AYI NEDJIMI Consultants

Politique de sécurité du SI : rédaction et déploiement

Catégorie : Consulting Lecture : 8 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Rédigez et déployez une PSSI efficace et conforme ISO 27001. Structure, validation direction, sensibilisation et maintien dans la durée expliqués.

Résumé exécutif

La politique de sécurité du système d'information constitue le document fondateur qui définit la vision stratégique, les principes directeurs et le cadre organisationnel de la cybersécurité au sein de l'organisation. Ce guide détaille méthodiquement la rédaction, la validation, le déploiement opérationnel et le maintien d'une PSSI efficace et conforme aux exigences normatives et réglementaires actuelles, incluant ISO 27001, NIS 2 et RGPD, en s'appuyant sur les recommandations de l'ANSSI et des retours d'expérience terrain démontrant que la qualité de la PSSI conditionne directement l'efficacité de l'ensemble du dispositif de sécurité de l'information et la capacité de l'organisation à faire face aux menaces cyber contemporaines avec un cadre de référence clair, partagé par tous et opérationnel au quotidien pour l'ensemble des collaborateurs, managers, prestataires et parties prenantes de l'écosystème numérique.

La politique de sécurité du système d'information est trop souvent perçue comme un document administratif poussiéreux, rangé dans un classeur que personne ne consulte jamais après sa rédaction initiale. Cette perception est dangereuse car elle dénature fondamentalement le rôle de la *PSSI* qui devrait être le document de référence vivant et opérationnel encadrant l'ensemble des décisions de sécurité de l'organisation. Une PSSI bien conçue, correctement déployée et régulièrement actualisée constitue le socle sur lequel repose tout le dispositif de cybersécurité : elle définit les **principes directeurs** qui guident les choix techniques et organisationnels, établit les **responsabilités** de chaque acteur dans la protection du patrimoine informationnel, fixe les **règles de sécurité** applicables à l'ensemble des utilisateurs du système d'information et détermine le cadre de **gouvernance** dans lequel s'inscrivent les processus de gestion des risques, de gestion des incidents et de conformité réglementaire. La directive NIS 2 impose explicitement aux entités essentielles et importantes d'adopter des politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information, faisant de la PSSI un livrable réglementaire obligatoire dont l'absence ou l'inadéquation expose l'organisation à des sanctions financières significatives et à une responsabilité personnelle des dirigeants.

Comment structurer une PSSI conforme aux référentiels ?

La structure d'une PSSI efficace s'organise autour de plusieurs sections complémentaires couvrant l'ensemble des domaines de la sécurité de l'information. L'introduction définit le contexte, le périmètre d'application et les objectifs de sécurité alignés sur la stratégie de l'organisation. La section **gouvernance** décrit l'organisation de la sécurité, les rôles et

responsabilités (RSSI, DPO, propriétaires d'actifs, utilisateurs) et les instances de pilotage. La section **gestion des risques** précise la méthodologie retenue (EBIOS RM, ISO 27005) et les critères d'acceptation des risques validés par la direction.

Les sections thématiques couvrent ensuite les domaines de sécurité définis par l'annexe A de l'ISO 27001 : sécurité des ressources humaines, gestion des actifs, contrôle d'accès, cryptographie, sécurité physique, sécurité des opérations, sécurité des communications, acquisition et développement des systèmes, relations avec les fournisseurs, gestion des incidents et continuité d'activité. Pour chaque domaine, la PSSI énonce les principes directeurs et renvoie aux procédures détaillées et aux standards techniques applicables. Cette structure s'aligne naturellement avec les exigences de conformité NIS 2 et facilite les audits de certification ISO 27001.

Votre PSSI date-t-elle de plus de deux ans et reflète-t-elle encore fidèlement les pratiques réelles de votre organisation, ou est-elle devenue un document fantôme que personne ne consulte ?

Quelles sont les erreurs classiques dans la rédaction de la PSSI ?

La première erreur fréquente consiste à rédiger une PSSI trop longue et trop détaillée, mélangeant les principes stratégiques avec les procédures opérationnelles et les configurations techniques. Une PSSI de 200 pages ne sera lue par personne et sera impossible à maintenir à jour. La PSSI doit rester un document stratégique de 30 à 50 pages maximum, renvoyant aux procédures et standards pour les détails opérationnels et techniques. La deuxième erreur est de copier un modèle générique sans l'adapter au contexte spécifique de l'organisation.

La troisième erreur est de rédiger la PSSI en silo technique sans impliquer les directions métier, ce qui produit un document déconnecté des réalités opérationnelles et perçu comme une contrainte imposée par la DSI. La quatrième erreur est l'absence de processus de révision et de mise à jour, transformant la PSSI en document figé qui perd progressivement sa pertinence. La cinquième erreur est de ne pas prévoir de **sanctions graduées** en cas de non-respect des règles de sécurité, privant la politique de tout mécanisme d'enforcement. Ces erreurs compromettent l'efficacité de la PSSI et de l'ensemble du dispositif de protection des données.

