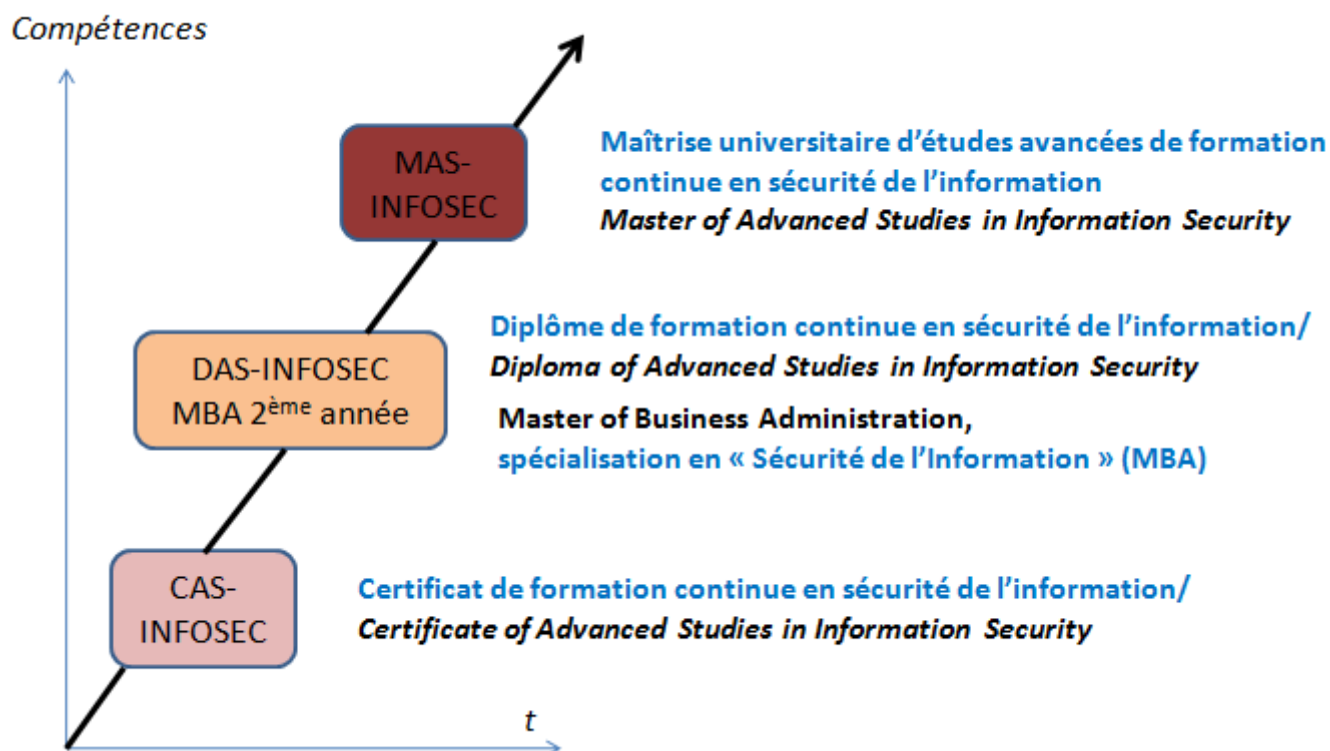




Se former et se perfectionner à la Sécurité de l'Information

Programmes en cours d'emploi



Sommaire

| | |
|--|----|
| Contexte de la formation..... | 3 |
| Objectifs de notre formation..... | 3 |
| Spécificités de chaque type de diplôme | 4 |
| Durée des formations en sécurité de l'information et passerelles possibles | 6 |
| Public visé | 6 |
| Méthodes pédagogiques | 7 |
| Une formation académique interdisciplinaire..... | 7 |
| Responsables de la formation continue en sécurité de l'information, HEC Genève | 7 |
| Intervenants (<i>sous réserve d'éventuelles modifications</i>)..... | 8 |
| Modules proposés | 9 |
| Planning des modules 2013-2014..... | 10 |
| Descriptif de chaque module..... | 11 |
| Évaluation des connaissances | 13 |
| Charge de travail..... | 13 |
| Conditions d'obtention et titres délivrés..... | 13 |
| Conditions d'admission | 14 |
| Renseignements pratiques | 16 |
| Horaire / Organisation..... | 17 |
| Contacts et informations | 17 |
| Bulletin d'inscription – Formation Continue Universitaire | 18 |

IT = Information Technologies, SI = Système(s) d'information, SSI = Spécialisation en Sécurité de l'Information, CAS-InfoSec = Certificate of Advanced Studies in Information Security, DAS-InfoSec = Diploma of Advanced Studies in Information Security, MAS-InfoSec = Master of Advanced Studies in Information Security. Les autres acronymes font référence à des normes ou standards connus.

Si le masculin est utilisé à des fins de simplification de la rédaction, les textes s'appliquent aussi bien aux hommes qu'aux femmes.

Contexte de la formation

Aujourd'hui, le métier de responsable de la sécurité de l'information est en pleine mutation. Au-delà d'une maîtrise technique généraliste, le responsable de la sécurité de l'information doit être également un communicateur, un stratège, un auditeur, un formateur, un manager, un coordinateur, etc. Les compétences multi disciplinaires exigées pour cette personne orchestre sont un véritable défi pour une formation pertinente. Pour répondre aux nouveaux besoins sécuritaires des entreprises, plusieurs formations diplômantes destinées aux professionnels de la sécurité ont été créées.

Objectifs de notre formation

Les évolutions actuelles exigent de nouvelles compétences de la part des professionnels en charge de la sécurité physique, la sécurité de l'information et des systèmes d'information en conformité avec le cadre légal et les règles d'entreprise. Ils se doivent d'être en mesure d'identifier les risques nouveaux, de planifier et d'assurer le suivi de la mise en place des mesures de prévention, de détection et de correction adéquates pour y faire face, et surtout de sensibiliser les collaborateurs de manière à ce que chacun puisse acquérir les bons réflexes. Diverses fonctions dans le domaine de la sécurité de l'information conduisent à des positions hiérarchiques différentes selon la nature des ressources à protéger. La fonction la plus couramment répandue est celle de RSSI (Responsable de la Sécurité des Systèmes d'Information) en charge de la mise en œuvre de la politique organisationnelle de sécurité de l'information dans les entreprises et administrations. Dans les pays anglo-saxons, la dénomination est "*Information Systems Security Officer*", *Chief Information Security Officer (CISO)* ou encore *Chief Security Officer (CSO)*.

