Politique Logging & Monitoring ISO 27001 : Word [A.8.15-16]

15 mai 2026 • Mis à jour le 17 mai 2026 • 35 min de lecture • 3355 mots •

17 vues •

> Les contrôles A.8.15 (logging) et A.8.16 (monitoring) imposent la collecte, l'analyse et la conservation des journaux de sécurité. Ce modèle Word défini.

À RETENIR

Template gratuit · Word — Politiques

Les contrôles A.8.15 (logging) et A.8.16 (monitoring) imposent la collecte, l'analyse et la conservation des journaux de sécurité. Ce modèle Word définit les événements à logger par type d'actif, les durées de rétention et les use cases SIEM/SOC.

Télécharger (Word gratuit)

La **politique de logging et monitoring** ISO 27001 est un pilier fondamental de la détection des incidents de sécurité et de la traçabilité des actions dans le Système de Management de la Sécurité de l'Information. Elle répond aux exigences des contrôles **A.8.15 — Journalisation** et **A.8.16 — Surveillance des activités** de l'Annexe A ISO/IEC 27001:2022, qui imposent respectivement que les journaux enregistrant les activités des utilisateurs, les exceptions, les défaillances et les événements de sécurité soient produits, protégés et conservés pendant la durée appropriée, et que les réseaux, les systèmes et les applications soient surveillés pour détecter les comportements anormaux et les événements pouvant indiquer des compromissions. Dans le contexte de la cybersécurité moderne, le logging et le monitoring ne sont plus des activités optionnelles réservées aux grandes organisations : les PME sont tout autant ciblées par des acteurs malveillants sophistiqués, et sans visibilité sur les événements de leurs systèmes, elles sont incapables de détecter une compromission avant que les dommages ne soient irréversibles. Ce template Word, développé par **Ayi NEDJIMI**, consultant cybersécurité Lead Implementer ISO 27001, définit les événements à journaliser pour chaque type d'actif (serveurs Windows/Linux, équipements réseau, applications web, Active Directory, services cloud), les durées de rétention conformes aux exigences légales et aux bonnes pratiques (12 mois minimum pour les logs de sécurité), les cas d'usage SIEM/SOC (use cases de détection couvrant les attaques les plus fréquentes), les procédures de protection des logs contre la modification ou la suppression, et les KPI de surveillance à communiquer en revue de direction. Il s'adresse aux RSSI qui définissent la stratégie de visibilité sécurité, aux équipes SOC et IT qui opèrent les outils de logging et monitoring, aux auditeurs internes qui vérifient la conformité des pratiques de journalisation, et