NIS2 : Votre feuille de route de conformité

A.CARBONNIER — It Séla

Résumé exécutif

La directive NIS2 (Sécurité des Réseaux et Systèmes d'Information) représente un tournant majeur pour la cybersécurité en Europe. Entrée en vigueur en début 2023, elle élargit considérablement le périmètre des entreprises concernées, incluant désormais les petites et moyennes entreprises.

Les faits essentiels :

- Entre **15 000 et 18 000 entreprises françaises** seront concernées
- Délai de conformité complète : **fin 2027** (3 ans)
- Sanctions financières : jusqu'à **7 millions d'€ ou 1,4 % du CA** pour les Entités Importantes
- Phase 1 (2025-2026) : identification et enregistrement
- Phase 2 (2026-2028) : mise en conformité effective

Chez Séla, nous avons conçu une approche éprouvée : supervision proactive 24/7, architecture de sécurité renforcée, accompagnement expert sur les 20 objectifs de l'ANSSI. Ce guide vous montre comment transformer NIS2 en avantage compétitif en vous appuyant sur une infogérance sécurisée.

1. Pourquoi NIS2 change la donne pour les PME

Depuis deux décennies, les cybermenaces évoluent à un rythme exponentiel. La directive NIS2 reconnaît que la sécurité de l'écosystème numérique européen dépend également de la robustesse des petites et moyennes entreprises.

Pourquoi cette expansion ? Les attaquants n'ont pas de discrimination de taille : une PME peut être la porte d'entrée vers une grande entreprise cliente. Une supply chain compromise affecte l'ensemble du réseau.

Impact concret : Votre PME doit passer d'une posture défensive et réactive à une approche proactive, documentée et contrôlable — exactement ce que Séla apporte via sa supervision 24/7 et sa sécurité intégrée.

Aspect	Avant (NIS 1)	Après (NIS 2)
Périmètre	Grandes entreprises	PME + secteurs importants
Obligations	Générales	Spécifiques et mesurables
Incidents critiques	Informatif	Déclaration 24-72h obligatoire
Responsable désigné	Optionnel	Obligatoire
Sanctions	Modérées	Comparables au RGPD

2. Qui est concerné ?

La directive NIS2 classe les organisations en deux catégories :

Entités essentielles (EE)

Énergie, transports, santé, finance, administration publique, infrastructure numérique

100 % des obligations

Entités importantes (EI)

Fabrication, chimie, agroalimentaire, services IT, télécomunications, PME et ETI de secteurs critiques (< 50 salariés, < 10 M€ CA)

Obligations identiques dans le principe, avec une application proportionnée pour les entités importantes.

Vous êtes concerné si :

- Vous opérez dans secteur listé ci-dessus
- Vous fournissez services critiques (cloud, hébergement, cybersécurité)
- Vous êtes sous-traitant d'une entité essentielle/importante
- Vos systèmes numériques sont critiques pour vos clients

3. Les 20 objectifs de l'ANSSI

Ceci une synthèse Séla inspirée des 20 objectifs :

1

Gouvernance (4 objectifs)

1. Gouvernance cybersécurité au niveau direction/conseil
2. Évaluation des risques formalisée
3. Politique de sécurité écrite
4. Responsable NIS2 désigné

2

Mesures Techniques (10 objectifs)

1. Inventaire actifs et cartographie flux
2. Chiffrement données en transit/repos
3. Authentification forte (MFA)
4. Gestion accès et principes du moins privilège
5. Segmentation réseau
6. Sauvegardes immédiates + tests réguliers
7. Plan de continuité (BCP/DRP)
8. Gestion des correctifs et mises à jour

3

Détection & Réponse (3 objectifs)

1. Système de détection et alertes
2. Plan de gestion des incidents
3. Déclaration incidents à l'ANSSI (24-72h)

4

Ressources Humaines (3 objectifs)