Compétences

Pour assurer cette mission, ces spécialistes doivent se former à la culture multidimensionnelle du champ de la **sécurité de l'information et de la gestion du risque** :

- **dimension managériale** : évaluer et gérer des risques de l'information, mettre en place d'indicateurs et métriques, retour sur investissements, organisation de la sécurité, plan de continuité d'activités, méthodologie d'audit, etc.
- **dimension organisationnelle et humaine** : plan d'assurance qualité et référentiels qualité, management de projets, sensibilisation et motivation du personnel, plans de secours informatique, etc.
- **dimension technologique** : nouvelles applications de l'informatique, refonte des systèmes d'information, sécurité des réseaux et des communications internet, architectures de sécurité, etc.
- **dimension juridique** : mise en conformité avec les réglementations (de type IFRS, Sarbanes-Oxley ou Bâle II par exemple), avec les lois actuelles (protection des données, propriété intellectuelle, etc.) et les conventions internationales.
- **Dimension stratégique et de gouvernance** : intégration de la sécurité de l'information au cœur de la Direction d'entreprise. Maîtrise de la communication, y compris en cas de crise.

Des formations modulaires diplômantes et en cours d'emploi

Nos programmes de formation continue permettent d'aller au-delà de la seule sécurité informatique pour englober tous les processus liés à la protection de l'information et d'acquérir non seulement les compétences fondamentales, mais également une expertise complète dans le domaine de la sécurité de l'information.

A cette fin, quatre formations modulaires ont été créées permettant d'obtenir les diplômes suivants :

- Le **CAS-InfoSec** : Certificat de formation continue en Sécurité de l'Information / *Certificate of Advanced Studies in Information Security*
- Le **DAS-InfoSec** : Diplôme de formation continue en Sécurité de l'Information / *Diploma of Advanced Studies in Information Security*
- Le **MAS-InfoSec** : Master de formation continue en Sécurité de l'Information / *Master of Advanced Studies in Information Security*
- Le **MBA** : *Master of Business Administration* avec spécialisation en Sécurité de l'Information

Chaque programme permet aux professionnels de maîtriser les fondamentaux du domaine et les nouvelles tendances en matière de sécurité de l'information. Selon son projet de formation et ses besoins professionnels, l'étudiant s'inscrit dans un programme spécifique et obtient le titre de CAS/DAS/MAS ou MBA de l'Université de Genève.

L'accès aux fondamentaux pour les étudiants relativement novices se fait au niveau du CAS1-InfoSec, protection de l'information : technologies et services. Ils peuvent éventuellement poursuivre avec les modules du DAS-InfoSec, voire du MAS-InfoSec dans la foulée, sous réserve de l'acceptation de leur dossier par le comité scientifique. Pour les conditions d'accès au MBA avec spécialisation en sécurité de l'information, voir page 15.

Spécificités de chaque type de diplôme

Le Certificat de formation continue en Sécurité de l'Information (CAS-InfoSec)

Les fondamentaux : l'objectif est de former l'étudiant aux concepts fondamentaux de la sécurité de l'information. Il s'agit de comprendre le mode opératoire d'une analyse des risques, les mécanismes permettant d'assurer la continuité des activités et de gérer une crise majeure. Les aspects techniques de la sécurité des réseaux informatiques sont étudiés pour mettre en place une sécurité adéquate. Enfin, les nouvelles tendances technologiques avec leurs solutions sécuritaires sont également abordées en tant que processus de veille. Les 5 modules du CAS-InfoSec représentent 15 crédits ECTS¹ et 120 heures de cours. En cas de réussite, ils peuvent être crédités, dans le cadre du DAS-InfoSec.

Le Diplôme de formation continue en Sécurité de l'Information (DAS-InfoSec)

L'approfondissement : l'objectif est d'apporter de nouvelles compétences sur des aspects organisationnels de l'entreprise liées à la gouvernance de la sécurité de l'information et aux processus métiers. En particulier, un module juridique est consacré à la protection des données et à la propriété intellectuelle et un autre module permet de travailler sur des cas d'audit de sécurité. Enfin, pour compléter la formation intramuros à Uni Mail, les étudiants s'inscrivent à des séminaires en sécurité proposés sur le bassin Romand pour s'ouvrir aux préoccupations actuelles dans ce domaine. Les 9 modules du DAS-InfoSec représentent 240 heures de cours (30 crédits ECTS). En cas de réussite, ils peuvent être crédités, dans le cadre du MAS-InfoSec.

Le Master of Advanced Studies en Sécurité de l'Information (MAS-InfoSec)

L'élargissement : l'objectif de cette formation a pour vocation de former des experts où tous les domaines de la sécurité de l'information sont abordés, y compris ceux qui traitent de sujets de pointe. Pour développer ces compétences, un module est consacré aux clauses contractuelles, un autre traite plus particulièrement de la cybercriminalité et un autre encore des aspects liés à l'intelligence économique. Le module « Savoir communiquer » est également proposé afin de permettre une meilleure compréhension des projets avec les responsables métiers de l'entreprise.

¹ European Credit Transfer and accumulation System

Les 15 modules du MAS-InfoSec y compris le travail de mémoire de diplôme représentent 60 crédits ECTS et se déroulent sur deux années.

Le MBA avec spécialisation en Sécurité de l'Information

Le fait d'obtenir le diplôme DAS-InfoSec peut aider à intégrer le programme MBA d'HEC-Genève. La première année du MBA comprend 13 modules. L'une des spécialisations de la 2^e année du MBA (mention « Sécurité de l'information ») inclut les modules traités au DAS-InfoSec / MAS-InfoSec. Davantage de précisions sont apportées en page 15. Le programme MBA représente 90 crédits ECTS sur deux années.

Ces différentes spécialisations nous permettent de proposer trois types de parcours :

A) Un parcours dans une logique de continuité d'apprentissage

La session 2013/2014 est organisée de manière à pouvoir suivre les divers modules dans l'ordre chronologique prévu pour permettre l'obtention d'un CAS puis éventuellement un DAS et MAS ou MBA de l'Université de Genève. Dans ce cas, chaque programme plus spécialisé est en continuité avec le précédent.

