Association suisse de la sécurité de l'information
Clusis
Rapport annuel d'activité et de gestion
à l'assemblée générale
14 avril 2015

L'association suisse de la sécurité de l'information, Clusis

L'association suisse de la sécurité de l'information - Clusis - consolide son image de lieu d'échange à l'intention des personnes qui ont déjà suivi une des nombreuses formations actuelles proposées à l'EPFL, dans les Universités ou dans les HES ainsi qu'à celles qui bénéficient d'une expérience acquise dans les organisations.

Le Clusis enrichit la formation continue par des événements de haute qualité: Journée stratégique, conférences, ateliers et témoignages qui aident à la consolidation des concepts théoriques et méthodologiques et facilitent leur mise en œuvre dans les organisations. L'expérience transmise par la présentation de cas réels, enrichis par des exposés de l'état de l'art est encore augmentée par l'échange avec les participants qui ont, eux aussi, une grande expérience.

Par ses activités, ses membres et leurs compétences réunies, le Clusis se positionne comme l'organisme suisse de référence en matière de sécurité de l'information, de cybersécurité et de toute activité dans ce domaine.

Le Clusis, association suisse de la sécurité de l'information consolide sa position privilégiée d'échanges d'expériences et de compétences au bénéfice des membres de l'association.

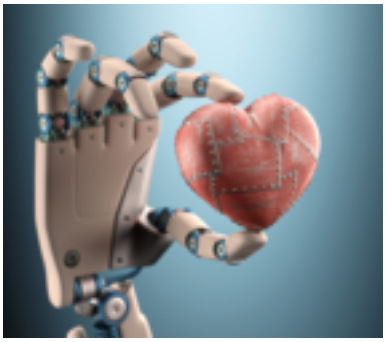
Tout au long de l'exercice, le comité a développé ses activités dans le but de réaliser un programme en réponse aux attentes et en prévision des besoins futurs de tous les membres de l'association.

L'association suisse de la sécurité de l'information

En 2015 à ce jour, 8 sponsors, 112 organisations, 109 personnes font partie du Clusis. Au total 229 personnes ou organisations.

Les sources de financements sont les cotisations entreprises, individuelles et les sponsors. Les charges de fonctionnement sont resserrées afin de disposer des meilleures conditions à la production des événements.

La haute qualité des événements et leur promotion renforcent l'image du Clusis et le leadership du comité, composé de personnes compétentes dans les différents domaines de la cybersécurité



Du droit des robots à la cybersécurité des systèmes de contrôle

Lausanne, 14 avril 2015,
72 participants

La robotique figure au nombre des technologies clés à l'horizon 2020 et l'essor des projets techniques rend incontournable la problématique du cadre juridique applicable. La question du droit et de la cybersécurité sont déterminants de l'acceptabilité de cette technologie.
L'activité robotique peut-elle s'autoréguler elle-même ou faut-il créer un cadre juridique spécifique ?