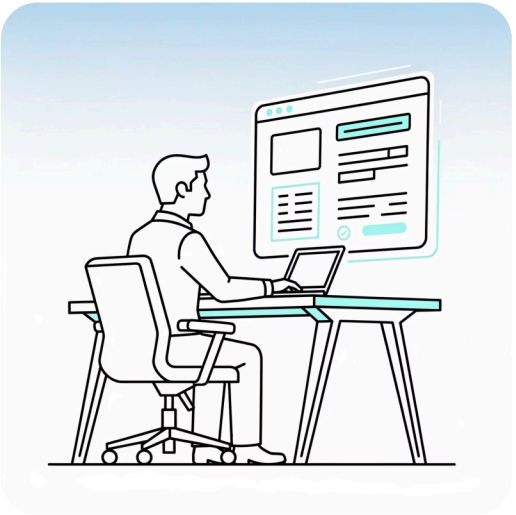
1. Formation cybersécurité continue
2. Tests de sensibilisation (phishing)
3. Chaîne d'approvisionnement sécurisée

Principe clé : Pour les PME (Entités Importantes), les obligations sont adaptées à taille et ressources — proportionnalité, pas égalité.

4. Les 3 phases de mise en conformité

Phase 1 : Identification et Enregistrement (2025-2026)

Objectif : S'identifier formellement auprès de l'ANSSI



Actions :

1. S'enregistrer sur MonEspaceNIS2
2. Désigner responsable NIS2
3. Audit de l'existant : cartographie systèmes, risques, données critiques
4. Documenter point de départ

Délai : Avant fin 2026

Rôle Séla : Cartographie infrastructure, logs actuels, diagnostic sécurité

Phase 2 : Mise en conformité (2026-2028)

Objectif : Déployer mesures et atteindre conformité complète

Actions structurantes :

Gouvernance

Politique écrite, revues régulières

Techniques

Chiffrement, MFA, segmentation, sauvegardes testées

RH

Formation 100% collaborateurs, simulations phishing

Tiers

Audit prestataires critiques, clauses contractuelles

Délai : Avant fin 2028

Rôle Séla (partenaire opérationnel clé) :

- Supervision 24/7 pour détecter anomalies avant incidents (Obj. 15)
- Sauvegardes testées + plan continuité (Obj. 12 & 13)
- Gestion correctifs automatisée (Obj. 14)
- Chiffrement + MFA sur tous accès (Obj. 8 & 9)
- Segmentation réseau et gestion accès (Obj. 11)
- Support cloud sécurisé (Obj. 8)

> Vous gardez maîtrise stratégique, Séla garantit exécution technique quotidienne.

Phase 3 : Contrôle et amélioration continue (2027+)

Audits internes annuels

Tests sécurité (pentest, vulnérabilités)

Simulations d'incidents

Déclaration incidents à l'ANSSI sous 24-72h

Rôle Séla : Audit annuel, reporting conformité, assistance en cas contrôle ANSSI

5. Les risques de non-conformité

Sanctions financières

- Jusqu'à **7 millions d'€ OU 1,4 % du CA annuel** (le plus élevé)
- Escalade graduelle : mise en demeure → injonctions → audits répétés → amendes

Risques commerciaux

- Risque élevé d'être écarté de certains marchés sensibles.
- Perte de confiance et contrats futurs
- Dévaluation commerciale

Impact opérationnel

- Arrêt d'activité en cas cyberattaque non prévue
- Récupération coûteuse (ransomware, perte données)
- Charge administrative : audits répétés, corrections d'urgence

Approche Séla : La supervision proactive réduit significativement le nombre d'incidents majeurs — assurance de rester conforme ET opérationnel.

6. Modèles de mise en conformité

Approche 1 : Interne seul ❌

Ressources : Responsable NIS2 interne + équipe IT existante

Inconvénients : Charge massive, expertise limitée, risque d'erreur réglementaire

Verdict : Non recommandé pour PME

Approche 2 : Hybride ✅ RECOMMANDÉE

Ressources : Responsable NIS2 interne + Séla infogérance + audit spécialisé

Avantages :

- Infrastructure 24/7 ✓
- Expertise NIS2 garantie ✓
- Déploiement sécurisé ✓
- Coût optimisé (paiement échelonné) ✓

Rôle Séla :

Infogérance complète

Infrastructure + supervision 24/7

Cybersécurité & sauvegardes

Mesures techniques NIS2

Cloud & télétravail

Accès sécurisés

Accompagnement

Documentation, audit, escalade incidents

Pourquoi c'est le meilleur choix (modèle choisi par la plupart des PME) :

1. Équilibre optimal : garde-fous réglementaires + efficacité opérationnelle
2. Scalable : coût accessible, s'adapte à croissance
3. Traçable : responsable NIS2 interne reste pilote
4. Garantie : si audit ANSSI, Séla fournit les preuves techniques nécessaires lors d'un audit
5. Flexible : collaboration positive, exit facile