B) Un parcours par thème

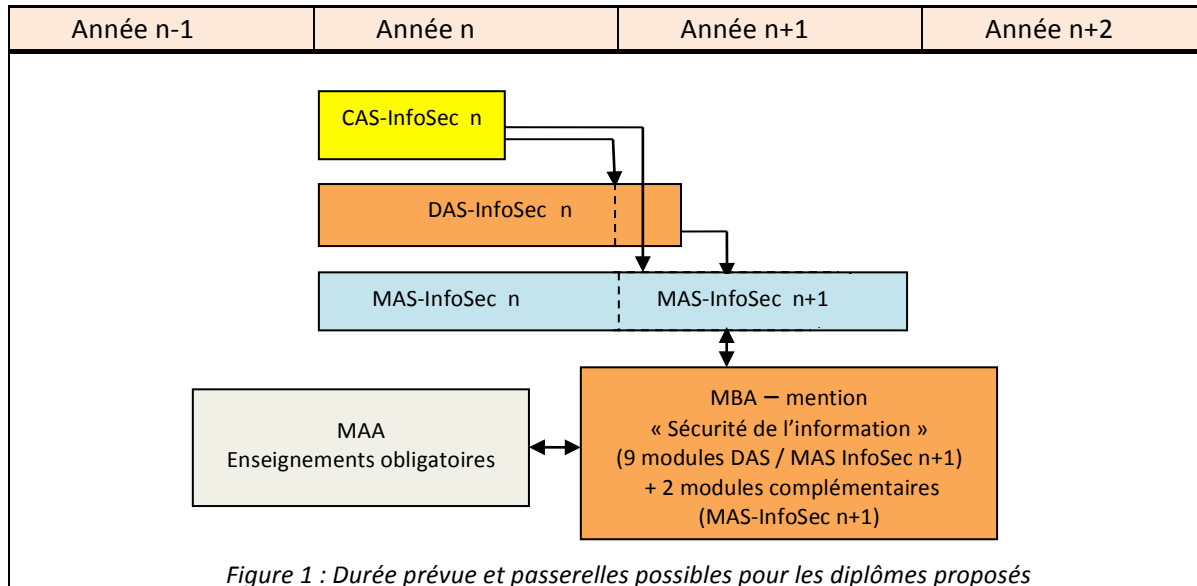
Selon le parcours professionnel du futur candidat, il est possible que certains futurs participants préfèrent intégrer les modules « Gouvernance de la sécurité de l'information en entreprise » de manière à compléter leurs acquis initiaux par une approche plus managériale. D'autres déjà très spécialisés recherchent des cours uniquement liés à la « sécurité de l'information dans sa globalité », pour acquérir des sujets pointus ou nouveaux. Chaque thème spécifique peut valider un CAS-InfoSec. Une combinaison de deux CAS-InfoSec permet l'obtention d'un DAS-InfoSec. Enfin, le jeu des combinaisons CAS-InfoSec ou DAS-InfoSec ouvre vers l'obtention du MAS-InfoSec.

C) Un parcours à la carte et personnalisé

Les modules de la formation InfoSec peuvent être suivis « à la carte » et de manière indépendante pendant la session 2013/2014 sans obtenir de diplôme. Si un nombre de crédits ECTS peuvent être acquis par une combinaison de plusieurs modules, il sera alors possible d'obtenir un CAS-InfoSec ou DAS-InfoSec « personnalisé ». Cependant, cette possibilité devra être validée par le comité InfoSec en tenant compte de l'expérience du candidat et d'éventuels modules en pré-requis.

Durée des formations en sécurité de l'information et passerelles possibles

Le schéma ci-dessous représente la durée théorique qui doit être consacrée par un étudiant pour valider l'un des diplômes suivi (CAS-InfoSec, DAS-InfoSec, MAS-InfoSec et MBA). Un diplôme peut également servir de passerelle (représentation par une flèche) pour accéder à un programme plus ambitieux en validant les crédits acquis. Les formations plus pointues s'appuient sur les modules dispensés dans les formations de base. En conséquence, des modules sont communs à l'ensemble des formations.



Chaque module se compose de 24 heures d'enseignement chacun, y compris le contrôle des connaissances et équivaut à 3 crédits ECTS à l'exception du module « Séminaires en sécurité de l'information » qui correspond à 6 ECTS. Le mémoire de diplôme du MAS-InfoSec représente 15 crédits ECTS.

- La durée des études pour le **Certificat** est d'1 semestre (15 crédits ECTS).
- La durée des études pour le **Diplôme** est de 2 semestres (30 crédits ECTS).
- La durée des études pour le **MAS** est de 4 semestres (60 crédits ECTS).
- La durée des études pour le **MBA en emploi** est de 4 semestres (90 crédits ECTS).

Sous réserve de places disponibles, les personnes ne souhaitant pas suivre l'intégralité d'une formation peuvent s'inscrire à un ou plusieurs modules isolés. Il est possible de déposer une demande d'admission ultérieurement dans un des programmes proposés.

Public visé

Ces formations s'adressent tout particulièrement aux différents responsables œuvrant dans le domaine de la sécurité de l'information :

- Responsables de la sécurité de l'entreprise et/ou de la gestion des risques
- Responsables de la sécurité de l'information et du Risk Management
- Responsables des systèmes d'information
- Responsables sécurité des réseaux et systèmes
- Responsables des politiques de protection des ressources liées aux systèmes d'information et de communication
- Chefs de projets d'informatisation, de projets en e-commerce et e-business
- Conseillers à la protection des données des entreprises ou administrations
- Consultants en informatique, en sécurité, en Risk Management
- Responsables chargés de l'évaluation des risques opérationnels
- Auditeurs des systèmes d'information
- Juristes d'entreprises chargés de sécurité et de conformité de l'information

Méthodes pédagogiques

Le programme est animé par des universitaires et des professionnels, tous spécialistes des domaines relatifs à la sécurité de l'information et des systèmes d'information. La diversité des compétences des enseignants et intervenants 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 participants d'une volée et des volées précédentes.

L'enseignement donné de manière didactique fait appel à des études de cas, à des exercices pratiques ainsi qu'à l'étude de sites web dédiés à la sécurité de l'information.

Le lieu central d'échange entre les enseignants et les participants est le site web du programme qui leur est réservé.

Une formation académique interdisciplinaire

Ce programme est organisé par l'Université de Genève en collaboration étroite avec les milieux économiques, des associations professionnelles et d'autres institutions universitaires.

Le programme est soutenu par la conférence universitaire de Suisse occidentale (CUSO).

En partenariat avec notre programme de formation, diverses associations (CLUSIS, ISACA, GRIFES, FGS, FMQ, etc.) organisent de nombreux séminaires en Suisse Romande qui permettent de compléter la formation de nos étudiants.

Responsables de la formation continue en sécurité de l'information, HEC Genève

Direction et coordination

Directeur : Dimitri KONSTANTAS, Professeur ordinaire, Université de Genève

Co-directeur, Jean-Luc PILLET, Adjoint Scientifique, Université de Genève

Comité Scientifique

- Jean BLOCH, Directeur Aud-IT, Genève
- Éric CHOFFAT, Global Information Security & Risk Control Lead, JT International
- Jean-Paul DE BLASIS, Professeur honoraire, Université de Genève, Faculté des S.E.S / HEC
- Nadji HAMED-BEY, Responsable du Système d'Information et Sécurité, Caisse Cantonale Genevoise de Chômage
- Eugène HORBER, Professeur Sciences Sociales, Université de Genève-SES/SOCOC
- Jeremy KENAGHAN, Responsable Sécurité des Systèmes d'Information, CHUV, Lausanne
- Dimitri KONSTANTAS, Professeur et Vice-doyen, Université de Genève – SES
- Michel MARTI, DCTI – CTI Sécurité et événements spéciaux, État de Genève
- Claude MAURY, Consultant indépendant, ancien président du CLUSIS
- Jean MENTHONNEX, Professeur, Université de Franche-Comté et Directeur Euroqual, Lausanne
- Jean-Henry MORIN, Professeur associé, Université de Genève, Faculté des S.E.S / HEC
- Gérald PAGE, Avocat, Brown & Page Avocats, Genève
- Jean-Luc PILLET, Adjoint Scientifique, Université de Genève
- Victor POLIC, IT Security Officer, International Labour Organization (ILO), Genève
- Jean-Roland SCHULER, Professeur HES, École d'ingénieurs et d'architectes de Fribourg
- Jean-Pierre THERRE, CSO, Pictet & Cie Banquiers, Genève
- Mauro VIGNATI, Senior Advisor, MELANI, Berne
- Lilia VOGT, CISO, OMS