Faut-il un droit des robots ? Conférence de Me Alain Bensoussan, avocat technologue, Cabinet Bensoussan, président et fondateur de l'Association du Droit des Robots (ADDR)
Le développement des marchés de la robotique, de l'internet des objets et de la virtualisation conduit à l'émergence d'une nouvelle spécialité : le Droit des Robots.
Sur le plan technique la robotique est au croisement de plusieurs secteurs d'activités : mécatronique, électronique, optronique, logiciel embarqué, énergie, nanomatériaux, intelligence artificielle, connectique.
Si le droit des objets tel qu'il existe actuellement encadre les robots ménager de type grille-pain, il est totalement inadapté aux nouvelles générations de robots nés et à naître.
Les robots nouvelle génération dont il est question, sont des machines dotées d'une intelligence artificielle capable de prendre une décision dans un environnement mobile avec une interactivité avec l'homme. Le droit des biens est à moderniser, celui des personnes sans doute aussi. C'est la technologie qui va révolutionner le droit et tous les droits nationaux vont devoir s'adapter. Ils ne sont plus de simples objets, ne sont certes pas assimilables à un animal et encore moins à un être humain, mais les robots nouvelle génération vont désormais avoir des responsabilités du fait de leur capacité d'interaction avec leur environnement. A l'instar de ce qui existe pour les personnes morales, il convient de créer une personnalité-robot… Tel est le thème sur lequel interviendra Me
Le développement des marchés de la robotique, de l'internet des objets et de la virtualisation conduit à l'émergence d'une nouvelle spécialité : le Droit des Robots. Sur le plan technique la robotique est au croisement de plusieurs secteurs d'activités : mécatronique, électronique, optronique, lo- giciel embarqué, énergie, nanomatériaux, intelligence artificielle, connectique.
Si le droit des objets tel qu'il existe actuellement encadre les ro- bots ménager de type grille-pain, il est totalement inadapté aux nouvelles générations de robots nés et à naître. Les robots nouvelle génération dont il est question, sont des machines dotées d'une intelligence artificielle capable de prendre une décision dans un environnement mobile avec une interacti- vité avec l'homme. Le droit des biens est à moderniser, celui des personnes sans doute aussi. C'est la technologie qui va révolu- tionner le droit et tous les droits nationaux vont devoir s'adapter. Ils ne sont plus de simples objets, ne sont certes pas assimilables à un animal et encore moins à un être humain, mais les robots nouvelle génération vont désormais avoir des responsabilités du fait de leur capacité d'interaction avec leur environnement. A l'ins- tar de ce qui existe pour les personnes morales, il convient de créer une personnalité-robot...
Tel est le thème sur lequel interviendra Me Alain Bensoussan.

Faut-il certifier la cybersécurité des systèmes d'automatismes et de contrôle industriel (IACS en anglais, SCADA par exemple) ? Conférence de Monsieur Paul Théron, PhD, FBCI, ThalesCommunications & Security's Cyberdefence Bids Manager and Expert on cyber-resilience.
La DG Joint Research Centre (JRC) de la Commission Européenne a lancé un projet d'étude relatif au besoin de « certifier » la cybersécurité des systèmes d'automatismes et de contrôle industriel (IACS en anglais), voici déjà 5 ans. Après une première phase qui a permis de voir toute la difficulté du sujet, un deuxième groupe de travail, que M. Paul Théron a dirigé, a été créé par la DG JRC.
Ce groupe a confirmé tout d'abord le besoin d'intégrer des composants cyber-sûrs dans les systèmes industriels aujourd'hui encore très peu, voire pas du tout sécurisés. M. Théron présentera donc tout d'abord le sens de cette idée directrice et son cadre normatif et sécuritaire.
Ensuite, au terme de diverses consultations et réunions, le groupe a précisé la notion de certification, ses divers niveaux envisageables et ses modalités possibles. Le conférencier présentera donc ces éléments qui ne constituent aujourd'hui que des points de repère pour des travaux encore à venir.

Enfin, le groupe a élaboré une proposition de plan d'action et de recherche pour 2015-2020. Paul Théron présentera donc, en montrant notamment le besoin de s'y impliquer pour les industriels et les fournisseurs de solutions d'automatisme et de contrôle industriels (tel ABB par exemple, Schneider, Siemens, etc.).
Au-delà, Paul illustrera les concepts de cyber-naïveté, de cyber-crise, et de cyber-résilience.

Automatisation ou autonomisation ? Conférence de Me Pascal Verniory, avocat, docteur en philosophie (option transdisciplinarité), juriste Etat-Major de la Direction générale des systèmes d'information de l'Etat de Genève.
La complexité semble le propre de notre époque où les développements des technologies de l'information et de la communi- cation nous ont propulsé de l'ordinateur individuel à l'internet et nous annoncent des robots «autonomes» au point de bousculer ce que nous croyons savoir sur les fondements de la responsabilité, qu'elle soit éthique ou juridique.
Cela nous interroge sur les conditions des choix que nous faisons et leurs conséquences. L'imprévisibilité, conséquence de la complexité, est-elle comparable à la surprenance propre aux êtres libres? Sommes-nous dépassés par notre techno-science, comme nous l'affirmait Günter Anders? Cette complexité peut-elle au contraire nous faire découvrir qui nous sommes? Comment la phénoménologie peut-elle nous aider dans cette réflexion?

