DNT108 - Droit de la cybersécurité

Mis à jour le 19-02-2026

Code : DNT108

Unité d'enseignement de type cours

6 crédits

Volume horaire de référence (+/- 10%) : **50 heures**

Responsabilité nationale :
EPN14 - Droit et immobilier / Guillaume DESGENS

Contact national :

EPN14 - Droit

2 rue Conté
75003 Paris

Yasmina NABBACH
par_cnam.droit@lecnam.net

Présentation

Prérequis

Juristes d'entreprise, juristes en collectivités locales ou en administration, juristes d'associations, délégués à la protection des données (DPD) ou référent « informatique et libertés », professions réglementées, responsables conformité, déontologues, contrôle interne et gestion des risques, audit interne, direction qualité, DSI ou RSSI disposant d'une sensibilisation à la dimension juridique, DRH, consultants externes en informatique ou en organisation, personnes en recherche d'emploi ou en reconversion professionnelle.

Avoir le niveau de l'unité d'enseignement de l'UE DRA001 "Présentation générale du droit" ou posséder de bonnes connaissances de base en droit du numérique.
Pour les auditeurs qui souhaitent suivre cette UE dans le contexte d'une montée en compétences RGPD / DPO, il est recommandé, sur le plan pédagogique, de suivre également les UE du certificat de spécialisation DPO (UE DNT 104, DNT 105, DNT 106).

Objectifs pédagogiques

Connaître le cadre juridique et les référentiels applicables au droit de la sécurité des systèmes d'information et de la cybersécurité en France et en Europe ;
Être sensibilisé aux problématiques cybernétiques telles que la connaissance des réseaux, des systèmes et l'étude de leur fonctionnement, et des risques liés aux cybermenaces ;
Identifier les cas d'usage en lien avec les enjeux de sécurité des systèmes d'information et cyber en entreprise ou en structure publique, et savoir établir les plans d'actions associés ;
Connaître les acteurs de la régulation cyber en France et en Europe (ANSSI, CNIL, ENISA, etc.) ;
Disposer des savoir-faire et des bonnes pratiques pour réagir en cas d'intrusion dans un système informatique ou en cas de violation de données.

Programme

Contenu

Sensibilisation aux concepts et enjeux de sécurité des systèmes d'information / cybersécurité
Identification des acteurs français et européens de la sécurité des systèmes d'information (ANSSI, CNIL, ENISA, etc.)
Panorama français et européen des réglementations, référentiels et normes applicables en matière de sécurité des systèmes d'information et de cyber
Étude des règles de protection des données personnelles et des obligations de sécurité, notamment anonymisation et pseudonymisation
Sensibilisation aux enjeux contractuels liés aux hébergements cloud
Connaissance des règles applicables en cas d'intrusions dans un système informatique et les violations de données
Documentation de la conformité et bonnes pratiques de sécurité dans le secteur public et privé (bug bounty, hacktaton…)
Enjeux contractuels de la sécurité des systèmes d'information et de la cybersécurité

Modalités de validation

- Examen final

Description des modalités de validation

Examen final. Une note égale ou supérieure à 10 est exigée.