Intervenants (sous réserve d'éventuelles modifications)

Christophe BARMAN, CEO Unirisc Group ; **Jean BLOCH (Lead Auditor)**, Directeur Aud-IT, Genève ; **Claudine BURTON-JEANGROS (PHD)**, Professeure, Département de Sociologie, Université de Genève ; **Charles-Henri CARLIN**, Consultant, ELCA Informatique SA, Lausanne ; **Éric CHOFFAT (MBA, CSSI, CISA, CISM, CISSP)**, Global Information Security & Risk Control Lead, JT International ; **Alessandro COLARUSSO (CISA)**, Responsable Audit informatique, Lombard Odier Darier Hentsch & Cie, Genève ; **Frédéric DOMMART**, Risk Manager, Banque Cantonale Vaudoise, Lausanne ; **Arnaud DUCROT (SEQI, MBA)**, Chef Département Conseil & Ingénierie, Protectas S.A., Genève ; **Dimitri KONSTANTAS (PHD)**, Professeur, Vice-Doyen Faculté SES / HEC Genève ; **Jean-Charles LAMONATO**, Chief Security Officer, Hôpitaux Universitaires de Genève ; **Dirk LANGER**, Avocat, Brown&Page, Genève ; **James-Louis LINDER (SEQI, CISSP)**, Responsable sécurité, Banque Cantonale Vaudoise, Lausanne ; **Olivier LUXEREAU**, Consultant, NetExpert, Gland ; **Sylvain MARET**, Expert Sécurité – Founder MARET Consulting ; **Michel MARTI**, DCTI-CTI, Sécurité, État de Genève ; **Claude MAURY (Lead Auditor)**, Ancien Président du CLUSIS, Consultant ; **Jean MENTHONNEX (PHD)**, Professeur, Université de Besançon et Directeur du Centre EUROQUAL, Lausanne ; **Jean-François MILHOMME (CSSI, MBA)**, Solution Architect, Sun Microsystems, Gland ; **Philippe OECHSLIN (PHD, CISSP)**, Senior Researcher, LASEC/EPFL et conseil en sécurité informatique, Lausanne ; **Gérald PAGE**, Avocat, Etude Brown&Page, Genève ; **Jean-Luc PILLET (PHD, DSSI)**, Adjoint Scientifique, Faculté SES, HEC Genève ; **David ROYSTON**, Directeur, Royston Consulting, Genève ; **Jean-Marc SOLLEDER (CSSI)**, Security Engineer, SCRT, Prévèrenge ; **Lambert SONNA MOMO (PHD)**, IT Consultant ; **Paul SUCH**, Directeur, SCRT, Prévèrenge ; **Jean-Pierre THERRE (MBA)**, Chief Security Officer, Pictet & Cie Banquiers, Genève ; **Mauro VIGNATI**, Analyst MELANI/Cybercrime, Berne ; **François-Xavier VINCENT**, Gouvernance de la sécurité de l'information, Groupe AXA, France.

Modules proposés

La formation continue en Sécurité de l'Information est constituée par les modules suivants avec 3 options possibles :

A) Le parcours dans la continuité d'apprentissage

Cette formule impose la participation du participant **dans l'ordre des modules**. La validation d'un diplôme permettra une inscription à une formation plus pointue. Par exemple, la réussite au DAS-InfoSec permet l'inscription dans la continuité au MAS-InfoSec.

| N° des modules | Intitulé des modules | Modules «continuité» requis pour le : CAS / DAS / MAS | Crédits ECTS |
|----------------|--|--|--------------|
| 11 | Fondements de la sécurité de l'information | | 3 |
| 12 | Gestion des risques de l'information | | 3 |
| 13 | Continuité des activités, gestion de crise et sécurité physique | | 3 |
| | Systeme d'exploitation, composants réseaux et protocoles internet ² | | |
| 14 | Bonnes pratiques des dispositifs de sécurité logique | | 3 |
| 15 | Veille technologique en sécurité de l'information | | 3 |
| 21 | Gouvernance de la sécurité et processus métiers | | 3 |
| 22 | Aspects juridiques de la sécurité de l'information | | 3 |
| 23 | Audit des systèmes d'information | | 3 |
| 24 | Séminaires sur la sécurité de l'information | | 6 |
| 31 | Intelligence économique | | 3 |
| 32 | Clauses contractuelles en sécurité de l'information | | 3 |
| 33 | Savoir communiquer dans les organisations, y compris en cas de crise | | 3 |
| 34 | Cybercriminalité et recherche de preuves | | 3 |
| 35 | Développement et mise en œuvre de la politique de sécurité de l'information | | 3 |
| 40 | Mémoire MAS-InfoSec ou MBA | | 15 |

Tableau 1 : Appartenance des divers modules au type de diplôme (CAS-InfoSec, DAS-InfoSec, MAS-InfoSec, MBA)

B) Le parcours par thème

Le tableau 1 en page 9 précise les possibilités d'inscription par thème en tenant compte de l'indice du N° de module. Ainsi le thème 1 « **Protection de l'information : technologies et services** » comprend 5 modules référencés de 11 à 15 (CAS1-InfoSec). Le thème 2 « **Gouvernance de la sécurité de l'information dans les entreprises** » comprend 4 modules référencés de 21 à 24 (CAS2-InfoSec).

² Module optionnel sans crédits ECTS permettant de compléter les fondamentaux dans le domaine de la sécurité des réseaux informatiques. Ce module aura lieu à la Haute École d'Ingénieurs et d'Architectes de Fribourg et fera l'objet d'une facturation séparée. Les personnes intéressées sont priées de nous faire connaître de leur intention d'une inscription éventuelle.

Enfin, le thème 3 « **Gestion de la sécurité dans un contexte global** » est constitué par les modules 31 à 35 (CAS3-InfoSec). Chaque thème correspond donc à un CAS-InfoSec spécifique. En conséquence, par combinaison de 2 à 2, le participant peut valider 3 DAS-InfoSec distincts : DAS1 (CAS1+CAS2) ; DAS2 (CAS1+CAS3) ; DAS3 (CAS2+CAS3). Enfin, le cumul des 3 CAS-InfoSec plus la validation du mémoire (N° 40) permet de valider le MAS-InfoSec.