Clusis Campus, Uni-Mail 23 janvier 2015
250 participants
Comité d'organisation: Brian Henningsen, Président du comité d'organisation, Jacqueline Reigner, dr ès sciences, Présidente du Clusis, Sémafor Conseil Enrico Viganò, Vice-président du Clusis, Etat de Genève, Christophe Actis, Palo Alto, Lara Broi, Université de Genève, Nadia Dali, Etat de Genève, Sabah Detienne, Sunrise, Raoul Diez, FER, Isabelle Dubois, AD HOC RESOLUTION, Moscha Kardaras, Etat de Genève, Stefan Lueders, CERN, Prof. Giovanna Di Marzo Serugendo, Université de Genève, Joelle Mathey, Comité Clusis, Jean-Luc Pillet, Université de Genève, Mathieu Schaeffler. Etat de Genève, Pierre Toquard. BAM4S, Nicolas Vernaz, Addax Petroleum Ltd

La Journée Stratégique 2015 est une occasion unique de mise au point des connaissances en cybersécurité. Sur la lancée du succès de la JS2014: Veille stratégique et Intelligence économique de la JS 2013: Communication dans la gestion de crise informatique et de la JS 2012: Cybersécurité dans 5 ans, la prochaine JS2015 sera Clusis Campus. Un événement de haute tenue focalisé sur les thématiques majeures de la cybersécurité actuelle Il se tiendra le 23 janvier 2015 de 8h30 à 17h30 dans les locaux d'Uni Mail à Genève. Clusis Campus développera tout au long de la journée les six domaines suivants animés par des mises en situation, des ateliers, des présentations et des démonstrations qui privilégieront la participation de toutes les personnes présentes selon la recette qui a fait le succès des journées stratégiques du Clusis.
Le programme de la JS2015 est consacré à 6 thèmes d'actualité en cybersécurité traités en parallèle avec de nombreux ateliers:

