

Directive NIS2 : êtes-vous concerné ?

La réglementation européenne de cybersécurité change d'échelle et touche désormais des milliers de PME françaises, directement ou via leurs clients.

10 min de lecture · Niveau Avancé · cyberionis.fr/ressources/nis2

NIS2 est la directive européenne qui impose des exigences de cybersécurité à un périmètre d'entreprises considérablement élargi : de quelques centaines d'opérateurs en France sous NIS1, on passe à plusieurs dizaines de milliers d'entités. Et même les entreprises non concernées directement le deviennent souvent... par leurs clients.

1. Qui est concerné

Sont visées les entités « essentielles » et « importantes » de 18 secteurs : énergie, transports, santé, eau, infrastructures numériques, services informatiques, espace, poste, déchets, chimie, agroalimentaire, industrie manufacturière... Le critère de taille général : à partir de 50 salariés ou 10 millions d'euros de chiffre d'affaires dans un secteur couvert, avec des exceptions qui incluent certaines petites structures critiques.

L'effet le plus large est indirect : les entités régulées doivent sécuriser leur chaîne d'approvisionnement. Une TPE prestataire d'un client soumis à NIS2 se verra imposer des exigences contractuelles de sécurité — questionnaires, audits, clauses. La conformité devient un argument commercial.

2. Les obligations principales

- Gouvernance : la direction est responsable et doit être formée à la gestion des risques cyber
- Mesures de gestion des risques : analyse de risques, sécurité des systèmes, gestion des incidents, continuité d'activité, sécurité de la chaîne d'approvisionnement, chiffrement, MFA, sensibilisation
- Notification des incidents importants à l'autorité nationale : alerte précoce sous 24 h, notification sous 72 h, rapport final sous un mois
- Enregistrement auprès de l'ANSSI pour les entités concernées
- Des sanctions pouvant atteindre 10 millions d'euros ou 2 % du chiffre d'affaires mondial pour les entités essentielles

3. Par où commencer

- Déterminer si vous êtes dans le périmètre (secteur + taille) — l'ANSSI propose un test en ligne (« Mon espace NIS 2 »)
- Vérifier ce que vos clients régulés vont exiger de vous, même hors périmètre
- Faire un état des lieux : la plupart des mesures NIS2 sont... les fondamentaux couverts par nos autres guides
- Documenter : NIS2 exige de prouver, pas seulement de faire
- Suivre la transposition française, qui précise progressivement les obligations et les délais

4. NIS2 et le reste : s'y retrouver dans les sigles

- RGPD : protège les données personnelles — s'applique à tous, quel que soit le secteur
- NIS2 : impose un niveau de cybersécurité global aux entités des secteurs critiques et importants
- DORA : l'équivalent renforcé pour le secteur financier (banques, assurances, et leurs prestataires IT)
- AI Act : encadre les usages de l'intelligence artificielle selon leur niveau de risque
- Cyber Resilience Act : impose la sécurité des produits connectés mis sur le marché européen

BON À SAVOIR

Bonne nouvelle : ces textes se recouvrent largement dans leurs exigences concrètes. MFA, sauvegardes, gestion des accès, réponse à incident, sensibilisation, encadrement des sous-traitants : le socle décrit dans nos guides sert toutes ces conformités à la fois. Construisez le socle une fois, documentez-le, et chaque réglementation devient une déclinaison plutôt qu'un chantier nouveau.

L'essentiel à retenir

- 01 Vérifier votre appartenance au périmètre NIS2 (secteur et taille)
- 02 Interroger vos clients régulés sur leurs exigences fournisseurs
- 03 Former la direction à ses responsabilités cyber
- 04 Mettre en place et documenter les mesures de gestion des risques
- 05 Préparer une procédure de notification d'incident sous 24 h / 72 h
- 06 Suivre la transposition française et ses échéances

Questions fréquentes

Comment savoir avec certitude si nous sommes concernés ?

L'ANSSI propose un test en ligne (« Mon espace NIS 2 ») qui croise votre secteur d'activité et votre taille. En cas de doute — filiales, activités multiples, seuils limites — une consultation juridique tranche. Et même hors périmètre, vérifiez ce que vos clients régulés vont exiger contractuellement : c'est souvent par là que NIS2 arrive dans les PME.

Quelles sont les échéances ? Sommes-nous déjà en retard ?

La directive est en vigueur et la transposition française (loi résilience) déploie progressivement les obligations, avec des délais de mise en conformité s'étalant sur plusieurs années pour les mesures techniques. Le bon réflexe n'est pas la panique mais la trajectoire : enregistrement si vous êtes concerné, état des lieux, puis plan de mise à niveau documenté — les régulateurs valorisent la démarche engagée.

Quel budget représente la conformité NIS2 pour une PME ?

Tout dépend de votre point de départ : une entreprise qui a déjà les fondamentaux (MFA, sauvegardes, EDR, sensibilisation, gestion des accès) est à 70 % du chemin — l'effort restant est surtout de la documentation et de la gouvernance. Une entreprise qui part de zéro doit de toute façon faire ce chemin pour sa propre survie : NIS2 ne fait que fixer une échéance à ce qui était déjà nécessaire.

Que risque concrètement le dirigeant ?

NIS2 introduit la responsabilité personnelle des organes de direction : obligation de formation, d'approbation des mesures de gestion des risques, et possibilité de sanctions visant les dirigeants en cas de manquements graves. Le message du législateur est clair : la cybersécurité est un sujet de direction générale, plus un sujet « du service informatique ».

Pour aller plus loin

ANSSI — Mon espace NIS 2 (test d'éligibilité) — monespacenis2.cyber.gouv.fr

ANSSI — la directive NIS 2 expliquée — cyber.gouv.fr/la-directive-nis-2

Structurer sans vous noyer dans la paperasse ?

Audit, mise en conformité, chartes et sensibilisation des équipes : un accompagnement à la taille de votre entreprise.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr