LIVRE BLANC · ÉDITION JUIN 2026

NIS2 aux *Antilles françaises.*

Qui est concerné, ce que la loi exigera, et comment s'y préparer en 90 jours.

MANNÈV®

INGÉNIERIE NUMÉRIQUE

INGÉNIERIE IA · CARAÏBE

La fenêtre se referme *en 2026.*

La directive européenne NIS2 est le plus grand élargissement d'obligations de cybersécurité jamais imposé aux entreprises et administrations européennes. La France la transpose par la loi dite Résilience, en cours d'adoption finale.

15 000
ENTITÉS CONCERNÉES EN FRANCE, CONTRE ENVIRON 500 SOUS NIS1

10 M€
PLAFOND DE SANCTION, OU 2 % DU CA MONDIAL

24 h
DÉLAI D'ALERTE PRÉCOCE APRÈS UN INCIDENT SIGNIFICATIF

18
SECTEURS D'ACTIVITÉ COUVERTS PAR LA DIRECTIVE

Les départements et collectivités d'outre-mer ne sont pas épargnés. La Guadeloupe, la Martinique, la Guyane et Saint-Martin sont des régions ultrapériphériques de l'Union, où le droit européen s'applique pleinement. Les entreprises antillaises des secteurs visés, et de nombreuses collectivités, devront se conformer aux mêmes exigences que l'Hexagone, avec des contraintes propres au territoire : insularité, dépendance aux liaisons sous-marines, risque cyclonique, rareté des compétences cyber locales.

CE QUE CE DOCUMENT APPORTE

Un état des lieux factuel et sourcé, un autodiagnostic en dix questions, et un plan de mise en route en 90 jours, calibré pour des structures de 10 à 250 personnes.

Où en est la loi, *exactement.*

NIS2, directive UE 2022/2555, a été adoptée le 14 décembre 2022. La date limite de transposition, fixée au 17 octobre 2024, n'a pas été tenue par la France, qui fait l'objet d'une procédure d'infraction européenne. La transposition française passe par le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, qui transpose en un seul texte trois directives, REC, NIS2 et DORA.

DATE	ÉTAPE
14 déc. 2022	Adoption de la directive NIS2 par l'Union européenne.
17 oct. 2024	Date limite de transposition. Non tenue par la France.
15 oct. 2024	Présentation du projet de loi Résilience en Conseil des ministres.
11-12 mars 2025	Adoption du texte en première lecture au Sénat.
10 sept. 2025	Nouvelle version votée en commission spéciale de l'Assemblée nationale.
17 mars 2026	Présentation par l'ANSSI du Référentiel Cyber France, version de travail.
Juil. 2026	Examen en séance publique à l'Assemblée nationale, prévisionnel.
Été 2026	Promulgation attendue, puis décrets d'application et arrêtés techniques, prévisionnel.

LECTURE STRATÉGIQUE

Une période de transition de l'ordre de trois ans est évoquée après promulgation. Attendre serait pourtant une erreur. Les mesures exigées, inventaire, sauvegardes, MFA, gestion d'incidents, demandent des mois de mise en place, et la plateforme d'enregistrement ANSSI est déjà ouverte au pré-enregistrement volontaire. Les organisations qui s'y mettent en 2026 transforment une contrainte en avantage commercial.

Les dates prévisionnelles sont susceptibles d'évoluer selon le calendrier parlementaire. Sources : cyber.gouv.fr, dossier législatif du projet de loi Résilience, FAQ MonEspaceNIS2. Vérifiez l'état du texte au moment de votre lecture.

Suis-je dans *le périmètre ?*

Deux critères se combinent, le secteur d'activité et la taille. La directive distingue les entités essentielles et les entités importantes, soumises aux mêmes obligations de fond mais à des régimes de contrôle et de sanction différents.