C) Le parcours à la carte et personnalisé

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 l'étudiant valide 15 crédits ECTS, il obtient un CAS personnalisé sans thème. S'il valide 30 crédits ECTS, il obtient un DAS personnalisé sans thème. Les modalités pratiques et divers détails concernant cette inscription personnalisée devront être approuvées par le comité scientifique InfoSec. Le planning des modules est le suivant :

| N° module | Modules | Durée (*) | Début du module | Fin du module | Type de diplôme | ECTS |
|-------------------------------|---|-----------|-----------------|---------------|-----------------|------|
| 11 | Fondements de la sécurité de l'information | 24h | 09.01.13 | 13.02.13 | CAS-InfoSec | 3 |
| 12 | Gestion des risques de l'information | 24h | 13.02.13 | 20.03.13 | CAS-InfoSec | 3 |
| 13 | Continuité des activités, gestion de crise et sécurité physique | 24h | 20.03.13 | 24.04.13 | CAS-InfoSec | 3 |
| Module en option ³ | Système d'exploitation, composants réseaux et protocoles internet | 24h | 14.02.13 | 21.03.13 | - | - |
| 14 ⁴ | Bonnes pratiques des dispositifs de sécurité logique | 24h | 24.04.13 | 29.05.13 | CAS-InfoSec | 3 |
| 15 | Veille et tendances technologiques en sécurité de l'information | 24h | 29.05.13 | 03.07.13 | CAS-InfoSec | 3 |
| 10 ⁵ | Mémoire complémentaire CAS-InfoSec | | | | | 3 |
| | Vacances d'été | | | | | |
| 21 | Gouvernance de la sécurité et processus métiers | 24h | 04.09.13 | 09.10.13 | DAS-InfoSec | 3 |
| 22 | Aspects juridiques de la sécurité de l'information | 24h | 09.10.13 | 13.11.13 | DAS-InfoSec | 3 |
| 23 | Audit des systèmes d'information | 24h | 13.11.13 | 18.12.13 | DAS-InfoSec | 3 |
| 24 | Séminaires sur la sécurité de l'information | | | | DAS-InfoSec | 6 |
| | Vacances de fin année | | | | | |
| 31 | Intelligence économique | 24h | 08.01.14 | 12.02.14 | MAS-InfoSec | 3 |
| 32 | Étude des clauses contractuelles en sécurité de l'information | 24h | 12.02.14 | 19.03.14 | MAS-InfoSec | 3 |
| 33 | Savoir communiquer dans les organisations, y comprise en cas de crise | 24h | 19.03.14 | 23.04.14 | MAS-InfoSec | 3 |
| 34 | Cybercriminalité et recherche de preuves | 24h | 23.04.14 | 28.05.14 | MAS-InfoSec | 3 |
| 35 | Développement et mise en œuvre d'une politique de sécurité de l'information | 24h | 28.05.14 | 02.07.14 | MAS-InfoSec | 3 |
| 40 | Mémoire MAS-Sec Info ou MBA | | | | MAS-InfoSec | 15 |

Tableau 2 : calendrier prévu des CAS-InfoSec / DAS-InfoSec / MAS-InfoSec 2013 / 2014

(*) Chaque module est équivalent à 24 heures d'enseignement en salle de cours

³ Module optionnel sans crédits ECTS permettant de compléter les fondamentaux dans le domaine de la sécurité des réseaux informatiques. Ce module aura lieu à la Haute École d'Ingénieurs et d'Architectes de Fribourg et fera l'objet d'une facturation séparée.

⁴ Ce module aura lieu également à la Haute École d'Ingénieurs et d'Architectes de Fribourg

⁵ Ce mémoire est une option pour une inscription à un CAS personnalisé qui ne comporte que 4 modules d'enseignement.

Descriptif de chaque module⁶

Module 11 - Fondements de la sécurité de l'information

La notion d'information. La qualité dans l'organisation de la sécurité des informations. L'intégration de la sécurité lors d'une gestion de projet dans un contexte systèmes d'information. Le management de la sécurité et les liens métiers. Les relations de confiance, la connaissance sécuritaire des individus et leur comportement. La politique de sécurité en entreprise.

Module 12 : Gestion des risques de l'information

Présentation des standards, normes et méthodes utilisés 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'*Enterprise wide Risk Management* supporté par un standard global (ISO 31000, COSO II).

Module 13 - Continuité des activités, gestion de crise et sécurité physique

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

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.

Module 15 - Veille et tendances technologiques en sécurité de l'information

Des experts viendront exposer quelques nouvelles tendances des TIC (p. ex. mobilité, VoIP, nouvelles applications Internet, biométrie, ...) qui ont ou devraient avoir à terme un impact significatif en sécurité de l'information. En fin de module, les étudiants échangeront leurs idées et expériences en exposant par groupe les risques et opportunités que ces nouvelles tendances pourraient concrètement induire dans leurs organisations respectives, et les éventuelles parades possibles.

Module 21 - Gouvernance de la sécurité et processus métiers

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 22 - Aspects juridiques de la sécurité de l'information

La protection des données. Les dangers liés à la propriété intellectuelle. La signature électronique. Les différents types de responsabilité pour la diffusion sur le net. La surveillance au travail.

⁶ Sous réserve d'éventuelles modifications

Module 23 - Audit des systèmes d'information

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

Obligation pour les étudiants 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 31 - Intelligence économique

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 oeuvre 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. Etude de quelques cas pratiques.

Module 32 - Étude des clauses contractuelles en sécurité de l'information

Comment gérer des contrats internes. Les relations avec les SLA. Les clauses contractuelles avec les partenaires commerciaux. Le concept du FM, ses avantages et ses dangers. Les contrats spécifiques au Cloud Computing. La sécurité liée à la gestion des ressources RH internes ou tiers (engagement, transfert, départ; clauses de confidentialité). La RH en tant que source d'insécurité mais aussi d'amélioration.

Module 33 - Savoir communiquer en entreprise, y compris en cas de crise

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 oeuvre. La stratégie avec les médias.

Module 34 - Cybercriminalité et recherche de preuves

Analyse de la criminalité et TIC. Traces numériques et investigations, Sciences forensiques (en partenariat avec l'Institut de police scientifique de l'Université de Lausanne).

Module 35 - Développement et mise en oeuvre d'une politique de sécurité de l'information

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'affaire, 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 oeuvre vs bénéfices en termes de réduction des risques. La mesure de performance des P&P. « 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.

Note : Ce module est un module de synthèse utilisant la plupart des notions acquises dans les précédent modules (Risques, Conformité, Audit, Bonnes Pratiques, etc.). Il est basé sur une étude de cas.

Module 40 - Mémoire MAS-InfoSec

Ce travail doit permettre de démontrer que le candidat est apte à gérer un projet professionnel et à analyser puis résoudre des problèmes concrets dans le domaine choisi. Un superviseur ou directeur de mémoire contrôlera le choix du sujet, la planification du projet, la collecte des données, les actions à effectuer et les recommandations qui en découlent.

