Directive NIS 2 : Les 6 points essentiels pour comprendre et maîtriser cette réglementation

1 | Pourquoi la Directive NIS 2 ?

- **Renforcer la résilience** des infrastructures critiques face aux cybermenaces.
- **Harmoniser les exigences de sécurité** à travers l'Europe.
- **Encourager la coopération et l'échange** d'informations entre les États membres.

2 | Qui est concerné ?

- **Secteurs critiques :** santé, énergie, transport.
- **Fournisseurs de services numériques.**
- **Administrations publiques et autres services essentiels.**

3 | Principales obligations

- **Gouvernance :** Désignez un responsable de la sécurité des systèmes d'information (SI).
- **Mesures minimales :** IAM, détection des incidents, cryptage des données.
- **Signalement des incidents :**

24h	72h	3 mois
notification initiale	rapport intermédiaire	rapport final détaillé

4 | Phases de mise en conformité

1. **Évaluation des risques :** Identifiez les menaces et actifs critiques.
2. **Politiques de sécurité :** Développez une stratégie documentée.
3. **Gestion des incidents :** Préparez un plan de réponse structuré.
4. **Formation continue :** Sensibilisez votre personnel régulièrement.
5. **Surveillance & audits :** Ajustez vos mesures au fil des menaces.

5 | Conseils pratiques pour les DSI

- **Priorisez les risques** en fonction de leur impact.
- **Automatisez** la gestion des incidents et les contrôles d'accès.
- **Utilisez des référentiels matures** comme ISO 27001 ou les **guides ANSSI.**
- **Préparez des scénarios de crise** avec des fiches réflexes.

6 | Opportunité ou Contrainte ?

La directive **NIS 2** est une **opportunité** pour :

- **Protéger** vos données et infrastructures.
- **Renforcer la confiance** de vos clients et partenaires.
- **Assurer la continuité de votre business** face aux cyberattaques.

Vous souhaitez en discutez avec nos experts ?

Contactez-nous

01 34 80 72 92 sales@tersedia.fr tersedia.fr