AYI NEDJIMI
Consultants

Procédure Gestion des Incidents ISO 27001 Modèle Word [A.5.24-28]

15 mai 2026 • Mis à jour le 17 mai 2026 • 39 min de lecture • 4300 mots •

Télécharger le PDF

> La gestion des incidents (contrôles A.5.24 à A.5.28) suit un workflow normalisé. Ce modèle Word documente le processus complet : détection
> qualificati.

À RETENIR

📥 Template gratuit · Word

La gestion des incidents (contrôles A.5.24 à A.5.28) suit un workflow normal
Ce modèle Word documente le processus complet : détection → qualificatio

containment → eradication → recovery → leçons, avec diagramme d'escalad
délais de notification réglementaires.

📥 Télécharger (Word gratuit)

La **procédure de gestion des incidents de sécurité de l'information** est un docum
fondateur de tout SMSI conforme à la norme **ISO/IEC 27001:2022**. Elle matérialise
contrôle **A.5.24 — Planification et préparation à la réponse aux incidents** et cons
cadre de référence opérationnel pour les contrôles A.5.25 (évaluation des événem
A.5.26 (réponse aux incidents), A.5.27 (leçons apprises) et A.5.28 (collecte de pre
Sans procédure documentée, testée et connue des équipes, la gestion des incide
reste improvisée — avec les conséquences prévisibles sur le temps de réponse, la
de la documentation, et le respect des délais de notification réglementaires. Ce m
Word, développé par **Ayi NEDJIMI**, consultant cybersécurité Lead Implementer ISO
27001, couvre l'intégralité du cycle de vie d'un incident : de la détection initiale d'u
événement suspect jusqu'à la clôture formelle de l'incident et la capitalisation par
leçons apprises. Il intègre un diagramme de flux d'escalade clair, les délais de not
légaux (ANSSI sous 24h pour les OSE NIS 2, CNIL sous 72h pour les violations RG
des fiches réflexe par type d'incident (phishing, ransomware, fuite de données, ac
non autorisé), et les modèles de communication de crise interne et externe. Cette
procédure est indispensable pour les RSSI qui préparent une certification ISO 270
pour les équipes SOC qui gèrent les alertes au quotidien, pour les directions qui d
valider la robustesse du dispositif de réponse à incident, et pour les organisations
soumises à NIS 2 qui doivent démontrer une capacité de réponse opérationnelle a
incidents significatifs. Elle doit être revue au moins annuellement et testée par un
exercice de simulation (tabletop ou full-scale) pour rester pertinente face à l'évolu
des menaces.