Sensibilisation à la directive NIS 2

CYBERSÉCURITÉ

Objectifs	Sensibiliser les acteurs concernés aux exigences de la directive NIS 2, en vigueur à partir de 2024 - Comprendre les nouvelles obligations imposées aux entités essentielles et importantes - Anticiper les impacts organisationnels et techniques - Préparer les démarches de conformité dans un contexte de cybersécurité renforcée au niveau européen.
Participants	Responsables cybersécurité / RSSI - DPO - Directeurs généraux ou opérationnels - Responsables conformité ou juridique - Chefs de projet IT / sécurité - Responsables métiers dans des secteurs critiques - Auditeurs internes - Responsables qualité ou risques
Prérequis	Compréhension des enjeux réglementaires européens - gestion des risques - gouvernance SSI - sensibilisation aux opérateurs de services essentiels - culture cybersécurité.
Moyens pédagogiques	1 poste par participant - 1 vidéo projecteur - Support de cours fourni à chaque participant - Ateliers individuels - Modalités d'évaluation : Ateliers (TP) pendant tout au long de la formation et évaluation des acquis tout au long de la formation.
Méthodes pédagogiques	Exposés interactifs et démonstrations – Travaux pratiques individuels et en groupe – Échanges d'expériences et de bonnes pratiques.
Type de formation	Formation présentielle ou distancielle, selon les besoins et les contraintes des participants
Tarif inter-entreprise	2550 € HT
Durée	3 jour(s) - 21 heure(s)

Code : NCI_KR4JA72U

Programme :

Introduction à la directive NIS 2

Origine et objectifs de la directive NIS 2

Différences majeures avec la directive NIS (2016)

NIS 2 dans le contexte de la stratégie européenne de cybersécurité

Qui est concerné ? Typologie des entités (essentielles / importantes)

Nouvelles obligations de sécurité

Gouvernance cybersécurité et implication des dirigeants

Mesures techniques et organisationnelles exigées

Gestion des incidents : détection, signalement, réponse

Gestion des risques fournisseurs et chaîne logistique

Obligations de notification

Délais de signalement des incidents majeurs (24h / 72h)

Contenu des notifications à l'autorité nationale (ANSSI, etc.)

Exemple de scénario de notification à l'ENISA

Responsabilités et sanctions

Responsabilité de la direction générale

Pouvoirs accrus des autorités de contrôle

Sanctions administratives et pénales

Mise en cause personnelle des dirigeants

Mise en conformité NIS 2

Étapes recommandées : audit, cartographie, plan d'action

Intégration dans une démarche ISO 27001 ou RGPD

Coordination avec les dispositifs existants (PCA, PRA, sécurité SI)

Lien avec les politiques sectorielles de cybersécurité (santé, énergie, finance...)

Cas pratiques & exercices

Identification d'une entité soumise à NIS 2

Étude de cas : traitement d'un incident majeur et notification

Exercice : évaluer le niveau de préparation d'une organisation

Analyse d'un plan de gouvernance cybersécurité selon NIS 2

Clôture

Points clés à retenir de la directive

Ressources utiles (ENISA, ANSSI, textes officiels)

Premiers réflexes à adopter pour la mise en conformité

WEDO 365 by NCI

Caen - Paris - Lyon - Rennes - Nantes - Le Havre - Nice - Montpellier - Lille - Toulon

Saint-Etienne - Toulouse - Montpellier - Bordeaux - Grenoble - Le Mans - Tours - Marseille

www.wedo365.fr - commercial@nci.fr - Tél : +33 (0)2 14 99 00 20