Évaluation des connaissances

Chaque module est validé par un contrôle des connaissances comportant, en principe, l'évaluation d'un travail individuel ou d'un travail en groupe et d'un examen final formel. Le module 24 est validé par la remise de synthèses et d'analyses critiques des séminaires suivis. Le module 40 est validé lorsque le mémoire de diplôme remis par l'étudiant est conforme aux exigences d'un mémoire MAS.

Charge de travail

Pour chaque heure d'enseignement, il faut compter de deux à trois heures de travail personnel sous forme de lectures pour la préparation des séances, de rédaction des travaux d'évaluation, individuels ou en groupe, ainsi que le temps consacré à la révision de l'examen final de chaque module.

D'après l'enquête réalisée auprès des étudiants des volées précédentes, il ressort qu'en moyenne, ils ont consacré environ 12 heures par semaine à leur formation.

Conditions d'obtention et titres délivrés

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

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

Toute absence doit être justifiée. Une moyenne générale de 4.0/6.0 est exigée pour réussir le programme. Concernant les diplômes CAS / DAS, les notes entre 3.0 et 3.75 à un module seulement peuvent être compensées pour autant que la moyenne générale soit au moins égale à 4.0. Une note inférieure à 3.0 ne donne pas droit aux crédits et nécessite la répétition du module l'année suivante. Dans le cas spécifique du MAS, chaque module doit être réussi avec une note supérieure ou égale à 4.00.

L'Université de Genève délivre les titres suivants aux étudiants 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).
Cette formation s'adresse à des candidats ayant déjà une certaine expérience professionnelle dans au moins un des domaines de la sécurité de l'information et qui souhaitent acquérir les fondamentaux conceptuels et pratiques. Les compétences développées dans le programme s'apparentent à une fonction de RSSI (IS Security Officer).
- **Le Diplôme de formation continue en Sécurité de l'Information (*Diploma of Advanced Studies in Information Security*)** (30 crédits ECTS).
Le public visé concerne les détenteurs d'un CAS-InfoSec qui souhaitent approfondir leurs connaissances en vue de prendre des responsabilités dans le domaine de la sécurité de l'information. Les compétences développées dans le programme s'apparentent à une fonction de CISO (Chief Information Security Officer).
- **Le Master of Advanced Studies en Sécurité de l'Information (*Master of Advanced Studies in Information Security*)** (60 crédits).
Concerne les détenteurs d'un DAS-InfoSec qui veulent élargir leurs connaissances à des compétences de management de la sécurité au sens large pour gérer les diverses équipes responsables de la sécurité de l'entreprise. Les compétences développées dans le programme s'apparentent à une fonction de CSO (Chief Security Officer)

- **Le MBA avec spécialisation en sécurité de l'information (90 crédits ECTS).**
Peut concerner les détenteurs d'un MAS-InfoSec et les diplômés de l'enseignement supérieur visant à obtenir un titre reconnu mondialement assorti d'une spécialisation en sécurité de l'information. Les compétences développées dans le programme s'apparentent à une fonction d'encadrement de haut niveau, CIO, CSO, etc.

Les participants inscrits à un ou plusieurs modules isolés recevront une attestation de réussite s'ils satisfont aux conditions d'attribution des crédits ECTS correspondants.

Conditions d'admission

Certificat CAS-InfoSec/ Diplôme DAS-InfoSec

1. Peuvent être admis(es) comme candidat(e)s au Certificat / Diplôme de formation continue les personnes qui :
 - a. titulaires d'une maîtrise universitaire de l'Université de Genève, d'un Master d'une Haute Ecole Spécialisée ou d'un titre jugé équivalent ;
ou titulaires d'un baccalauréat universitaire de l'Université de Genève, d'un bachelor d'une Haute Ecole Spécialisée ou d'un titre jugé équivalent ;

et

 - b. peuvent faire état d'une expérience professionnelle d'au moins 3 ans dans le domaine concerné.
2. Le Conseil scientifique se réserve le droit d'accepter la candidature de personnes ne répondant pas aux exigences stipulées sous 1. après examen de leur dossier.
3. Les personnes qui suivent la session en cours (CAS-InfoSec) et qui ont déjà validés leurs modules peuvent s'inscrire directement au DAS-InfoSec de la même session.
4. Sont également admises les personnes qui s'inscrivent au DAS-InfoSec et qui sont déjà détentrices d'un CAS-InfoSec d'une volée plus ancienne (ou anciennement CSSI). Le Conseil scientifique accordera une éventuelle validation d'un ou plusieurs modules au cas par cas lors de l'examen du dossier.

Master of Advanced Studies (MAS-InfoSec)

Peuvent être admises comme candidates au MAS, les personnes qui sont :

- a. titulaires d'une maîtrise universitaire de l'Université de Genève, d'un Master d'une Haute Ecole Spécialisée ou d'un titre jugé équivalent ou
- b. titulaires d'un baccalauréat universitaire de l'Université de Genève, d'un bachelor d'une Haute Ecole Spécialisée ou d'un titre jugé équivalent et peuvent faire état d'une expérience professionnelle d'au moins 3 ans dans le domaine concerné.

Les personnes qui suivent la session en cours (CAS-InfoSec ou DAS-InfoSec) et qui ont déjà validés leurs modules peuvent s'inscrire directement au MAS-InfoSec de la même session.

Sont également admises sous réserve de l'acceptation du Conseil scientifique, les personnes qui s'inscrivent au MAS-InfoSec et qui sont déjà détentrices d'un CAS-InfoSec / DAS-InfoSec d'une volée précédente (ou anciennement CSSI ou DSSI). Le Conseil scientifique accordera une éventuelle validation d'un ou plusieurs modules au cas par cas lors de l'examen du dossier.

MBA en emploi

Les conditions d'admission au MBA sont les suivantes :

- Être titulaire d'un diplôme universitaire (Maîtrise universitaire, licence, Bachelor universitaire ou Master ou Bachelors HES ou titre jugé équivalent)
- Avoir réussi le Diplôme MAA
- Justifier d'une expérience professionnelle pertinente de trois années au minimum
- Posséder une excellente maîtrise parlée et écrite du français comme de l'anglais
- Avoir la pratique des logiciels bureautiques de base
- GMAT ou autres bases en gestion et informatique

Deux options sont possibles pour intégrer le MBA en emploi de l'Université de Genève.

1^{ère} option : MBA mention « sécurité de l'information »

Pour les candidats déjà titulaires d'un diplôme universitaire (master, licence, bachelor ou titre jugé équivalent) et bénéficiant de 3 ans d'expérience professionnelle dans le domaine de la formation, il est judicieux de postuler d'abord à l'admission au programme du **Master en Business Administration (MBA)** de HEC-Genève. La 1^{ère} année de formation au management général doit, en principe, être acquise en premier, Cela permettra aux étudiants d'obtenir le diplôme en **Management et Administration des Affaires (MAA)**. Puis ils s'inscriront au programme du **DAS-InfoSec en tant que spécialisation du MBA**. Le travail de mémoire du MBA se fera dans le domaine de la sécurité de l'information. Le MBA comporte 90 crédits ECTS, dont 60 crédits pour la partie MAA et 30 crédits pour la partie DAS-InfoSec.

