



# MANAGEMENT DE LA SÉCURITÉ DES DONNÉES NUMÉRIQUES

L'OBJECTIF DE CE MBA, EST DE FORMER, AVEC L'APPRENTISSAGE EN PART TIME, DES MANAGERS DES SYSTÈMES D'INFORMATION ET DES DONNÉES NUMÉRIQUES. UNE DEMANDE EN FORTE EXPANSION, QUI REGROUPE DE NOMBREUX MÉTIERS, POUR LES ENTREPRISES, LES ADMINISTRATIONS PUBLIQUES, LES COLLECTIVITÉS TERRITORIALES ET LES INSTITUTIONS DE RÉGULATION.

Sous la direction d'experts internationaux les étudiants acquièrent :

- . Méthodes d'analyses des risques
- . Connaissance de la sécurité des architectures (adressage, routage, trafic, protocoles, certificats, cryptologie, Cloud Computing, Big Data, modélisations, systèmes embarqués, BYOD, IAM),
- . Création et protection du patrimoine informationnel de l'entreprise, règles du management
- . Gestion des SI complexes, ERP, CRM, incidents, fuites
- . Réalisation d'audits

- . Organisation d'un plan de sécurité numérique
- . Mise en place d'une sécurité marketing,
- . Réponse à des appels d'offre.
- . Expertise du droit de la communication, des normes de la sécurité numérique, du droit pénal lié à la cybercriminalité, du droit assurantiel et du droit commercial dans le cyberspace,
- . Expertise en e-administration, intelligence économique, géopolitique du cyberspace
- . Sécurité des projets et données des Etats,
- . Prospective du Big Data, des monnaies virtuelles, des objets connectés numériques.

## DEVENEZ ...

- . Ingénieur expert en sécurité réseaux
- . Chef digital officer
- . Ingénieur / Consultant expert en sécurité de l'information et des réseaux
- . Conseiller auprès de la Direction sur la sécurité des données numériques
- . Responsable cellule veille sur les cybermenaces et leurs contre-mesures
- . Gestionnaire des contrats avec les partenaires et les sous-traitants sur la cybersécurité.
- . Ingénieur expert en développement d'applications sécurisées
- . Chef de projet sécurité
- . Conseiller sécurité en marketing numérique
- . Expert audit sécurité numérique

## ILS NOUS FONT CONFIANCE

ACADÉMIE DE L'INTELLIGENCE ÉCONOMIQUE, ALCATEL, AIRBUS GROUP, AXA, BNP PARIBAS, CEIS, COGNITIS, CLUB DES DIRECTEURS DE SÉCURITÉ DES ENTREPRISES, EDF, FORUM ATENA, HSBC, NOMURA, SPALLIAN, ORANGE, SOCIÉTÉ GÉNÉRALE, THALES, TOTAL, TECHNIP

# ORGANISATION

## PART TIME

Le programme du MBA spécialisé Management de la sécurité des données numériques en **part-time ou full time, est organisé sur 12 mois** :

- 387 heures de cours et séminaires, et 20 heures de conférences, répartis sous forme de 5 jours / mois en 4 modules : fondamentaux, gestion de la sécurité juridique des réseaux numériques, gouvernance, gouvernance internationale du risque.

Les étudiants, bac+4 ou équivalence, sont déclarés admissibles après l'étude de leur dossier et admis après un oral d'admissibilité devant le comité d'orientation pédagogique.

**L'obtention du diplôme nécessite une assiduité et la moyenne pour chacun des modules et pour le mémoire soutenu à la fin de la formation magistrale.**



Issu du ministère de la Défense, mon but est de simplifier la vie des organisations tout en maîtrisant la complexité de l'espace numérique. Une sécurité robuste ne se conçoit qu'en étant partagée et ce MBA nous permet justement d'interagir avec une multiplicité d'acteurs. Ce cursus nous transmet des outils pour identifier les opportunités de l'espace numérique en développant une culture de l'anticipation. Sur le plan professionnel, je suis Officier de marine. Après plusieurs années en mer et en conduite des opérations, ce MBA complète mon parcours en cybersécurité en lien avec la société civile."

**Pierre-Marie LORE**, Officier de marine  
(promotion 2015-2016)



En tant que Criminologue - Expert en protection des entreprises et en Intelligence Economique, m'intéresser à cette nouvelle forme de gouvernance de risques dans le domaine du numérique m'est apparu comme naturel. Participer au MBA, c'est vouloir réaliser une formation hautement qualifiée composée d'intervenants de qualité. Pour moi, la finalité même de cette formation est d'acquérir une réelle expertise pour accompagner les entreprises dans leur stratégie globale de sécurisation et de mise en sûreté de leur entreprise."