CATÉGORIE	SEUILS INDICATIFS	CONTRÔLE
Entité essentielle	250 salariés et plus, ou plus de 50 M€ de CA, dans un secteur hautement critique	A priori et a posteriori
Entité importante	50 salariés et plus, ou plus de 10 M€ de CA, dans un secteur critique ou hautement critique	A posteriori

SECTEURS HAUTEMENT CRITIQUES

Énergie, transports, banques et infrastructures financières, santé, eau potable et eaux usées, infrastructures numériques, gestion des services TIC, administrations publiques, espace.

AUTRES SECTEURS CRITIQUES

Services postaux, gestion des déchets, chimie, agroalimentaire, fabrication de dispositifs médicaux, électronique, machines et véhicules, fournisseurs numériques, recherche.

SPÉCIFICITÉS DU TERRITOIRE

Le projet de loi français intègre les régions, départements, communes de plus de 30 000 habitants et leurs établissements publics. En Guadeloupe, plusieurs communes avoisinent ou dépassent ce seuil. Saint-Barthélemy a un statut particulier vis-à-vis de l'Union, à vérifier dans le texte final. Même hors périmètre direct, une TPE fournisseur d'une entité régulée subira ses exigences contractuelles de sécurité. C'est le principal vecteur d'impact pour le tissu antillais.

Ce que la loi *exigera.*

Trois familles d'obligations pèsent sur les entités régulées, l'enregistrement auprès de l'ANSSI, la gestion des risques, la notification des incidents. Le cœur technique tient en dix mesures minimales.

N°	MESURE	TRADUCTION OPÉRATIONNELLE POUR UNE PME
01	Analyse des risques	Identifier ce qui est vital et ce qui le menace, par écrit
02	Gestion des incidents	Une procédure, qui détecte, qui décide, qui notifie
03	Continuité d'activité	Sauvegardes testées, plan de reprise, gestion de crise
04	Chaîne d'approvisionnement	Exigences cyber dans les contrats fournisseurs
05	Acquisitions et développements	Sécurité intégrée dès l'achat ou la conception
06	Évaluation de l'efficacité	Audits et revues périodiques
07	Hygiène et formation	Sensibilisation de tous, dirigeants inclus
08	Cryptographie	Données sensibles chiffrées, au repos et en transit
09	Sécurité des accès	Comptes nominatifs, droits minimaux, départs gérés
10	Authentification multifacteur	MFA sur messagerie, VPN, comptes à privilèges

GOUVERNANCE, LES DIRIGEANTS EN PREMIÈRE LIGNE

Les organes de direction doivent approuver les mesures de gestion des risques, en superviser la mise en œuvre et suivre une formation à la cybersécurité. Leur responsabilité peut être engagée en cas de manquement. La conformité NIS2 n'est pas délégable au seul informaticien.

Le compte à rebours *et l'addition.*

Tout incident significatif déclenche une obligation de notification à l'autorité nationale selon un calendrier serré, incompatible avec l'improvisation.

24 h

ALERTE PRÉCOCE APRÈS DÉTECTION DE L'INCIDENT

72 h

NOTIFICATION DÉTAILLÉE, ÉVALUATION, GRAVITÉ, IMPACT

1 mois

RAPPORT FINAL, CAUSES, MESURES PRISES, IMPACT

RÉGIME DE SANCTIONS

	ENTITÉS ESSENTIELLES	ENTITÉS IMPORTANTES
Amende maximale	10 M€ ou 2 % du CA annuel mondial, le montant le plus élevé étant retenu	7 M€ ou 1,4 % du CA annuel mondial
Autres mesures	Injonctions, astreintes, audits imposés. La responsabilité des dirigeants peut être recherchée.	

LE VRAI COÛT N'EST PAS L'AMENDE

Pour une PME antillaise, le risque premier reste l'arrêt d'activité. Un rançongiciel immobilise facturation, plannings et paie pendant des semaines, sur un territoire où l'assistance spécialisée est rare et où tout délai logistique s'allonge. La conformité NIS2 est d'abord une assurance de continuité d'exploitation.

