UniCamp

SYLLABUS

PREPARER SA CONFORMITE NIS-2

BELKACEM EL KHRISSI

INFORMATIONS GÉNÉRALES

Titre du cours : Préparer sa conformité NIS-2

Début de la formation : 21/09/2026 Fin de la formation : 04/10/2026

Prérequis : aucun

Volume horaire : 9 heures (7h asynchrones et 2 h synchrones).

Temps synchrones :

- Mardi 22 septembre de 10h30 à 11h30
- Mardi 29 septembre de 10h30 à 11h30

RESPONSABLE PÉDAGOGIQUE

Belkacem El Khrissi,

Ancien Responsable Informatique, ayant occupé plusieurs postes allant du support technique au pilotage stratégique. Belkacem El Khrissi accompagne aujourd'hui les organisations dans l'optimisation de leurs systèmes et le durcissement de leur sécurité, par approche puisant ses racines dans une première vie professionnelle : dédiée à la lutte contre la fracture numérique au début des années 2000. Cette expérience fondatrice en tant que travailleur social a forgé une conviction : la technologie ne vaut que par sa maîtrise par l'utilisateur.

Aujourd'hui, Belkacem El Khrissi se positionne comme un vulgarisateur au service de la performance, réconciliant l'expertise technique et la pédagogie pour garantir que la sécurité des systèmes d'information devienne une compétence partagée et durable au sein des équipes.

OBJECTIFS DE LA FORMATION

La directive européenne NIS2 renforce les exigences en matière de cybersécurité pour de nombreuses organisations publiques et privées. Elle introduit notamment de nouvelles obligations de gouvernance, une approche structurée de la gestion des risques et un cadre de responsabilité renforcé pour les dirigeants.

Ce cours propose une présentation claire et structurée des principes fondamentaux de la directive NIS2. Il permet aux participants de comprendre :

- Les objectifs de la directive
- Les organisations concernées
- Les principes de gouvernance attendus
- La place de la gestion des risques dans la cybersécurité.

Le cours met l'accent sur la logique de décision et de priorisation introduite par la directive, afin de permettre aux apprenants de comprendre les mécanismes de gouvernance associés à NIS2.

Ce cours constitue un socle de sensibilisation et de compréhension, et ne vise pas la mise en œuvre opérationnelle complète de la directive.

Des temps de visio-conférence seront programmés pour revenir sur des questionnements et l'actualité de la réglementation.

À l'issue de la formation, les apprenants seront capables de :

Identifier la directive NIS2 dans le cadre de la cybersécurité européenne

> Examiner les objectifs de la directive NIS2 et les évolutions introduites dans le cadre réglementaire européen de la cybersécurité.

Déterminer les organisations concernées par la directive NIS2

> Situer le périmètre d'application de la directive et identifier les organisations susceptibles d'être concernées.

Identifier le mécanisme d'auto-identification des entités

> Examiner le mécanisme permettant aux organisations de se positionner comme entité essentielle ou entité importante.

Déterminer les principes de gouvernance en cybersécurité introduites par NIS2

> Appliquer les exigences de gouvernance attendues par la directive et la place de la cybersécurité dans les décisions des organisations.

Déterminer la logique de gestion des risques dans le cadre de NIS2

> Situer la place de la gestion des risques dans la directive et le rôle d'une approche structurée dans la prise de décision.

ORGANISATION DU COURS

Le cours est structuré en plusieurs modules courts permettant une progression progressive dans la compréhension de la directive.

Module 1 – Comprendre le contexte de la directive NIS2

- Pourquoi une directive européenne sur la cybersécurité
- Les limites du cadre précédent (NIS1)
- Le passage d'une approche déclarative à une approche démonstrative
- La place de la gestion des risques dans la cybersécurité

Module 2 – Identifier les organisations concernées

- Secteurs hautement critiques
- Secteurs critiques
- Critères de taille des organisations
- Comprendre le périmètre d'application de la directive

Module 3 – Comprendre la logique d'auto-identification

- Entité essentielle
- Entité importante
- Principe d'auto-identification
- Positionnement des organisations

Module 4 – Gouvernance et gestion des risques

- Gouvernance de la cybersécurité
- Rôles et responsabilités
- Chaîne d'approvisionnement et prestataires
- Logique de décision et de priorisation

Module 5 – Structurer la gestion des risques

- Pourquoi utiliser une méthode
- Gouvernance et gestion des risques
- Introduction à la démarche EBIOS RM
- Cohérence des décisions dans le temps

MODALITES D'EVALUATION

L'évaluation repose sur :

- Des quiz de compréhension à l'issue des modules
- Un quiz final permettant de valider les connaissances acquises.
- Une attestation de suivi est délivrée aux apprenants ayant validé l'évaluation finale.