**Bernadette LEROY**, Présidente d'AESATIS  
(promotion 2015-2016)

40K€

SALAIRE MOYEN BRUT ANNUEL (JUNIOR),  
90K € SALAIRE MOYEN BRUT ANNUEL (SÉNIOR)  
OBJECTIFS SALARIAUX DU SECTEUR DU  
MANAGEMENT DES DONNÉES NUMÉRIQUES

387

HEURES DE COURS THÉORIQUE ET SÉMINAIRES

100%

D'INTERVENANTS PROFESSIONNELS

# PROGRAMME

L'objectif de cette formation est de former des cadres et des étudiants qui possèdent les éléments fondamentaux du management et de la gouvernance de la sécurité des projets et des données numériques, et qui seront directement opérationnels. Cela aussi bien pour les entreprises publiques que privées, les collectivités territoriales, les Etats ou les organisations internationales. Pour atteindre cet objectif, l'approche retenue est fondée sur des cours fournis par des professionnels reconnus, sur un apprentissage en relation directe avec la formation, et une thèse d'apprentissage qui s'oriente vers un problème d'actualité, rédigée sous la direction d'un tuteur. Le programme s'appuie sur les recommandations des professions visées. Il est dirigé par une équipe pédagogique et un comité d'orientation

## LES COMPÉTENCES VISÉES

- . Conseil opérationnel
- . Cellule de veille
- . Gestion de contrats.
- . Marketing numérique
- . Environnement international
- . Interactions avec les autres fonctions de l'entreprise
- . Développement de capacité managériale
- . Maîtrise des risques juridiques
- . Gestion des risques

## • Nombre d'heures d'enseignement :

387 heures et 20 heures de conférences

## • Nombre de modules, séminaires, d'ateliers : 20

MODULES	NOM	MATIÈRES
1	<b>Fondamentaux pour le management et la sécurité des projets et des données numériques</b> 100 heures	<p>Connaissances fondamentales de la sécurité des architectures et gestion 1 : adressage, routage et trafic sur internet ; les protocoles, Les télécoms et leurs vulnérabilités, le chiffrement et les réseaux privés virtuels (VPN), la signature électronique et la gestion des certificats numériques, le big data et ses applications à la cybersécurité, sécuriser le cloud</p> <p>Connaissances fondamentales de la sécurité des architectures et gestion 2 : modélisation et simulation, les systèmes embarqués et sécurité, le BYOD, sa gestion et ses dangers, les objets communicants, l'IAM (Information &amp; Access Management)</p> <p>Gestion de crise et communication de crise</p> <p>Plan de continuité et de reprise des activités, Maintien en condition opérationnelle</p> <p>Patrimoine informationnel de l'entreprise ; présence sur l'internet ; Propriété intellectuelle dans l'entreprise et valorisation des actifs immatériels ; Données personnelles dans l'entreprise ; accountability, Privacy by design, Privacy impact assessment, Encadrement de la vie privée et professionnelle dans l'entreprise ; les chartes d'utilisation</p>
2	<b>Gestion de la sécurité juridique des projets et des données réseaux numériques</b> 80 heures	<p>Introduction aux contrats informatiques (services Cloud, etc.), Commerce électronique BtoB et BtoC, protection des concepts et des projets, marques, brevets, dessins et modèles, protection du savoir-faire et des secrets d'affaires ; réseaux sociaux : identification électronique, et services de confiance</p> <p>Droit assurantiel dans le cyberspace, les réseaux, entreprises</p> <p>Droit de la communication, propriété intellectuelle des Data hébergés obligations devant la CNIL et devant l'ANSSI et éthique de la donnée ; Gouvernance et sécurité du multimédia avancé, des réseaux sociaux et des réseaux mobiles</p> <p>Sécurité marketing, Normes de sécurité numérique, appréhension des risques informatiques ; management de la gestion d'un système de sécurité (famille ISO 27 000) ; gestion qualité (ISO 9001)</p>
3	<b>Gouvernance de la sécurité des projets et des données numériques</b> 100 heures	<p>Gestion de projets SI complexes ; analyse fonctionnelle ; attentes des utilisateurs en expression fonctionnelle et en cahier des charges ; gestion client et approvisionnements ; mettre en place un ERP, un CRM, un système décisionnel, ou encore ouvrir le SI vers ses clients ou ses fournisseurs dans le cadre de l'entreprise étendue</p> <p>Audit et plan de sécurité numérique</p> <p>Gestion des incidents, des vulnérabilités et des non conformités (SIEM, SOC et cyber-défense)</p> <p>Sécurité marketing</p> <p>Prévention contre la fuite des données sensibles et gestion (DLP). Veille technologie, connaissance des offres logicielles en matière d'offres de sécurité. Réponse à un appel d'offres sur les architectures sécurité, répondre à un AO sur une architecture de réseaux sécurisés calcul ROI d'une solution IT, amortissement, structure offre financière. VPM. Modélisation et simulation ; Les systèmes embarqués et leur sécurité, le BYOD, les objets communicants, l'IAM (Information &amp; Access Management)</p>
4	<b>Géopolitique et prospective de la sécurité des projets et des données numériques</b> 100 heures	<p>Intelligence économique , évolution des offres, gestion des risques réseaux</p> <p>E-administration. Management et sécurité des projets et des données numérique de l'Etat ; sécurité missions ANSSI ; délégation interministérielle sécurité, Etalab et open data gouvernemental, dématérialisation et etalab Décret et charte internet de l'Etat ; stratégie digitale</p> <p>Risque pays</p> <p>Prospective: TEDx, Big Data, nouveaux enjeux de la Cyber Sécurité (APT), Web 2.0, 3.0 et monnaies virtuelles, Trading hautes fréquences droit du cyberspace, objets connectés dans l'entreprise</p> <p>Cybercriminalité, cyberguerre, cyberespionnage et cyberhacktivisme</p>
5	<b>Stage et méthodologie de la thèse</b> 7 heures	<p>Stage</p> <p>Méthodologie de la thèse d'apprentissage et méthode</p> <p>Tutorat</p>
6	<b>Conférences obligatoires</b> 20 heures/an	<p>Dont les "lundis de l'Intelligence Économique"</p> <p>Conférences: Droit pénal et cybercriminalité</p>