PROGRAMME

Café accueil 8h30-9h Espace 6 Sous-sol							
Introduction 9h00-9h20	Madame Sylvie Perrinjaquet						
	Internet des Objets IOT Giovanna Di Marzo Serugendo Pierre Toquard	**Big Data** Jean-Luc Pillet	**BYOD** Sabah Detienne Nadia Dali Isabelle Dubois Raoul Diez	**Open Source** Brian Henningsen Christophe Actis	**Secure web** Enrico Viganò Nicolas Vernaz	**Hackers corner** Stefan Lüders Jacqueline Reigner Joëlle Mathey Mathieu Schaeffler	**Transparence** Isabelle Dubois Jean-Henry Morin
	S030	S040	S050	O150	O160	O170	Espace 6
Atelier 1 9h30-10h15	Nouveau challenge pour votre sécurité et vie privée Xavier Maumon Antonino Mannisi	Contrôle des données Stéphane Droxler	BYOD, une alternative ouverte à EMM Isabelle Dubois Henri Severac	Les différentes fonctionnalités de wireshark Jean-Roland Schuler	Attaques site webs et WAF Cédric Dutoit	Démystifier l'accès par intrusion Dominique Climenti	
Pause café 10h15-10h45 Espace 6 Sous-sol							La Transparence pour et par VOUS Isabelle Dubois Jean-Henry Morin
Atelier 2 10h45-11h25	Analyse du firmware d'une voiture - Paul Such Capteurs sur Internet Pierre Toquard	La protection de données le mobile crowd sensing Dr Laura Georg	Le bilan financier Toni Lassezens,	Suricata: Détection des intrusions avec une déclinaison de Snort. Julien Bachmann	Web Application Vulnerabilities Workshop Sebastian Lopienski	DDOS attack prevention: solutions, techniques and technologies. Alain Reiser Michal Nowakowski Julien Fiches	La Transparence pour et par VOUS Isabelle Dubois Jean-Henry Morin
Atelier 3 11h30-12h15	Réseau basse consommation à couverture globale pour l'internet des objets Didier Hélal	Measures proposed to meet healthcare costs out to 2020 Dr John Gunson	La mise en oeuvre pragmatique Stéphane Zwettler	La gestion et l'analyse des APT avec Cuckoo Sandbox Alain Sutam	Web Application Vulnerabilities Workshop Sebastian Lopienski	DDOS attack prevention: solutions, techniques and technologies. Alain Reiser Michal Nowakowski Julien Fiches	La Transparence pour et par VOUS Isabelle Dubois Jean-Henry Morin
Buffet-repas 12h15-14h00 Espace 5 Rez							
Atelier 4 14h00-14h45	Evolution of Mobile Threats Dirk Kolberg	Risques liés aux interfaces des devices médicaux Dr Paolo Masci	Approche théorique et pratique Yvan Monteagudo Diego Carrillo	Analyse dynamiques de sites web avec ZAP Proxi Nicolas Oberli	Etude hacking et remédiation Thierry Silly	Comment les pirates accèdent à nos informations: exemple avec un fait d'actualité Dominique Vidal	La Transparence pour et par VOUS Isabelle Dubois Jean-Henry Morin
Pause-goûter 14h45-15h15 Espace 6 Sous-sol							
Atelier 5 15h15-16h00	MyAccessWeb dans le domaine du sport Jean-Pierre Garnier Robots sur Internet Prof. Giovanna Di Marzo	Cloud services for Big Data management and analytics Dr Verena Kantere	Protéger l'information en mobilité Arnaud Simon	Tails, The Amnesic Incognito Live System Alain Hugentobler	Implémentation SSL/TLS, encore robuste en 2014? Emmanuel Bailleul	Windigo: Coulisses d'une opération malveillante en constante évolution Vincent Brillault	
Événement final 16h00-16h30	Patrick Ghion, chef de la brigade de criminalité informatique, Genève Prof. Nicolas Tavaglione						
Apéritif 16h30-17h30 Espace 6 Sous-sol							

Ouverture par Mme Sylvie Perrinjaquet, conseillère nationale

Internet des objets / IOT

- Xavier Maumon, Antonino Mannisi, Kondor SA: Nouveau challenge pour votre sécurité et votre vie privée
- Paul Such, SCRT: Analyse du firmware d'une voiture
- Pierre Toquard, BAM4S: Capteurs sur Internet, Indicateurs d'activités, des signaux faibles, risques et corrélations.
- Didier Helal, Orbiwise: Réseau basse consommation à couverture globale pour l'internet des objets
- Gilles Peter, Kaspersky
- Jean-Pierre Garnier: GSInformatique SA: Le Cloud interactif MyAccessWeb dans le domaine du sport
- Prof. Giovanna Di Marzo Serugendo, UniGE: Capteurs et Robots sur Internet, ateliers interactifs

Big data

- Laura Georg, experte de la Commission Européenne: La protection de données dans le mobile crowd sensing
- Stéphane Droxler, Uditis: Atelier Big Data: Contrôle des données
- John Gunson, Webster University: Measures proposed to meet healthcare costs out to 2020. Case studies: Obamacare (USA), NHS (UK), Swiss Health2020 (CH)
- Paolo Masci, Queen Mary University of London: Risques liés aux interfaces des devices médicaux
- Verena Kantere, Université de Genève: Cloud services for Big Data management and analytics

BYOD Bring your own device

- Isabelle Dubois, AD HOC RESOLUTION et Henri Severac, Stradefi SA: Le BYOD, une alternative ouverte à EMM (Enterprise Mobility Management)
- Toni Lazazzera, Tmanco SA: Le bilan financier du BYOD
- Stephane Zwettler, SZ Informatique: La mise en œuvre pragmatique du BYOD
- Yvan Monteagudo Diego Carrillo, Thinko Sàrl : Approche théorique et pratique sur les solutions BYOD
- Arnaud Simon, CheckPoint Europe SE: Protéger l'information en mobilité