2^e option : postuler pour le DAS-InfoSec (1^{ère} année) puis au MAA (2^e année)

Les candidats ayant entrepris une démarche de validation des acquis de l'expérience (VAE) dans le cadre du programme de licence en gestion d'entreprise HEC-Université de Savoie peuvent postuler pour un diplôme DAS-InfoSec, Si les conditions d'admission au MBA sont remplies l'année suivante, le candidat conservera le bénéfice des modules validés du DAS-InfoSec. Il lui suffira alors de suivre en 2^e année les modules du MAA. Une fois tous les modules validés, le candidat pourra obtenir le titre de MBA mention « sécurité de l'information ».

Pour toute information complémentaire, prière de s'adresser directement au :

Programme MBA

HEC – Université de Genève

Uni Mail – 40, bd du Pont-d'Arve – 1211 Genève 4

Tél. : + 41 (22) 379 88 09

e-mail : mba-hec@unige.ch

<http://mba.unige.ch>



Conditions d'admission

L'admission des candidats est prononcée par le conseil scientifique sur examen d'un dossier constitué du bulletin d'inscription, auquel doivent être annexés :

- 1) un curriculum vitae complet (formulaire à télécharger sur <http://infosec.unige.ch>)
- 2) une lettre de motivation
- 3) une lettre de recommandation, si possible
- 4) 1 photo passeport
- 5) une photocopie de la carte d'identité et des diplômes

Aucune candidature ne sera recevable après le début des cours, sauf dans le cas d'une inscription à un module isolé.

Connaissances préalables requises

Les candidats doivent être familiarisés 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

- 1) **Option continuité** : la candidature d'inscription doit parvenir **avant le 30 novembre 2012**,
- 2) **Option à thèmes** : la candidature d'inscription doit parvenir **1 mois** avant le début du premier module choisi par le candidat
- 3) **Option modules individuels et personnalisés** : la candidature d'inscription doit parvenir **1 mois** avant le début du module choisi par le candidat

Les candidatures d'inscription doivent être adressées au : Dr. Jean-Luc Pillet, Formation en Sécurité de l'Information, HEC-Genève, Université de Genève, Bd du Pont-d'Arve 40, 1211 Genève 4

Remarque : les demandes arrivées après ce délai seront prises en compte en fonction des places disponibles.

Frais de participation⁷

CAS-InfoSec

- CHF 7'000.- 5 modules (15 ECTS)

DAS-InfoSec

- CHF 10'000.- 9 modules (30 ECTS)

MAS-InfoSec

- CHF 15'000.- 15 modules (60 ECTS).

MBA, 2^{ème} année de spécialisation en sécurité de l'information

- **Contactez directement les coordinateurs du programme MBA :**
Tél. : + 41 (22) 379 88 09 ; e-mail : mba-hec@unige.ch ; <http://mba.unige.ch>

Les étudiants qui suivent actuellement l'une de nos formations peuvent prétendre à s'inscrire dans la foulée à une formation plus pointue. Les frais d'inscription facturés correspondent uniquement aux modules supplémentaires à suivre (CHF 1'000.- CH par module).

Pour les étudiants qui sont détenteurs d'une formation InfoSec antérieure, les frais d'admission tiendront compte du nombre de modules à suivre suite à la décision du Conseil Scientifique.

L'admission à un ou plusieurs modules isolés est subordonnée au nombre de places disponibles. Le coût est de **CHF 1'700.-** par module sauf pour le module optionnel dont le coût est de **CHF 1'200.-**

⁷ Les tarifs indiqués correspondent à la session 2013/2014

L'État de Genève encourageant la formation professionnelle des adultes, un chèque annuel de CHF 750.- peut être demandé avant le début des cours par les étudiants répondant aux critères d'attribution. Informations disponibles sur : <http://www.geneve.ch/bourses>

Horaire / Organisation

Les modules des diplômes CAS-InfoSec / DAS-InfoSec et MAS-InfoSec sont agencés un soir de semaine de 17h15 à 21h00 (sauf Module 24 et 40). La plupart des séances d'examen clôturant chaque module auront lieu de 14h15 à 17h00 avant le début du module suivant. Un planning horaire annuel précis sera disponible prochainement sur le site de la formation InfoSec (<http://infosec.unige.ch>) et sera également remis en début de programme.

Lieu des cours

Université de Genève, Uni-Mail, Bd du Pont-d'Arve 40, 1211 Genève 4, sauf pour le module à option qui aura lieu à la Haute École d'Ingénieurs et d'Architectes de Fribourg.

Principes de validation des candidatures et règles d'annulation

Après délibération du conseil scientifique, les candidats sont informés par courrier de l'acceptation ou non de leur dossier. Les candidats retenus doivent avoir réglé la finance d'inscription à la date indiquée sur le courrier pour valider leur inscription sinon elle est annulée de fait. Tout renoncement dans les 30 jours suivants, mais avant le début des cours, entraîne la perception d'une retenue de CHF 500.- pour frais administratifs. Tout renoncement après le début des cours donne lieu au remboursement de 50 % du montant au prorata des modules non intégralement suivis. Les demandes de report ou d'annulation doivent être formulées par écrit.

Contacts et informations

Le Dr. Jean-Luc Pillet, coordinateur des formations en Sécurité de l'Information, se tient volontiers à disposition pour tout renseignement complémentaire sur le contenu du programme :

tél. + **41 (22) 379 81 35** fax : + **41 (22) 379 81 04** email : jean-luc.pillet@unige.ch

Vous pouvez trouver également des informations sur notre site : <http://infosec.unige.ch>

Pour toute autre question, contacter :

Secrétariat formation continue, HEC-Genève
UNI MAIL
Bd du Pont-d'Arve 40
CH-1211 Genève 4

Tél. : + 41 (22) 379 88 00
Fax + 41 (22) 379 81 04
Email : infosec-hec@unige.ch
<http://www.hec-executive.ch>

Renseignements généraux

Je souhaite participer au :

- | | |
|--|---|
| <input type="checkbox"/> CAS1-InfoSec (protection de l'information) | <input type="checkbox"/> DAS1-InfoSec (CAS1InfoSec + CAS2-InfoSec) |
| <input type="checkbox"/> CAS2-InfoSec (gouvernance de la sécurité de l'information) | <input type="checkbox"/> DAS2-InfoSec (CAS1-InfoSec + CAS3-InfoSec) |
| <input type="checkbox"/> CAS3-InfoSec (gestion de la sécurité dans sa globalité) | <input type="checkbox"/> DAS3-InfoSec (CAS2-InfoSec + CAS3-InfoSec) |
| <input type="checkbox"/> MAS-InfoSec | |
| <input type="checkbox"/> 2 ^{ème} année MBA, spécialisation en Sécurité de l'Information | |