Approche 3 : Entièrement externalisé ⚠️

Ressources : Séla + cabinet spécialisé NIS2 complet

Avantages : Solution clé-en-main, expertise maximale

Inconvénients : Coût élevé, moins de contrôle, dépendance

Verdict : À considérer si PME manque ressources RH complètement

7. Les 10 priorités immédiates (avant fin 2025)

Même avec 3 ans, commencer maintenant = **avantage compétitif + réduction risques**

1

Enregistrement ANSSI

Créer compte MonEspaceNIS2 (avant fin 2025)

2

Audit technique initial

Séla + cabinet spécialisé (T0 + 3 mois)

3

Politique sécurité

Document écrit 3-5 pages (T0 + 2 mois)

4

Inventaire actifs

Registre systèmes/données critiques (T0 + 3 mois) — Séla fournit via CMDB

5

MFA

Déployer sur accès sensibles (T0 + 6 mois) — Séla déploie Azure AD

6

Sauvegarde testée

Immédiates + tests mensuels (T0 + 4 mois) — Séla garantit RPO/RTO

7

Chiffrement

Données repos/transit (T0 + 6 mois) — Séla met en place

8

Formation initiale

100% collaborateurs (T0 + 3 mois)

9

Test sensibilisation

Simulation phishing (T0 + 4 mois)

10

Audit tiers

Prestataires critiques (T0 + 6 mois)

8. Comment choisir votre partenaire d'infogérance

Critères Essentiels :

- **Expertise NIS2 :** expérience cas clients, connaissance 20 objectifs, supervision 24/7 intégrée
- **Infrastructure proactive :** détection anomalies avant incident, sauvegarde immédiate + tests, BCP/DRP documenté
- **Tarif adapté PME :** transparent, échelonné (phases 1/2/3), service à la carte, support réactif
- **Garant conformité :** fourniture documentaire, audit annuel, assistance audit ANSSI, accompagnement complet vers la conformité
- **Guichet unique :** Infogérance + sécurité + cloud + support, un responsable unique

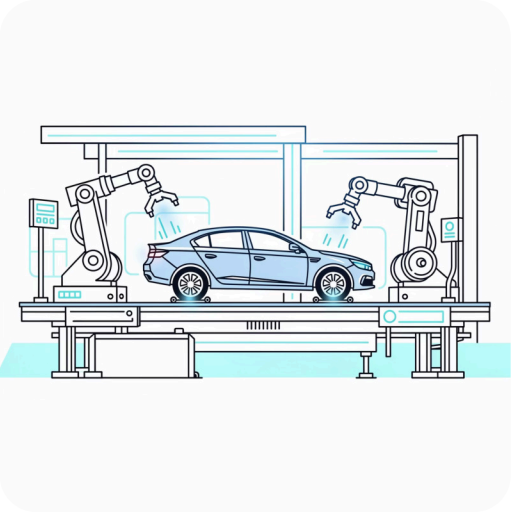
Questions critiques à poser :

1. "Avez-vous des clients conformes NIS2 ? Combien ?"
2. "Supervision détecte-t-elle anomalies avant incidents ? Exemple ?"
3. "Temps de récupération garanti ? Contractualisé ?"
4. "MFA : sur quels accès ? (admin, cloud, email, VPN)"
5. "En cas incident NIS2, qui déclare à l'ANSSI ? Sous quel délai ?"

Benchmark : Séla vs Standard Marché

Critère	Standard	Séla
Supervision 24/7	Option	Incluse
Sauvegarde + tests	Basique	Immédiate + régulière
Chiffrement	À négocier	Standard
MFA cloud	Option coûteuse	Incluse
Récupération garantie	Rare	Contractualisée
Contact unique	Non	Oui
Tarif PME	Élevé	Accessible

9. Cas d'étude : ManuTech (PME manufacturière)



Contexte : Fabrication pièces automobiles — 38 salariés, 4,2M€ CA, 60% clients Tier-1 (Entités Essentielles)

Situation Initiale : Pas responsable cybersécurité, 1 technicien IT débordé, sauvegardes non testées, pas MFA, pas segmentation réseau

Diagnostic NIS2 : 16/20 objectifs non conformes — risques : données vulnérables, arrêt production possible, exclusion marchés

Plan d'action hybride Séla :