Open source

- Jean-Roland Schuler, HES-SO Fribourg: Capturer des trames sur différents types de réseaux (Ethernet, PPP, loopback, …), avec Wireshark
- Julien Bachmann, Kudelski Security: Suricata, une autre approche IDS / IPS, et de Network Security Monitoring engine.
- Alain Sullam, Lenz & Stahëlin: la gestion et l'analyse de nouveaux malwares avec Cuckoo Sandbox.
- Nicolas Oberli, Audemars Piguet: W3AF est un framework dédié à l'analyse de sites Web dynamiques comportant de nombreux modules dédiés aux vulnérabilités les plus communes.
- Alain Hugentobler, Université de Genève: Tails protège votre vie privée avec l'anonymisation de vos connections internet, et des traces laissées sur les ordinateurs.

Secure web

- Cédric Dutoit, Ingénieur en Sécurité eb-Qual SA – Démonstration d'attaques de sites Web et leur déploiement contre un grand nombre de cibles, et des différentes techniques utilisées aujourd'hui par les WAF (Web Application Firewall) pour combattre ce type d'attaques
  .
- Sebastian Lopienski, Deputy Computer Security Officer at CERN - Workshop "Web application vulnerabilities" - In this workshop, participants will be asked to find vulnerabilities in a provided web application, and exploit them. The online documentation will gradually reveal more and more information to help participants in this task. Participants will be able to see their progress, and compete against others teams.
- Thierry Silly, Check Point Suisse: Etude d'un exemple de Hacking et protectionà confirmer: Atelier firewall
- Emmanuel Bailleul, Lanexpert, Implémentation SSL/TLS, encore robuste en 2014?

Hacker corner

- Alain Reiser, Julien Fiches et Michal Nowakowski, Sunrise Communications AG: DDOS attacks prevention: solution, techniques et technologies
- Dominique Climenti, Kyos: Démystifier l'accès par intrusion
- Dominique Vidal, Seculabs: Démystifier le vol d'informations précieuses
- Vincent Brillault, CERN: Windigo: coulisses d'une opération malveillante en constante évolution.

La transparence pour vous et par vous, Isabelle Dubois et Jean-Henri Morin: L'accès à l'information des institutions fédérales et cantonales, publiques et parapubliques, est un droit et une responsabilité citoyenne. Venez l'expérimenter et participer collaborativement à la démocratie.

Patrick Ghion, chef de la brigade de criminalité informatique, Genève

Prof. Nicolas Tavaglione, UniGe: conclusion philosophique et table-ronde.

DATA PROTECTION OFFICER:
de l'indépendance légale à l'indépendance d'action
28 octobre 2014, Geneve. *107 participants*
Comité d'organisation: Isabelle Dubois, AD HOC RESOLUTION, Jacqueline Reigner, Présidente du Clusis, Sömafor Conseil, Enrico Viganò, Vice-président du Clusis, Etat de Genève