1^{ère} Option - parcours continuité : Bulletin d'inscription et dossier complet à renvoyer **avant le 30 novembre 2012** à :
PILLET Jean-Luc, Université de Genève, SES-HEC, Bd du Pont-d'Arve 40, CH-1211 Genève 4
Fax: + 41 (0)22 379 81 04, email : jean-luc.pillet@unige.ch

2^{ème} option – parcours à thèmes : bulletin d'inscription et dossier complet **dans un délai d'un mois avant la participation à un premier module de la formation.**

3^{ème} option – parcours individualisé : bulletin d'inscription et dossier complet **dans un délai d'un mois avant la participation à un premier module de la formation.**

S.V.P. à remplir en lettres majuscules et cases à cocher

Madame Monsieur

Nom: Prénom:

Date de naissance (jour/mois/année): Age : Nationalité:

Coordonnées professionnelles

Entreprise/Institution:

Adresse:

NP/Ville/Pays:

Téléphone: Fax:

E-mail:

Coordonnées privées

Adresse:

NP/Ville/Pays:

Téléphone: Fax:

E-mail:

Adresse pour l'envoi postal: (cocher une seule case)

privée professionnelle

Adresse de facturation: (cocher une seule case)

privée professionnelle autre (indiquer) :

Avez-vous déjà été immatriculé dans une haute école suisse: oui/non Numéro matricule suisse:

Si vous n'êtes pas en mesure d'indiquer votre numéro matricule, veuillez indiquer le nom de la dernière haute école que vous avez fréquentée en Suisse. Cette information nous permettra de retrouver votre numéro matricule:

Niveau fin d'études

- Certificat de capacité (CFC)
- Maturité professionnelle
- Maturité générale / Baccalauréat (secondaire)
- Bachelor/Master des Hautes Ecoles Spécialisées / Hautes Ecoles Pédagogiques
- Bachelor/Master/Doctorat des Universités, Ecoles polytechniques Fédérales
- Autre :

Intitulé du diplôme (plus haut titre obtenu) :

Autre(s) expérience(s) de formation continue au cours des 2 dernières années :

(Merci de considérer tous types de formation, y compris séminaires, colloques, conférences, débats, etc.)

Aucune autre expérience de formation continue

Nombre de formations d'une journée ou moins (≤ 8 heures) :

Nombre de formations de plus d'une journée (> 8 heures) :

Nombre de formations diplômantes (Certificat/Diplôme/Master of Advanced Studies, etc.) :

Activité professionnelle

Exercez-vous actuellement une activité professionnelle ?

- Oui à 100%
 Oui à temps partiel => Taux d'occupation :%
 Non => car vous êtes : En recherche d'emploi En congé formation A la retraite
 Autre, précisez :

Note : Si vous n'exercez actuellement pas d'activité professionnelle, merci d'indiquer ci-dessous les réponses correspondant à la dernière activité professionnelle que vous avez occupée.

Profession :

Fonction (titre du poste):

Position hiérarchique

- Indépendant Cadre supérieur Cadre intermédiaire Employé

Secteur d'activité:

- Activité indépendante ONG
 Administration publique ou para-publique Organisation européenne
 Association Organisation Internationale
 Entreprise privée

Taille de l'entreprise:

- moins de 10 personnes de 11 à 50 personnes de 51 à 100 personnes
 de 101 à 500 personnes de 501 à 1000 personnes plus de 1000 personnes

Inscription

1^{ère} et 2^{ème} option : je souhaite participer au parcours « continuité ou à thèmes »

- CAS-InfoSec et m'engage à verser la somme de **CHF 7'000.-** dès réception de la confirmation de mon inscription.
 DAS-InfoSec et m'engage à verser la somme de **CHF 10'000.-** dès réception de la confirmation de mon inscription.
 MAS-infoSec et m'engage à verser la somme de **CHF 15'000.-** dès réception de la confirmation de mon inscription.
 2^{ème} année MBA, spécialisation en Sécurité de l'Information et m'engage à verser la somme de **CHF 10'000.-** dès réception de la confirmation de mon inscription.

3^{ème} option et 4^{ème} option : je souhaite m'inscrire au(x) module(s) isolé(s) suivant(s) ou à un ensemble de modules au parcours personnalisé

- Module 11 Module 12 Module 13 Module 14 Module 15
 Module 21 Module 22 Module 23 Module 31 Module 32
 Module 33 Module 34 Module 35

et m'engage à verser la somme de **CHF 1'700.-** par module dès réception de la confirmation de mon inscription.

Les participants inscrits au CAS-InfoSec, DAS-InfoSec, MAS-InfoSec et 2^{ème} année de spécialisation MBA sont prioritaires en cas de places limitées.

SVP joindre les pièces suivantes :

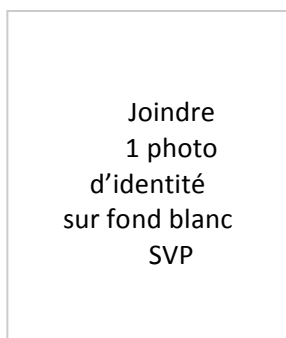
- 1 CV détaillé + copies des diplômes 1 photo ID 1 lettre de recommandation, si possible
 1 copie d'une pièce d'identité 1 lettre de motivation

Conditions d'annulation (CAS-InfoSec, DAS-InfoSec, MAS-InfoSec, 2^{ème} année spécialisation MBA -Sécurité de l'Information)

J'ai connaissance que, si ma candidature est acceptée, mon inscription doit être confirmée par le versement des frais de participation. Si me désiste avant le début des cours, je m'engage à régler CHF 500.- pour frais administratifs. Si je renonce après, je ne serais remboursé que de 50% des modules que je n'aurais pas suivis entièrement.

Lieu et date : Signature:

Fiche complémentaire d'informations



Comment avez-vous eu connaissance de cette formation ? (plusieurs réponses possibles)

- Recommandations personnelles
- Mon entreprise
- Un professionnel de la formation/orientation
- Une annonce dans un journal => si oui, lequel :
- Une brochure / prospectus / affiche / catalogue des offres de formation continue de l'Université de Genève
- Le site internet de la formation continue de l'Université de Genève www.unige.ch/formcont
- Un autre site => si oui, lequel : www.....
- Renseignement directement auprès de l'Université de Genève
- Un e-mail annonçant la formation
- Lors d'une Foire, d'un Salon (ex : Salon RH, Eduqua) => si oui, lequel :
- Autre:.....

Vos atouts et motivations

Langue maternelle :

Autres langues maîtrisées :

Vos principaux points forts :

Vos principaux points faibles :

Si vous avez un diplôme de 2nd cycle universitaire, envisagez-vous de vous inscrire d'abord au MBA ?

oui

non