Dix questions. *Trente minutes.*

Répondez par oui ou par non, sans complaisance. Chaque non désigne un chantier prioritaire. Basé sur les exigences NIS2 et le guide d'hygiène informatique de l'ANSSI.

01

Savez-vous précisément quels matériels, logiciels et données font tourner votre activité ?

Un inventaire à jour des postes, serveurs, applications et comptes est le préalable à toute sécurisation.

[ ] OUI [ ] NON

02

Vos sauvegardes sont-elles automatiques, externalisées et testées par une restauration réelle ?

Une sauvegarde jamais restaurée est une hypothèse, pas une protection.

[ ] OUI [ ] NON

03

L'authentification multifacteur est-elle active sur la messagerie et les accès distants ?

La compromission de messagerie est la porte d'entrée la plus courante. Le MFA en bloque l'essentiel.

[ ] OUI [ ] NON

04

Chaque collaborateur a-t-il un compte nominatif avec les seuls droits nécessaires ?

Comptes partagés et droits administrateur généralisés transforment toute erreur en sinistre global.

[ ] OUI [ ] NON

05

Vos systèmes sont-ils mis à jour dans un délai défini après publication des correctifs ?

Les attaques exploitent massivement des failles corrigées depuis des mois.

[ ] OUI [ ] NON

06

Sauriez-vous détecter une intrusion, et qui appeler dans l'heure qui suit ?

Sans journalisation ni procédure d'alerte, une intrusion se découvre des semaines trop tard.

[ ] OUI [ ] NON

07

Pourriez-vous notifier un incident à l'ANSSI sous 24 heures, avec les bons éléments ?

C'est l'obligation NIS2 la plus chronométrée. Elle se prépare avant l'incident.

[ ] OUI [ ] NON

08

Vos équipes, direction comprise, ont-elles été sensibilisées depuis moins d'un an ?

NIS2 impose la formation des organes de direction. L'hameçonnage reste le premier vecteur.

[ ] OUI [ ] NON

09

Vos contrats avec prestataires incluent-ils des exigences de sécurité ?

La chaîne d'approvisionnement est une exigence explicite, et le vecteur d'impact principal pour les TPE.

[ ] OUI [ ] NON

10

Survivriez-vous à la perte totale de votre système pendant une semaine, cyclone ou rançongiciel ?

Continuité et gestion de crise sont des mesures NIS2 à part entière, doublement critiques en zone cyclonique.

[ ] OUI [ ] NON

LECTURE DU SCORE

Huit à dix oui, socle solide, formalisez et documentez. Cinq à sept oui, exposition réelle, le plan 90 jours ci-après est fait pour vous. Moins de cinq oui, chaque semaine compte, commencez par les questions 02, 03 et 05.

90 jours pour passer de l'angle mort *au pilotage.*

J1 À J15 · VOIR CLAIR

- [ ] Désigner un référent cybersécurité, même non technique, mandaté par la direction.
- [ ] Inventorier matériels, logiciels, comptes, données critiques et accès distants.
- [ ] Réaliser l'autodiagnostic des pages précédentes et vérifier votre statut sur la plateforme ANSSI.
- [ ] Identifier les trois processus dont l'arrêt stopperait l'entreprise, facturation, paie, prise de commande.

J15 À J45 · FERMER LES PORTES BÉANTES

- [ ] Activer l'authentification multifacteur, messagerie, accès distants, comptes administrateurs.
- [ ] Mettre en place une sauvegarde automatique externalisée selon la règle 3-2-1, puis tester une restauration complète.
- [ ] Passer tous les systèmes en mise à jour automatique ou planifiée, supprimer les logiciels obsolètes.
- [ ] Reprendre la gestion des comptes, nominatifs, droits minimaux, suppression immédiate des partants.
- [ ] Chiffrer les postes nomades et les supports amovibles.

