîtrise universitaire de l'Université de Genève, d'un master d'une Haute École Spécialisée ou d'un titre jugé équivalent, ou titulaire d'un baccalauréat universitaire de l'Université de Genève, d'un bachelor d'une Haute École Spécialisée ou d'un titre jugé équivalent
- Expérience professionnelle d'au moins 3 ans dans le domaine concerné

L'admission est prononcée, par le Comité directeur, sur examen d'un dossier.

Bulletin d'inscription à télécharger sur
www.unige.ch/formcont/cours/mas-infosec

Connaissances préalables requises

Les candidat-es doivent être familiarisé-es avec les outils, méthodes et normes de base de gestion et d'utilisation des systèmes d'information. La connaissance de l'anglais technique est recommandée.

Délai d'inscription

- Pour chaque CAS, DAS ou MAS, l'inscription doit parvenir au moins 1 mois avant le début de la formation.
- Option modules individuels et personnalisés: la candidature d'inscription doit parvenir 1 mois avant le début du module choisi par le/la candidat-e.

Les candidatures d'inscription doivent être adressées à:

- En ligne via: Cliquez ici
- infosec@unige.ch ou
- Philippe Doerks, Centre universitaire d'informatique (CUI), Batelle - Bâtiment A, Route de Drize 7, CH 1227 Carouge, Genève

Remarque: les candidatures soumises hors délai ne sont considérées que dans la mesure où des places seraient encore disponibles.

Finances d'inscription
CAS: CHF 7'000.-
DAS: CHF 10'000.-
MAS: CHF 15'000.-
Prix par module: CHF 1'700.-

L'État de Genève encourageant la formation professionnelle des adultes, un chèque annuel de CHF 750.-, cumulable pendant 3 ans, peut être demandé avant le début des cours par les participant-es répondant aux critères d'attribution. Informations disponibles sur: www.ge.ch/beneficier-cheque-annuel-formation.

Lieu des cours

Fédération des Entreprises Romandes, Rue de Saint-Jean 98, 1201 Genève (sauf indication contraire)

Horaires
17:15 – 21:00 ou
17:30 – 21:15 (en fonction de l'année)
Comprenant une pause de 15 minutes

Renseignements complémentaires
Université de Genève
CUI – Infosec
Battelle - bâtiment A
7, route de Drize
CH-1227 Carouge
infosec@unige.ch | Tél:+41 22 379 01 16

Partenariats

DPO Associates

Schweizerisches Qualitätszertifikat für Weiterbildungsinstitutionen
Certificat suisse de qualité pour les institutions de formation continue
Certificato svizzero di qualità per istituzioni di formazione continua
Swiss Quality Certificate for Adult Continuing Education Institutions

swissuniversities

Centre pour la formation continue et à distance | CFCD

Université de Genève | CH-1211 Genève 4

Tél: +41 (0)22 379 78 33 | info-formcont@unige.ch

www.unige.ch/formcont