



Registre des Incidents ISO 27001 : Template Excel [A.5.24]



15 mai 2026



Mis à jour le 17 mai 2026



41 min de lecture



4340 mots



2 vu



Télécharger le PDF

Le registre des incidents de sécurité (A.5.24 à A.5.28) est obligatoire pour démontrer une gestion structurée. Ce template Excel intègre les délais de

À RETENIR



Template gratuit · Excel

Le registre des incidents de sécurité (A.5.24 à A.5.28) est obligatoire pour démontrer une gestion structurée. Ce template Excel intègre les délais de

notification ANSSI (24h pour OSE) et CNIL (72h RGPD), avec un onglet KPI pour le pilotage mensuel.

 **Télécharger (Excel gratuit)**

Le **registre des incidents de sécurité de l'information** est un document obligatoire pour toute organisation engagée dans une démarche ISO 27001:2022. Les contrôles **A.5.28** de l'Annexe A forment un ensemble cohérent qui encadre la gestion complète du cycle de vie d'un incident : planification et préparation de la réponse (A.5.24), signalement des événements (A.5.25), évaluation et décision (A.5.26), réponse aux incidents (A.5.27), et capitalisation par les leçons apprises (A.5.28). Sans registre structuré, il est impossible de démontrer à un auditeur de certification que votre organisation gère les incidents de manière systématique, traçable et améliorable. Ce template Excel, développé par **Ayi NEDJIMI**, consultant cybersécurité Lead Implementer ISO 27001, répond à l'ensemble de ces exigences en un seul fichier. Il intègre les délais de notification légaux et réglementaires : **24 heures** pour les opérateurs de services essentiels (OSE) soumis à la directive NIS 2 qui doivent notifier l'ANSSI des incidents significatifs, et **72 heures** pour la notification à la CNIL en cas de violation de données personnelles (Article 33 du RGPD). Le registre est conçu pour être utilisable immédiatement par les RSSI, les SOC analysts, les responsables conformité et les auditeurs internes. Il permet de tracer chaque incident depuis sa détection jusqu'à sa clôture formelle, d'analyser les tendances mensuelles grâce aux KPI automatisés, de préparer les rapports de revue de direction, et de constituer le dossier de preuves pour l'audit de certification. La gestion rigoureuse des incidents n'est pas seulement une exigence normative : c'est un levier concret de réduction du risque cyber et d'amélioration continue du SMSI, au cœur de la clause 10 d'ISO 27001.