> **RÈGLE DE MÉTHODE**
>
> Aucune de ces mesures ne demande un budget lourd. Toutes demandent une décision et un responsable nommé. La conformité est d'abord une question de gouvernance, ensuite seulement d'outillage.

J45 À J70 · SE PRÉPARER À L'INCIDENT

- [ ] Rédiger une procédure d'incident d'une page, qui constate, qui décide, qui isole, qui notifie, qui communique.
- [ ] Préparer les modèles de notification ANSSI, alerte 24 h, notification 72 h, rapport final un mois.
- [ ] Activer la journalisation sur les équipements critiques et centraliser les alertes.
- [ ] Lister les contacts d'urgence, ANSSI, cybermalveillance.gouv.fr, assureur, prestataires, banque.

J70 À J90 · ANCRER LA GOUVERNANCE

- [ ] Former la direction et sensibiliser l'ensemble des équipes.
- [ ] Intégrer des clauses de sécurité dans les contrats fournisseurs et prestataires.
- [ ] Rédiger un scénario de continuité, perte du système une semaine, mode dégradé, ordre de reprise.
- [ ] Planifier la revue semestrielle, audit du socle, test de restauration, exercice d'incident sur table.

1 page

SUFFIT POUR UNE PROCÉDURE D'INCIDENT UTILISABLE UN DIMANCHE À 22 H

2 / an

REVUES DU SOCLE DE SÉCURITÉ POUR RESTER CONFORME DANS LA DURÉE

Conformité NIS2, une journée *pour démarrer.*

MANNÈV® anime une formation intensive d'une journée, en présentiel sur votre site en Guadeloupe ou à distance pour les autres territoires, conçue pour des dirigeants et des équipes non techniques.

PARAMÈTRE	DÉTAIL
Tarif	800 € HT par participant, trois participants minimum.
Format	Une journée, cas pratiques sur vos propres systèmes et documents.
Programme	Périmètre et obligations NIS2, autodiagnostic guidé, les dix mesures appliquées à votre structure, procédure d'incident et notification, feuille de route 90 jours personnalisée.
Livrables	Support complet, modèles de procédures et de notification, plan d'action daté et attribué.
Public	Dirigeants, DAF, office managers, référents informatiques de TPE-PME et collectivités.

POURQUOI UN SEUL CABINET DE GROUPE SUFFIT

Le minimum de trois participants est pensé pour le tissu antillais. Un cabinet, une PME ou une mairie atteint ce seuil seul, ou en mutualisant avec deux structures voisines. La session devient alors un exercice réel de mise en conformité collective du territoire.

Le contenu s'appuie sur les référentiels publics, directive NIS2, projet de loi Résilience, guide d'hygiène informatique de l'ANSSI, kit cybermalveillance.gouv.fr et version de travail du ReCyF. Il est mis à jour à chaque évolution du texte français.

Un cabinet d'ingénierie, *pas une agence.*

01

Ancré en Guadeloupe

WhatsApp prime sur l'email, les réseaux de confiance sur la publicité. Ces codes s'inscrivent dans chaque livrable.

02

Prix fixes et publics

Cinq offres de 190 à 3 500 € HT, livrables listés, délais contractuels. Aucun coût caché.

03

Propriété totale

Fichiers sources, accès, configuration IA, tout appartient au client à la livraison. Données hébergées chez vous.

04

Vitesse d'exécution

Site livré en 72 heures, agent IA en 5 jours. Communication directe, décisions rapides.

05

Expertise territoriale

Insularité, connectivité, risque cyclonique, conformité NIS2, intégrés à l'architecture de chaque projet.

06

Capacité limitée

Deux missions simultanées maximum. Chaque client a l'attention entière du cabinet.

Lucas Jean · Fondateur

+590 690 32 11 87 · contact@mannev.fr · mannev.fr

MANNÈV® · Baie-Mahault, Guadeloupe · SIRET 902 423 698