## INFORMATIONS PRATIQUES

- **Président de l'ILV** : Driss AÏT YOUSSEF
- **Responsable du programme** : Yves ROUCAUTE

## CANDIDATURE ET INSCRIPTION

- **Admission**
  - . A partir de bac+4 d'une école de commerce ou d'ingénieur
  - . A partir d'un Bac+3 avec une expérience professionnelle (après validation du dossier par la commission d'autorisation de candidature)
- **Processus d'admission**

La sélection des candidats est effectuée en trois temps :

  1. Examen du dossier de candidature (admissibilité)
  2. Convocation à un entretien individuel devant un jury de sélection
  3. Délibération du jury d'admission
- **Coût du programme**
  - . Frais de dossier : 89 euros (full time), 129 euros (part time)
  - . Frais de scolarité : nous consulter

## POUR PLUS D'INFORMATION

**Service admissions**  
Tél. : 01 41 16 73 37  
ilv@devinci.fr

## COMITÉ D'ORIENTATION PÉDAGOGIQUE

**Driss AÏT YOUSSEF** : Docteur en droit, Président de l'Institut Léonard de Vinci, Co-directeur du MBA, Auditeur de l'Institut national des hautes études de la sécurité et de la justice

**Alain JUILLET** : Président du Club des directeurs de sécurité des entreprises, Président de l'Académie d'intelligence économique, Membre du collège du CNAPS

**Jean Pierre LEGENDRE** : Président de COGNITIS, Président Cercle d'Intelligence Économique MEDEF Paris

**Laurent MEREYDE** : Directeur de la Sûreté du groupe TECHNIP

**Renaud PROUVEUR** : P.D.G. Spallian

## DIRECTION PÉDAGOGIQUE

**Yves ROUCAUTE** : Directeur du MBA, Professeur des Universités, agrégé de droit public-science politique et de philosophie, représentant la France à International Association of Criminology, concepteur du paradigme de sécurité globale, ex-Président du conseil scientifique de l'INHESJ

**Jean-Jacques BRUN** : Directeur adjoint du MBA Directeur du pôle management des risques de CEIS, directeur du DSI de CEIS, spécialiste en cyber-sécurité, Cyber threat intelligence, Gestion des risques et des crises, Due diligence, Business intelligence et veille.

**Gérard PELIKS** : Directeur adjoint du MBA, Président de l'atelier sécurité du Forum ATENA, Membre de association des réservistes du chiffre et de la sécurité de l'information (ARCSI), Ingénieur diplômé, Lieutenant-colonel de la réserve citoyenne de cyberdéfense (DGGN)

**Lionel GUILLET** : Commandant dans la Réserve citoyenne de cyberdéfense, membre de l'Association des réservistes du chiffre et de la sécurité de l'information (ARCSI)

**Paul RICHY** : Expert sécurité de l'information Orange - SG/DSEC (Direction de la sécurité du Groupe), Vice-président du comité sécurité de l'information, AFNOR