T0-3 mois

Audit + documentation + enregistrement ANSSI

T3-12 mois

Déploiement Séla (MFA, sauvegardes testées, supervision 24/7, chiffrement, segmentation) + formation

T12-24 mois

Renforcement chiffrement cloud, tiers-audits, simulations incidents

T24+

Maintenance conformité mode Séla

Résultats (24 mois) :

- Conformité NIS2 attestée (18 objectifs atteints, les 2 restants couverts par proportionnalité)
- Zéro incident malveillant (supervision proactive)
- RPO/RTO contractualisés et garantis
- +3 nouveaux clients (demandaient NIS2-ready)
- Audits clients simplifiés
- Tarif assurance cyber optimisé
- Technicien IT redéployé sur stratégie

ROI : Dans cet exemple, ROI atteignable en année 2 via nouveaux clients + gains assurance

10. Conclusion & prochaines étapes

Pourquoi commencer avant fin 2025

Facteur temps

ANSSI renforce équipes → audits 2026, prestataires saturent *(montée en puissance des contrôles dès 2026)*

Facteur compétitif

Conformité précoce = avantage marché, clients recherchent "NIS2-ready" *(tendance observée dans les secteurs sensibles)*

Facteur financier

Approche progressive échelonnée, budget mieux accepté

Facteur sécurité

Cyberattaques PME +25%/an, supervision 24/7 = protection proactive

5 Points-clés à retenir

1. **NIS2 s'applique vraiment aux PME** — pas de dérogation
2. **Délai 3 ans n'est pas une excuse** — audits ANSSI commencent 2026
3. **20 objectifs ANSSI ne sont pas vagues** — spécifiques et testables
4. **Investissement initial ‹‹ Coût cyberattaque/perte marché** — inaction a un prix bien plus élevé
5. **Partenaire infogérance expert = différence** — supervision 24/7, sauvegardes garanties, MFA transparent

Avantages spécifiques Séla

- **Supervision Proactive 24/7** — anticipe la panne au lieu d'attendre
- **Sauvegardes Testées** — plans récupération garantis
- **MFA Intégré** — accès cloud/admin sécurisés
- **Guichet Unique** — responsable unique, pas tickets multiples
- **Tarif Adapté PME** — abonnement mensuel accessible
- **Approche Hybride** — stratégie interne + exécution technique garantie
- **Audit Annuel Inclus** — conformité vérifiée, pas improvisée

Votre feuille de route

Nov-Déc 2025

- Qualifier statut NIS2 (secteur + taille)
- Créer groupe pilotage (Direction + IT + RH)
- Contacter Séla pour diagnostic initial gratuit ← Démarrage

Jan 2026

Enregistrement MonEspaceNIS2, audit NIS2, signature accompagnement Phase 2

Fév-Juin 2026

Déploiement Séla (MFA, sauvegarde, supervision, formation)

Juil 2026-Juin 2027

Renforcement (chiffrement cloud, tiers-audits, simulations)

Juil 2027+

Audit final, conformité attestée ✓

Votre interlocuteur Séla

Pour démarrer conformité NIS2 :

Email : contact@it-sela.fr

Site : https://it-sela.fr

Téléphone : 03.65.17.00.80

Mentionnez :

Secteur d'activité, salariés, CA

Demande : "Diagnostic NIS2 initial gratuit + approche hybride"

Vous recevrez :

- Diagnostic technique initial (sans engagement)
- Rapport écart vs 20 objectifs ANSSI
- Proposition adaptée
- Planning personnalisé

Références

- [1] ANSSI. (2024). Directive NIS 2 : Recommandations. https://cyber.gouv.fr/directive-nis-2
- [2] Commission Européenne. (2024). Directive NIS2 Texte consolidé. Journal officiel UE, L 321.
- [3] IPSIP Security. (2025). NIS2 : obligations TPE/PME. https://security.ipsip.eu/nis2-obligations-tpe-pme-ipsip/
- [4] SoSafe. (2025). NIS2 : Guide complet 2025. https://sosafe-awareness.com/fr/blog/nis2-obligation-cybersecurite-strategie/
- [5] Orange Cyber Defense. (2025). Recommandations NIS2.
- [6] Séla. (2025). Infogérance Proactive pour PME. https://it-sela.fr

Transformez NIS2 en avantage compétitif avec Séla — votre partenaire de confiance pour une conformité sereine et une cybersécurité proactive.