

USCB2F - Droit, enjeux de sécurité, conformité

Présentation

Prérequis

Bac+2 informatique, BAC + 2 SI ou SHS. Il est conseillé d'avoir suivi le module SEC001.

Objectifs pédagogiques

- Connaître les lois, règlements, politiques et éthique en matière de cybersécurité et de protection de la vie privée.
- Connaître les principes fondamentaux du droit appliqués aux nouvelles législations RGPD et LPM.
- Connaître les principes de cybersécurité et de confidentialité.

Compétences

- Principes fondamentaux de droit, des lois du numérique et de sécurité numérique
- RGPD, les différents volets sous l'angle du droit et de la technique
- LPM, les différents volets sous l'angle du droit et de la technique
- Outils et RGPD et LPM
- Gouvernance nationale et internationale de la cybersécurité et de la sécurité des données

Programme

Contenu

Temps 1: principes

- Cours 1 : Principes fondamentaux de droit
 - Sources du droit (directes et indirectes)
 - Organisation juridictionnelle
 - Hiérarchie des normes
 - Présentation des lois, normes et standards, national et international
 - Domaine d'application de la règle de droit
 - Preuves et sanctions
- Cours 2 : les lois du numérique et de sécurité numérique
 - Principes fondamentaux de la république numérique
 - Lois principales : LCN, Godfrain,
 - Introduction aux lois LPM et RGPD
- Cours 3: Gouvernance nationale et internationale de la cybersécurité et de la sécurité des données
 - Gouvernance mondiale, européenne (organisme,...)
 - Les organismes nationaux :
 - ANSSI et CNIL
 - Les organismes internationaux
- TD3 recherche et analyse d'un cas réel : présentation.

Temps 2 : RGPD, les différents volets sous l'angle du droit et de la technique

- Cours 4 :
 - Enjeux : propriétés (vie privée et traçabilité)
 - Doctrine et stratégie de défense/attaque
 - Cible, menace, vulnérabilités
- Cours 5 : (développé ensuite dans UE)
 - Conformité du point de vue juridique
 - Normes ISO 27x
 - RGS
 - PSSI et biens informationnels
 - Objectifs, Mesures, indicateurs et tableau de bord spécifique)
- Cours 6 :
 - Sanctions

Valide à partir du 01-09-2026

Code : USCB2F

Unité spécifique de type mixte
6 crédits

Responsabilité nationale :
EPN05 - Informatique / Nicolas
PIOCH

Contact national :

Cnam Centre Régional de
Bretagne

Zoopôle Les Croix
2 rue Camille Guérin
22440 Ploufragan
0 972 311 312

Isabelle Guée

bzh_master_cybersecurite@lecnam.

- Organisation de la mise en place RGPD
 - Fonctions (DPO)
 - Responsabilités de l'entreprise
- TD6 RGPD

Temps 3 : LPM, les différents volets sous l'angle du droit et de la technique :

- Cours 7 :
 - Enjeux : propriétés (DIC et traçabilité)
 - Doctrine et stratégie de défense/attaque
 - Cible, menace, vulnérabilités des IT
- Cours 8 : (développé ensuite dans UE)
 - Normes ISO 27x
 - RGS
 - PSSI et IT
 - Objectifs, Mesures, Indicateurs et Tableau de bord
- Cours 9 :
 - Organisation de la mise en place LPM
 - SOC
 - Métiers
 - Outils
 - Responsabilités de l'entreprise
- TD9 LPM : mise en oeuvre au travers d'un cas d'étude suite de TD6 RGPD

Temps 4 : Outils et RGPD et LPM

- Cours 10 : Découverte référentiels métiers
- TD10 : Exemples de référentiels pour les normes de sécurité des données : Santé, PCI,...
- Cours 11 : Découverte big data
- TD11 : Big data : outils, méthodes et moteurs de recherche dans le big data
- Cours 12 : Découverte IA
 - Algorithmes : utilisation d'algorithmes de l'IA,
 - TD12 : petit algorithme d'apprentissage
- Cours 13 : Découverte OC et cookies
- TD13 :

Modalités de validation

- Contrôle continu
- Projet(s)
- Mémoire
- Examen final

Description des modalités de validation

Contrôle continu

Projet(s)

Mémoire

Examen final