Des préposés cantonaux au Data Protection Officer prévu par le futur Règlement européen, en passant par les conseillers en protection des données et les correspondants informatiques et liberté, tous doivent être – de par la réglementation – indépendants. Pourquoi? que cela implique-t-il, et surtout comment garantir cette indépendance?
Le CLUSIS vous invite à participer à la réflexion au détour de témoignages et d'échanges interactifs mettant en évidence les enjeux de la protection des données.
PROGRAMME
Ouverture par Isabelle Dubois. Qu'est-ce qu'un DPO? présentation des grandes lignes et du programme.
- Présentation par Hélène Legras, correspondant informatique et liberté du groupe Areva, de son poste et des enjeux liés à l'indépendance. Elle est CIL auprès de la CNIL, juriste dans les nouvelles technologies, membre de la direction juridiques d'Areva. Elle délivre consultations, conseils, formations internes et externes sur les aspects «informatique et libertés». Membre de l'Association Française des Juristes d'Entreprise et Administrateur de l'Association Française des Correspondants aux Données Personnelles.
- Le cas du Valais par Ursula Sury, avocate, spécialisée dans le domaine du droit de l'informatique et de la protection des données. Elle gère son cabinet d'avocat et enseigne à la Hochschule Luzern (Haute Ecole Spécialisée de Lucerne). Ursula Sury a travaillé pendant 4 ans en tant que préposée à la protection de données et à la transparence du Canton du Valais.
- Le cas genevois par Isabelle Dubois, expert en protection des données, co-fondatrice de Ad Hoc Resolution avec Pierre Antoine Gämperlé.
Qu'est-ce que l'indépendance et que suppose-t-elle? Vision d'un éthicien par Nicolas Tavaglione, Docteur en science politique, Maître assistant au Département de science politique et relations internationales, Unige. Nicolas Tavaglione est spécialisé en philosophie politique et en éthique appliquée, et ses travaux portent sur les rapports entre Etat et individu. Il est également consultant en éthique auprès du CICR et chroniqueur au Courrier.
Table ronde animée par Isabelle Dubois. Présentation de la future fonction de DPO dans le règlement européen. Qu'eut-il fallût pour que l'indépendance soit respectée en Valais et à Genève? Concrètement, pourquoi est-elle nécessaire? Exemple d'utilité du DPO.

CERT/CSIRT – Efficiently Responding to Incidents,
16 september 2014, Lausanne
Comité d'organisation: Stefan Lueders, Membre du comité, CERN, Brian Henningsen , Membre du comité Clusis, Jacqueline Reigner, Présidente du Clusis, Sémafor Conseil, Enrico Viganò, Vice-président du Clusis, Etat de Genève
108 participants

Despite statements from security solution providers, there is no 100% security possible. Attackers are holding all advantages to choose whom to attack, when and with which means. As a normal attack surface of a company — vulnerable Internet-facing servers, unpatched desktop computers, unencrypted laptops, sub-optimally trained IT personnel, negligent users — is immense, computer security incidents have happened, happen and will continue to happen. Companies and governments must be prepared to quickly, effectively and efficiently detect, contain and mitigate such incidents. This conference should give an overview on the "how".
Max Klaus (MELANI): How MELANI fights Cyber attacks. Over the past years, the World Wide Web has become more and more important for everybody: We use the Internet not only for business purposes, but also to organize and facilitate our private life: We book our vacation online, we buy books and clothes, we even pay our invoices online. Unfortunately, there are also lots of dark figures which want to steal our money, our credentials and our credit card numbers. This presentation shows you why an organization such as MELANI is indispensible for Switzerland and what types of cyber attacks occur daily.
Max Klaus has been working for the Swiss Government since 2002 and has a polytechnic degree in IT security. He started in the Swiss Federal Chancellery, where he worked for different E-Government and E-Voting projects. After 18 months as IT Security Officer in the Federal Department of Defense, People's Protection and Sports, he started his work as Deputy Head of MELANI on September 1st, 2008. He is responsible for the strategic development of this organization as well as for parliamentary affairs and public relation.
Michael Hausding (SWITCH): Drive-By Exploits - Mitigation and Takedown. Drive-By exploits is the #1 emerging threat, identified by the European Network and Information Security Agency (ENISA). More than 60% of all internet users have a vulnerable browser or plugin and are potentially infected when visiting a compromised website with drive-by code injections. The malicious code is injected by cyber-criminals on legitimate websites by using stolen credentials or taking advantage of unpatched Content Management Systems (CMS). To protect the internet users and avoid infections of their computers with malware the injected code needs to be removed from the websites as soon as it is detected. Due to the complexity of CMS the website owner is often unable to cope with the problem. The website hoster or webmaster are most likely the ones who need to do the cleanup or suspension. The Swiss telecom regulator has given the registry for the .ch&.li CC-TLD (SWITCH) a mandate to mitigate phishing and malware distributing websites. If no solution can be found the registry has the authority to temporally suspend the domain name. However the preferred solution is to clean the infected website. To achieve this goal SWITCH is cooperating with the hosters of the infected websites to clean them as fast as possible.
Michael Hausding is a Security Engineer for SWITCH the CC-TLD registry for .ch/.li. He is running the program to clean infected websites in Switzerland . He holds a master degree in Computer Science from TU Darmstadt and a Master of Advanced Studies in Management Technology and Economics (MTEC) from ETH Zürich.
Reto Inversini (MELANI/GovCERT.ch): The basic steps for an effective incident response using the showcase of an exemplary APT. The talk is going to show various aspects of an incident response in the case of an Advanced Persistent Threat, showing some detection techniques as well as a short demonstration of static and dynamic malware analysis. Some crucial decisions that have to be made by incident responders are covered by the speech as well.
Reto Inversini studied Geography/Climatology at the University of Berne and Information Technology at the University of Applied Science in Berne. He worked for various organizations first as a systems- and network engineer then as a security architect. Currently he works as a technical analyst for MELANI with a focus on malware analysis and network security. Apart from his daily work he teaches security architecture and incident response at the University of Applied Science in Berne. In his spare time he enjoys stargazing, meteorology and reading books.
Brian Henningsen & Stefan Lueders (CERN): A few short examples of handling real incidents.

