Nom de l'UE : Gouvernance de la sécurité	Semestre : S9

Objectifs de l'UE

L'ECUE Réglementation, normes et politiques de sécurité de cette UE présente les aspects liés à la réglementation, aux concepts inhérents aux outils organisationnels et réglementaires régissant la sécurité alors que l'ECUE Facteur humain et méthodes d'analyse de risques présente l'analyse des risques, le traitement des incidents de sécurité et l'impact du facteur humain sur la sécurité du système d'information. A l'issue de cette UE, l'étudiant saura :

- Identifier les principaux éléments juridiques liés à la SSI
- Reconnaître et définir les principaux acteurs chargés de la sécurité à l'intérieur et autour d'une entreprise, ainsi que les difficultés associées.
- Apprécier et appliquer les concepts régissant une politique de sécurité en fonction du cœur de métier
- Identifier les enjeux et les parties prenantes, au sein d'une organisation, pour définir et élaborer les briques de base d'une démarche de gouvernance de la sécurité
- Appliquer les concepts des politiques de sécurité et les différents documents associés dans une entreprise ou dans les cadres réglementaires usuels (PSSI E, guides officiels, etc.)
- Structurer et organiser les catégories de risques existant en matière de sécurité
- Caractériser et apprécier l'efficacité des procédures de gestion des incidents de sécurité
- Appréhender les besoins en sécurisation à satisfaire et les objectifs de sécurité à atteindre pour mettre en place des exigences de sécurité d'ordre juridique, organisationnel et technique au niveau des mesures de prévention de protection et récupération

Description des ECUE

Réglementation, normes et politiques de sécurité

- La PSSI, les Normes et référentiels relatifs à la sécurité du SI
- Présentation générale de l'ISO 27001 et des normes ISO 270xx associées
- Certification de systèmes de management de la sécurité informatique
- Bonnes pratiques pour la mise en œuvre et le contrôle des mesures de sécurité nécessaires
- Aspects juridiques : CNIL, RGPD, LCEN. Que faire en cas d'incident ?
- Certifications et audit de sécurité
- Principes d'évaluation de l'efficacité des systèmes de gestion de la sécurité
- Intégration de la protection des données personnelles (norme ISO 27701)
- Les référentiels métiers : PCI-DSS, CMMI

Facteur humain et méthodes d'analyse de risques

- Analyse de risque ISO 27005
- Méthode d'analyse de risques EBIOS, MEHARI, OCTAVE
- Détection des Vulnérabilités

- Gestion des incidents de sécurité
- Le CIRT (Suivi post-incident, analyse, recherche origine, actions de remédiation)
- Le PCA/PRA (Notion de BIA, phases du PCA : Organisation, Elaboration, Implémentation, gestion de crise).

Pré-requis

Sécurité et sûreté des données, bases théoriques de la sécurité, concepts de sécurité

Bibliographie

Alexandre Fernandez-Toro, Management de la sécurité de l'information. 4ème édition, 2018.

Anne Lupfer, Gestion des risques en sécurité de l'information : Mise en œuvre de la norme ISO 27005, 2010.