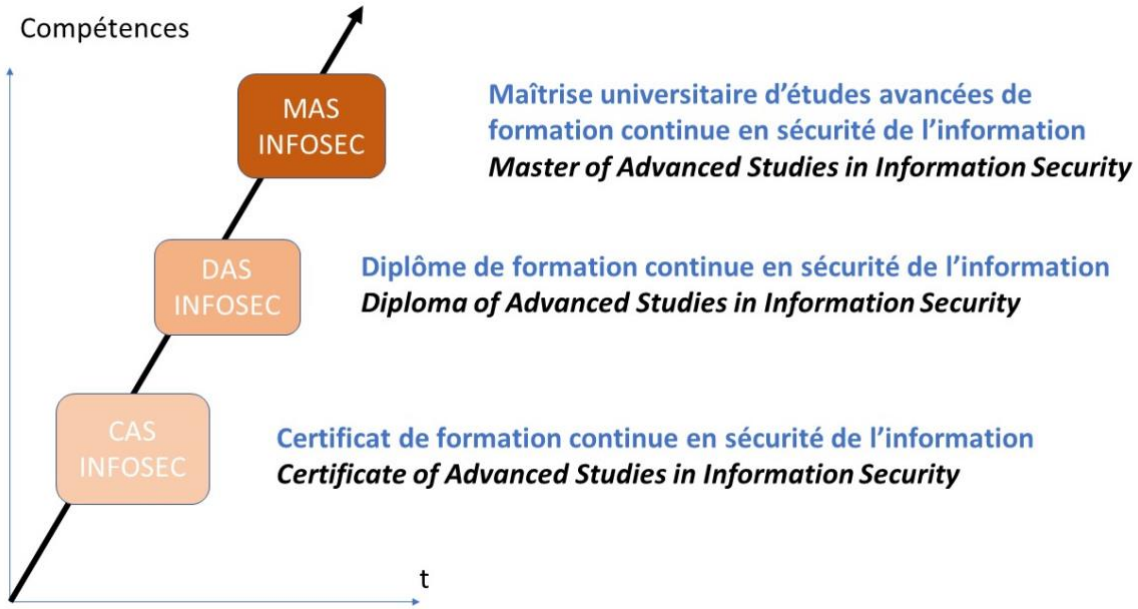
Se former et se perfectionner à la

Sécurité de l'Information

Programmes en cours d'emploi



UNIVERSITÉ DE GENÈVE

Sommaire

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, la personne en charge de la sécurité de l'information doit être également compétente en matière de communication, des stratégies, d'audit, de pédagogie, de management et de coordination, 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 et aux professionnelles de la sécurité ont été créées.

Objectifs de notre formation

Les évolutions actuelles exigent de nouvelles compétences en regard avec les expertes et experts 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. Elles et 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*

Chaque programme permet aux professionnelles et 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, la personne s'inscrit dans un programme spécifique et obtient le titre de CAS/DAS/MAS de l'Université de Genève.

L'accès aux fondamentaux pour les personnes relativement novices se fait au niveau du CAS1-InfoSec, protection de l'information : technologies et services. Elles 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.

Spécificités de chaque type de diplôme

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

Les fondamentaux : l'objectif est de se former 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 ECTS 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 10 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. Les 16 modules du MAS-InfoSec y compris le travail de mémoire de diplôme représentent 60 crédits ECTS et se déroulent 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 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 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 suivi « à la carte » et de manière indépendante pendant la session 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 pour valider l'un des diplômes suivi (CAS-InfoSec, DAS-InfoSec, MAS-InfoSec). 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.

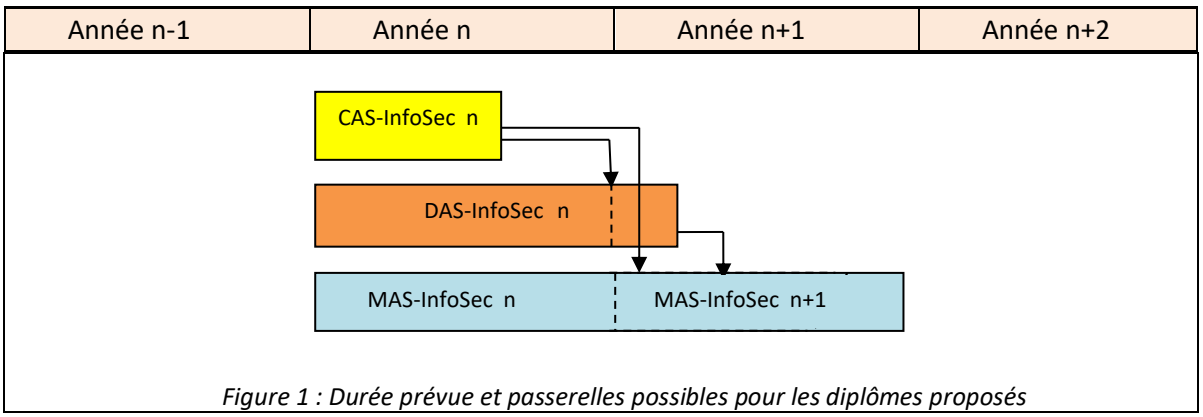


Figure 1 : Durée prévue et passerelles possibles pour les diplômes proposés

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 mémoire de diplôme du MAS-InfoSec qui représente 15 crédits ECTS[1].

