EGE Ecole de Guerre Economique

FORMATION INITIALE

RENTREE OCTOBRE

RSIC

2019 2020

Formation initiale

Risques, Sûreté Internationale et Cybersécurité

EGE Ecole de Guerre Economique
196, rue de Grenelle, 75007 Paris
Tél . : +33 1 45 51 00 02

contacts@ege.fr
www.ege.fr

SURVEILLER.
ANALYSER.
PROTEGER.
INFLUENCER.

Formation Risques, Sûreté Internationale et Cybersécurité

Risques, Sûreté Internationale et Cybersécurité

La question de la sûreté matérielle des entreprises ne peut plus être dissociée aujourd'hui de la problématique des menaces immatérielles qui affectent la vie économique via les réseaux informatiques et Internet.

La protection de l'entreprise et la sûreté internationale sont désormais des enjeux stratégiques qui ne peuvent plus être traités par une série de mesures techniques.

Objectifs de la formation

Le programme RSIC donne à l'étudiant les compétences techniques et managériales pour gérer un projet où l'information sera la matière stratégique à analyser.

Ce programme vous préparera à (objectifs pédagogiques):

- Connaitre la géopolitique de la cyber-sureté (risques pays…) les risques criminels (mafias…)
- Enseigner les savoir-faire de la Sureté, du Cyber (sans avoir un background technique) et le la gestion des risques à des cadres issus du privé comme du secteur public
- Comprendre les coopérations public / privé dans les domaines de la cyber et de la sureté : Gendarmerie, Police, DGSI DGSE DPRSD ANSSI…
- Assimiler la cartographie des acteurs des métiers de la Cyber-sureté et les rôles de chacun.
- Mettre en œuvre une politique de sureté au sein d'une entreprise ou organisation
- Savoir évaluer les risques dans leurs globalités (humains, installations complexes, maritimes…)
- Maitrise et management des risques de conformité et mener des due diligences
- Amener la discipline comme une matière essentielle dans la gouvernance de l'entreprise
- Concevoir une offre de services en Cyber-sureté (audit et étude)
- Sensibiliser et former le personnel à la Cyber-sureté
- Comprendre une architecture réseau et la place de la cybersécurité
- Anticiper la crise par ma mise en œuvre d'une politique de gestion des risques (Contrôle qualité, PCA, cellule spécifique…)
- Préparer une gestion et communication de crise (decision room, media-training…)
- Droit et Cyber-sureté (normes, certifications…)

Formation Risques, Sûreté Internationale
et Cybersécurité

Programme RSIC
2019/2020

Le programme RSIC se décompose en 7 modules :

(Module 0) : Pré-rentrée (étudiants n'ayant pas effectué le M1 RSIC)

- Cartographie d'un environnement (Mindmapping, matrices sociaux-dynamiques)
- Fonctionnement d'un réseau
- La collecte d'information
- Les grilles de lectures, géopolitique de la Puissance
- La cartographie d'acteurs

Module 1 : Définitions et géopolitique de la sécurité / sureté et du numérique

- Les concepts de sûreté/sécurité liés au numérique (le concept de « homeland security » à l'aube du XXIème siècle)
- Le marché de la cybersécurité et de la sûreté : les différentes prestations (audit, pentest, accompagnement juridique, assurance des SI…) et les différents labels/qualifications/certifications d'entreprises
- Cartographie des acteurs en matière de cybersécurité
- Géopolitique du cyberespace
- Travaux dirigés sur l'étude d'une stratégie nationale de cybersécurité

Module 2 : Les enjeux de la cybersécurité en entreprise

- Notions de base de la cybersécurité
- Panorama des menaces : l'état de l'art des hackers
- L'hygiène informatique : principes et mesures
- Identifier les risques et vulnérabilités des systèmes d'information
- Gestion de la cybersécurité au sein d'une entreprise (référent SSI, RSSI, chaîne fonctionnelle / organisationnelle)
- Systèmes d'informations internes / externalisation des SI
- Audit de cybersécurité : Connaître ses vulnérabilités
- Mode de pensée d'un hacker
- Initiation à la cryptographie

Module 3 : Les politiques de sûreté à l'internationale

- Géopolitique régionale - Moyen orient
- Géopolitique régionale - Afrique SubSaharienne
- Géopolitique régionale - Asie
- Géopolitique régionale - Monde Russe
- Géopolitique régionale - Amérique Latine
- Méthodologie de la constitution d'un « dossier pays »
- Sécurité individuelle du collaborateur en mission ou expatrié
- Sécurité de l'information et déplacement à l'étranger
- Security Management
- Le risque terroriste
- La sûreté de l'entreprise et des collaborateurs en zones isolées
- Le risque culturel
- La fonction sûreté au sein d'une ONG
- La sûreté en milieu maritime

Module 4 : Les entreprises faces aux enjeux de sûreté

- La fonction sûreté au sein de l'entreprise
- Enjeux et mise en œuvre d'une politique de sureté
- Méthodologie de l'audit de sureté/sécurité
- Nouvelles Technologies de la sûreté et de la sécurité (table ronde ?)
- Due diligence associée à l'usage du numérique
- Etablir une analyse de risque (EBIOS, MEHARI)

Module 5 : Le domaine réglementaire des aspects sûreté et sécurité du numérique

- Transfert du risque par l'assurance
- Management Stratégique et planification
- Mettre en place une politique de gestion du risque (vulnérabilité et menaces)
- Typologie des risques physiques et organisationnels
- Protection des installations complexes (industrielles, nucléaires, log....)
- Gestion des risques culturels
- La communication de crise liée à la sécurité du numérique
- Analyse de cas : e-Réputation d'une entreprise en crise
- Exercice de gestion de crise (War Room/ décision Room)
- Elaborer un Plan Continuation Activité (PCA)
- Elaborer un Plan de Reprise d'Activité (PRA)

Module 6 : La gestion des risques et le management des crises physiques et numériques

- Transfert du risque par l'assurance
- Management Stratégique et planification
- Mettre en place une politique de gestion du risque (vulnérabilité et menaces)
- Typologie des risques physiques et organisationnels
- Protection des installations complexes (industrielles, nucléaires, log....)
- Gestion des risques culturels
- La communication de crise liée à la sécurité du numérique
- Analyse de cas : e-Réputation d'une entreprise en crise
- Exercice de gestion de crise (War Room/ décision Room)
- Elaborer un Plan Continuation Activité (PCA)
- Elaborer un Plan de Reprise d'Activité (PRA)

Module 7 : Le rôle du manager en sûreté et en sécurité du numérique

- Nouvelle gouvernance de la Cyber-sureté
- Etablir une campagne de sensibilisation du personnel
- Mettre en place un Business Games au sein de l'entité
- Mise en place d'une instance en charge de la sûreté et de la cybersécurité
- Le rôle du CIL et du DPO (Data Protection Officer) dans la RGPD
- Le rôle du directeur de la sûreté et retours d'expériences
- Le rôle du RSSI et retours d'expériences
- Le rôle de l'État (gendarmerie / services...)

EGE Ecole de Guerre Economique

SURVEILLER. ANALYSER. PROTEGER. INFLUENCE.

196, rue de Grenelle, 75007 Paris / +33 1 45 51 00 02 / contact@ege.fr / www.ege.fr