Lefebvre Dalloz Compétences.

Tél.: 01 83 10 10 10
src-formation@lefebvre-dalloz.fr
formation.lefebvre-dalloz.fr

Cybersécurité : aspects juridiques, techniques et organisationnels - Blended learning

Prévenir et traiter les menaces existantes dans le cyberspace

Code	Durée	Tarif Inter*
701038	1 jour / 7 heures	990 € HT

Repas inclus (en présentiel)

PUBLIC

Directeurs juridiques - Responsables Juridiques - Juristes - Toute personne s'intéressant aux aspects juridiques et organisationnels de la cybersécurité

PRÉ-REQUIS

Aucun prérequis nécessaire

NIVEAU D'EXPERTISE

Perfectionnement

LES POINTS FORTS

Accès en amont de votre formation au E-learning : Que faire en cas de cyber-attaque ? - Durée 45 minutes

MOYENS PÉDAGOGIQUES

- Dispositif de formation structuré autour du transfert des compétences
- Acquisition des compétences opérationnelles par la pratique et l'expérimentation
- Apprentissage collaboratif lors des moments synchrones
- Parcours d'apprentissage en plusieurs temps pour permettre engagement, apprentissage et transfert
- Formation favorisant l'engagement du participant pour un meilleur ancrage des enseignements

SATISFACTION ET EVALUATION

- L'évaluation des compétences sera réalisée tout au long de la formation par le participant lui-même (auto-évaluation) et/ou le formateur selon les modalités de la formation.
- Evaluation de l'action de formation en ligne sur votre espace participant :
  - A chaud, dès la fin de la formation, pour mesurer votre satisfaction et votre perception de l'évolution de vos compétences par rapport aux objectifs de la formation. Avec votre accord, votre note globale et vos verbatims seront publiés

Objectifs pédagogiques

- Analyser le contexte juridique en matière de cybersécurité
- Engager les actions juridiques adaptées en cas d'incident cyber
- Anticiper et limiter les risques cyber

Programme de la formation

Engagement

Connectez-vous sur votre espace participant pour compléter les ressources pédagogiques indispensables au lancement de votre formation. Votre formateur recevra vos objectifs de progrès. Auto-évaluez vos compétences pour suivre vos progrès à l'issue de votre formation..Accès en amont de votre formation au E-learning : Que faire en cas de cyber-attaque ? - Durée 45 minutes

Analyser le contexte juridique en matière de cybersécurité

Mesurer les risques

- Définition des concepts clés en matière de cybersécurité
- Panorama du risque cyber
- Identification des risques et des sources de risques
- Mise en situation : identifier les sources et facteurs de risque au sein de votre entreprise

Identifier les dispositifs institutionnels de réponse au risque cyber

- Panorama des principaux organismes dédiés à la cybersécurité en France
- Principaux points de vigilance liés aux réglementations spécifiques applicables à certains opérateurs, avec un focus particulier sur la directive NIS 2
- Débat : connaître le rôle de l'Anssi

Engager les actions juridiques adaptées en cas d'incident cyber

Qualifier pénalement un incident cyber

sur notre site au travers d'Avis Vérifiés, solution Certifiée NF Service

- A froid, 60 jours après la formation pour valider le transfert de vos acquis en situation de travail

- Suivi des présences et remise d'une attestation individuelle de formation ou d'un certificat de réalisation

ACCOMPAGNEMENT FORMATION À DISTANCE

En cas de nécessité, une assistance technique et pédagogique est joignable entre 8h30 et 18h (jours ouvrés):

- par téléphone : 01 83 10 10 10
- par mail : care-formation@lefebvre-dalloz.fr

Une réponse immédiate est apportée ; si besoin, le demandeur est mis en relation avec un expert dans un délai maximum de 48h.

Atteintes aux STAD

- Infractions de droit commun
- Atteinte aux droits des personnes
- Mise en situation : adopter les bons réflexes pour qualifier juridiquement une cyberattaque

Déployer une réponse juridique adaptée

- Actions extra-judiciaires
- Actions judiciaires (civiles ou pénales)
- Notifications et actions réglementaires
- Partage d'expérience : échanger sur la mise en œuvre concrète d'une réponse juridique à une cyberattaque

Anticiper et limiter les risques cyber

Encadrer les responsabilités des parties prenantes

- Rappel des principes en matière de responsabilité
- Plan d'Assurance Sécurité (PAS)
- Principales clauses contractuelles à négocier
- Pilotage de la relation
- Mise en situation : comprendre les enjeux de responsabilité dans des projets complexes

Limiter les risques par des moyens techniques et opérationnels

- Mesures techniques
- Sensibilisation et formation
- Documentation interne (procédures, politiques, chartes,...)
- Plan de gestion de crise
- Débat : renforcer l'appropriation et l'application des politiques et process internes

En amont et en aval de la formation, le positionnement pédagogique sera effectué à l'aide d'un questionnaire d'auto-positionnement.

Transfert

Votre parcours de formation se poursuit dans votre espace participant. Connectez-vous pour accéder aux ressources, auto-évaluer vos compétences acquises pendant votre formation et faciliter la mise en œuvre de vos engagements dans votre contexte professionnel.
Accès en aval de votre formation au E-learning : Que faire en cas de cyber-attaque ? - Durée 45 minutes

A noter

En amont et en aval de la formation, le positionnement pédagogique sera effectué à l'aide d'un questionnaire d'auto-positionnement.

Prochaines sessions

PARIS

- 9 Sep. 2026
- 13 Nov. 2026

A DISTANCE

- 9 Sep. 2026
- 13 Nov. 2026

AIX-EN-PROVENCE

- 13 Nov. 2026

BORDEAUX

- 13 Nov. 2026

CHAMBERY

- 13 Nov. 2026

GRENOBLE

- 13 Nov. 2026

LILLE

- 9 Sep. 2026
- 13 Nov. 2026

LYON

- 9 Sep. 2026
- 13 Nov. 2026

MARSEILLE

- 13 Nov. 2026

MONTPELLIER

- 13 Nov. 2026

NANTES

- 13 Nov. 2026

NICE

- 13 Nov. 2026

NIORT

- 13 Nov. 2026

PAU

- 13 Nov. 2026

RENNES

- 13 Nov. 2026

ROUEN

- 13 Nov. 2026

STRASBOURG

- 13 Nov. 2026

TOULOUSE

- 13 Nov. 2026

TOURS

- 13 Nov. 2026