- La durée des études pour le **Certificat** est d'1 semestre (15 crédits ECTS).
- La durée des études pour le **Diplôm**e est de 2 semestres (30 crédits ECTS).
- La durée des études pour le **MAS** est de 4 semestres (60 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
- Responsables 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

Elles s'adressent aussi aux professionnelles et professionnels dans des fonctions qui peuvent être impactées par la sécurité de l'information, par exemple : chercheur, médecin, responsable RH, juriste gérant des données à caractère confidentiel.

Méthodes pédagogiques

Le programme est animé par des universitaires et des professionnelles et professionnels, toutes et tous spécialistes des domaines relatifs à la sécurité de l'information et des systèmes d'information. La diversité des compétences des enseignantes et enseignants 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 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.

[1] 1 crédit ECTS = 25-30 heures volume travail étudiant (enseignement + travail personnel)

Intervenants *(sous réserve d'éventuelles modifications)*

Lien avec le site : http://infosec.unige.ch/

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

(sous réserves d'éventuelles modifications)

Lien avec le site : http://infosec.unige.ch/

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
	Système 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	Les aspects sécuritaires liés à la digitalisation de la société		3
22	Gouvernance de la sécurité et processus métiers		3
23	Audit des systèmes d'information		3
24	Séminaires sur la sécurité de l'information		3
25	Protection des données appliquées		3
31	Intelligence économique		3
32	Le Big Data, intelligence artificielle et Cloud : comment gérer la sécurité		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		15

Tableau 1 : Appartenance des divers modules au type de diplôme (CAS-InfoSec, DAS-InfoSec, MAS-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 dune 'inscription éventuelle.

B) Le parcours par thème

Le tableau 1 en page 8 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 5 modules référencés de 21 à 25 (CAS2-InfoSec). 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

Voir les informations en ligne sur le site : http://infosec.unige.ch

Descriptif de chaque module[3]

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'*Entreprise 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 règlementaire, 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.

[3] Sous réserve d'éventuelles modifications

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.

Ce module optionnel d'une journée se déroule dans les locaux de la Haute Ecole d'Ingénieurs et d'Architectes de Fribourg (HEIA).
Incriptions directement auprès de la HEIA : jean-roland.schuler@hefr.ch

Module 14 - Bonnes pratiques des dispositifs de sécurité logique

Défense périmètrique. 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.
Pré-requis : connaissances réseau. Le module optionnel peut aider à cette préparation.

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

Des expertes et 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 étudiantes et 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.
Pré-requis : module 14

Module 21 - Les aspects sécuritaires liés à la digitalisation de la société

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 de cette évolution digitale mais également d'en étudier les aspects règlementaires et contractuels.

Module 22 - 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 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 25 – La protection des données appliquées

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

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 règlementaire, 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. Etude de quelques cas pratiques.

Module 32 - Le Big Data, intelligence artificielle et Cloud : comment gérer la sécurité

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 - 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 œuvre. 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).
Pré-requis : modules 11, 12, 14, 15, 31

Module 35 - Développement et mise en œuvre 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 œuvre 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.

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.
Pré-requis : modules 11, 12, 23, 32

Module 40 - Mémoire MAS-InfoSec

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 appliquées (standard et normes en sécurité de l'information), analyse effectuée au sein de l'entreprise, 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.

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 personnes 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 titulaires 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 titulaires 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)

Les personnes inscrites 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

Peuvent être admises comme candidat(e)s au Certificat / Diplôme de formation continue les personnes qui sont :

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

peuvent faire état d'une expérience professionnelle d'au moins 3 ans dans le domaine concerné.

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.

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.

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 :

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

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.

Renseignements pratiques

Conditions d'admission

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

1) un curriculum vitæ 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 familiarisé(e)s 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. Les pré-requis par module sont présentés dans les descriptifs de chacun des modules ci-dessus.

Délai d'inscription :

1) **Option continuité** : la candidature d'inscription doit parvenir **avant le 30 octobre de l'année en cours**,
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, Centre universitaire d'informatique (CUI), Battelle - Bâtiment A, Route de Drize 7, CH 1227 Carouge, Genève

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

Frais de participation

CAS-InfoSec

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

DAS-InfoSec

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

MAS-InfoSec

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

Les personnes qui suivent actuellement l'une des formations InfoSec 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.- par module).

Pour les personnes qui sont détentrices d'une formation InfoSec antérieure, les frais d'admission tiennent 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. Le module optionnel est géré directement par la Haute Ecole d'Ingénieurs et d'Architectes de Fribourg.

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 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 conditions 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 confirmer leur inscription.

Les demandes de report ou d'annulation doivent être formulées par écrit.

En cas de non paiement des frais d'inscription, tout renoncement avant le début des cours entraîne la perception d'une retenue de CHF 1000.- 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.

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*** email : ***jean-luc.pillet@unige.ch***

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

Bulletin d'inscription

A télécharger depuis le site http://infosec.unige.ch.