UNIVERSITÉ PARIS DESCARTES

EXERCICE 2018

CONSEIL D'ADMINISTRATION
Délibération n°D-CA/2018-027

Le conseil d'administration s'est réuni le 03 avril 2018 en séance plénière, sur convocation du Président de l'Université adressée le 23 mars 2018.

VU le code de l'éducation, notamment ses articles L613-2, L712-3 et L712-6-1 ;
VU les statuts de l'Université ;
VU l'avis favorable de la Commission de la Formation et de la Vie Universitaire en date du 20 mars 2018 ;

Point de l'ordre du jour : IIème Partie – P1.3 - DU Cyber Sécurité (IUT)

Exposé de la décision :

Historique :
Les réseaux informatiques sont au centre de la production économique mondiale et prennent une place devenue quasiment incontournable dans l'organisation sociale. Face à un nombre toujours croissant d'attaques et de menaces, il est nécessaire d'étudier et d'analyser l'ensemble des composantes associées à ces réseaux informatiques. Cela va des moyens de transport de données aux services applicatifs en passant par les équipements physiques, les systèmes d'exploitation, les logiciels de communication (architecture et protocoles associés). Dans cette formation l'ensemble de ces composantes sont étudiées et analysées afin de comprendre et d'identifier les menaces ainsi que les contre-mesures associées.

Selon une récente étude (juin 2017), faite par le Cabinet EY et mandatée par le Syntec Numérique, il a été conclu que : « la Cybersécurité constitue une filière dynamique et en croissance avec 24 000 emplois pour la branche du numérique, soit 3 % des effectifs totaux. La pénurie des talents en matière de Cybersécurité risque de s'intensifier dans les prochaines années. Tout doit être fait pour résorber cette pénurie et accroître l'attractivité de la Cybersécurité ».

La sécurité des réseaux informatiques est devenue ainsi un élément critique qu'il faut traiter sous les angles conceptuels et pratiques : c'est l'objectif du DU Cybersécurité.

Ce DU couvre l'ensemble des composantes fondamentales nécessaires à la maîtrise, l'analyse, la conception et la mise en œuvre de solutions de sécurité des systèmes et réseaux informatiques.

Problématique :
L'intégration croissante des nouvelles technologies dans les entreprises s'accompagne de nouveaux enjeux tels que la conformité réglementaire, l'évolution des systèmes et des compétences, la sensibilisation à la Cybersécurité ainsi que la sécurité et la confidentialité des données traitées, échangées et archivées. L'émergence accrue de nouvelles menaces liées à la cybercriminalité et leur médiatisation ont induit une prise de conscience générale au niveau de l'entreprise (dirigeants, métiers, comité d'audits, etc.). L'ensemble des entreprises est maintenant exposé à des attaques dont la maturité et la sophistication sont très élevées.

La Cybersécurité est devenue ainsi un élément stratégique pour l'entreprise. De plus en plus conscientes des enjeux, les entreprises investissent davantage dans la sécurité de leurs systèmes d'information. Plus qu'une simple fonction support, l'intégration de ces problématiques devient un atout différenciant sur le marché, notamment pour les grandes entreprises. Tous les acteurs économiques et les administrations publiques sont aujourd'hui concernés par la Cybersécurité. Suivant leur degré d'exposition au risque et à la nécessité de sécurité, les entreprises font le choix d'intégrer et développer en interne une expertise Cybersécurité et/ou de recourir à des prestataires ou fournisseurs externes.

UNIVERSITÉ PARIS DESCARTES

Se distinguent ainsi deux types d'acteurs de la Cybersécurité pour les entreprises du numérique :

- D'une part les entreprises dites « fournisseurs ou prestataires » de solutions ou de services en Cybersécurité : les éditeurs de solutions logicielles de sécurité (pour particuliers et professionnels) et les prestataires de services Cybersécurité acteurs pour le développement de logiciels et la mise en place de protections au sein des entreprises.
- D'autre part, les entreprises dites « utilisatrices » de la Cybersécurité, dont le cœur d'activité n'est pas directement lié à la Cybersécurité mais qui ont besoin d'assurer un certain niveau de protection des données : données clients, secrets de fabrication, commerce en ligne... Par définition de cette catégorie, ces entreprises ont au moins un professionnel dédié à la Cybersécurité parmi leurs employés.

Proposition de décision soumise au Conseil :
Au regard de ces enjeux sociétaux et professionnels, est demandée la création du DU Cybersécurité à destination de collaborateurs d'entreprise souhaitant monter en compétences dans le domaine de la sécurité des réseaux informatiques, et dont l'ouverture est prévue en octobre 2018.

Après en avoir délibéré, le Conseil d'administration approuve la présente délibération.

Nombre de membres constituant le Conseil : 36
Quorum : 18
Nombre de membres participant à la délibération : 20
Abstentions : 0
Votes exprimés : 20
Contre :0
Pour : 20

Fait à Paris, le 11 AVR. 2018

Le Président

Frédéric DARDEL

En application des articles R421-1 et suivants du Code de justice administrative, la présente délibération pourra faire l'objet, dans un délai de deux mois à compter de sa notification et/ou de sa publication, d'un recours gracieux auprès du Président de l'Université Paris Descartes et/ou d'un recours pour excès de pouvoir devant le Tribunal administratif de Paris.

Classé au registre des délibérations du Conseil d'administration, consultable au secrétariat de la Direction des affaires générales et juridiques

Relevé de décisions publié sur le site internet de l'Université le : 11 AVR. 2018
Transmis au Recteur le : 11 AVR. 2018

U-PC Université Sorbonne