Capitalisation des compétences développées par les membres du Clusis et d'autres organismes associés:

Projet de cartographie des formations en matière de sécurité de l'information

Le Clusis à rejoint l'initiative du comité scientifique du MAS Infosec de la HEC Genève afin de produire une cartographie des formations actuelles dans le domaine de la sécurité de l'information. Certaines entités de formation ont été approchées, dont l'IAE d'Aix-en-Provence, la Heg Genève, etc.

Leadership Jean-Luc Pillet, UNIGE, Suppléant Enrico Viganò, Etat de Genève

En plus le Clusis développe sa position de référence, notamment par l'édition de la publication : "Décideurs, ceci vous concerne", rédigée par un florilège de journalistes qui ont assistés à la Journée Stratégique 2015 Clusis-Campus.

Comité 2014-2015

Jacqueline Reigner, Présidente - Sémafor Conseil SA
Enrico Viganò, Vice-Président - Etat de Genève
Stephan Conradin - Consultant indépendant
Nadia Dali
Raoul Diez – FER
Charly Delay
Sabah Detienne
Isabelle Dubois - AD'HOC RESOLUTION
Henri Haenni – ardantic SA
Stéphanie Haesen-Perroud
Brian Henningsen
Stefan Lueders - CERN
Joelle Mathey
Giovanna Di Marzo Serugendo, Professeure Université de Genève
Jean-Luc Pillet - Université de Genève
Matthieu Schaeffler - Etat de Genève
Igli Tashi – Kudelski
Pierre Toquard – consultant indépendant
Nicolas Vernaz – Addaxpetroleum
Sam Vuilleumier - Etat de Vaud

Activités du comité

La Présidence et les membres du comité ont pris une part active dans l'organisation des conférences et des centres de compétences tant par les moyens de communication informatiques que par de nombreux téléphones entre deux activités professionnelles et par des réunions de travail autour d'un déjeuner rapide.
Le comité a de plus participé à des journées complètes de travail.

La Présidence a également organisé le travail administratif et financier avec le soutien de la fiduciaire Roubaty.

Rapport financier

En résumé, le bilan de l'association présente au 31 décembre 2014 un total de CHF 80'955.83
Les fonds propres sont de CHF 70'259.78 et le résultat 2014 est un bénéfice de CHF 1'404.75.

Les produits, essentiellement des cotisations, s'élèvent à CHF 77'414.84
Le montant consacré à l'organisation des manifestations est de CHF 40'336.90 pour un total des charges de fonctionnement de CHF 76'010.09
(voir le rapport de la fiduciaire Roubaty).

Au programme 2015-2016

-
-
-
-

.

Le 14 avril 2015

Jacqueline Reigner, dr ès sciences
Présidente

Enrico Viganò
Vice-Président