Mon avis : La meilleure PSSI que j'ai vue dans ma carrière tenait en 35 pages, était rédigée dans un langage compréhensible par tous les collaborateurs sans jargon technique inutile, et était accompagnée d'une version synthétique de 4 pages distribuée à chaque nouvel arrivant. La pire faisait 280 pages, personne ne l'avait jamais lue en entier y compris le RSSI qui l'avait commanditée, et elle contenait des références à des systèmes décommissionnés depuis trois ans. La sobriété documentaire est un facteur clé de succès.

Comment déployer la PSSI dans l'organisation efficacement ?

Le déploiement de la PSSI est une phase critique qui conditionne l'appropriation effective des règles de sécurité par l'ensemble des collaborateurs et parties prenantes de l'organisation. La première étape est la **validation formelle par la direction générale**, matérialisée par une lettre

d'engagement signée qui confère à la PSSI son autorité et sa légitimité organisationnelle. Sans cette validation visible du top management, la PSSI sera perçue comme un document technique de la DSI sans portée contraignante réelle.

La deuxième étape est la communication et la sensibilisation de l'ensemble des collaborateurs. Le lancement de la PSSI doit faire l'objet d'une communication officielle de la direction, suivie de sessions de sensibilisation adaptées aux différents profils de l'organisation : sessions dédiées pour les managers incluant leurs responsabilités spécifiques, sessions techniques pour les équipes IT couvrant les standards et procédures opérationnelles, sessions générales pour l'ensemble des collaborateurs focalisées sur les règles essentielles au quotidien. Chaque collaborateur doit signer un accusé de lecture attestant sa prise de connaissance des règles de sécurité, en articulation avec le plan de réponse aux incidents.

Section de la PSSI	Contenu principal	Référentiel aligné	Public cible
Introduction et périmètre	Contexte, objectifs, champ d'application	ISO 27001 clause 4	Tous
Gouvernance et organisation	Rôles, responsabilités, comités	ISO 27001 clause 5	Direction, RSSI
Gestion des risques	Méthodologie, critères d'acceptation	ISO 27001 clause 6	RSSI, risk managers
Contrôle d'accès	Authentification, habilitations, revue	ISO 27001 A.5.15-A.5.18	DSI, utilisateurs
Protection des données	Classification, chiffrement, RGPD	ISO 27001 A.5.12-A.5.14	DPO, métiers
Gestion des incidents	Détection, réponse, notification	ISO 27001 A.5.24-A.5.28	SOC, RSSI
Continuité d'activité	PCA, PRI, sauvegardes	ISO 27001 A.5.29-A.5.30	DSI, métiers

L'attaque par ransomware qui a paralysé le CHU de Corbeil-Essonnes en août 2022 a mis en lumière les conséquences d'une politique de sécurité insuffisamment déployée dans le secteur hospitalier. L'enquête post-incident a révélé que malgré l'existence d'une PSSI formelle, les règles de segmentation réseau, de gestion des accès privilégiés et de sauvegarde n'étaient pas effectivement appliquées sur le terrain, illustrant le fossé classique entre politique écrite et réalité opérationnelle que seul un déploiement rigoureux accompagné de contrôles périodiques permet de combler, en lien avec le monitoring du SOC.

Pourquoi la sensibilisation est-elle le pilier du déploiement ?

La sensibilisation des collaborateurs à la sécurité de l'information est le complément indispensable de la PSSI qui transforme un document écrit en comportements réels au quotidien. Le programme de sensibilisation doit être continu, varié dans ses formats et adapté aux profils et aux risques spécifiques de chaque population de l'organisation. Les formats

efficaces incluent les **campagnes de phishing simulées** avec debriefing pédagogique, les modules de e-learning interactifs avec validation des acquis, les ateliers pratiques sur les bonnes pratiques de sécurité et les communications régulières sur les menaces actuelles et les incidents survenus dans le secteur d'activité.

L'efficacité du programme de sensibilisation doit être mesurée par des indicateurs quantitatifs : taux de clic sur les campagnes de phishing simulé (objectif inférieur à 5 pour cent), taux de signalement des emails suspects, taux de complétion des modules de formation obligatoires et nombre d'incidents liés au facteur humain. Ces indicateurs alimentent le tableau de bord du RSSI et sont présentés au COMEX pour démontrer le retour sur investissement du programme de sensibilisation et justifier son maintien dans le temps, comme recommandé par l'ANSSI dans son guide d'hygiène informatique.

Comment maintenir la PSSI dans la durée ?

Le maintien de la PSSI dans la durée exige un processus formalisé de révision et de mise à jour intégré dans le cycle de vie du SMSI. La **révision complète** doit être conduite au minimum tous les deux ans ou lors de changements significatifs affectant l'organisation (nouvelle réglementation, changement d'architecture majeur, acquisition, incident grave). Les **mises à jour mineures** (corrections, précisions, ajout de références) peuvent être apportées en continu selon un processus de gestion documentaire défini, avec validation par le RSSI et information des parties prenantes concernées.

Chaque révision doit faire l'objet d'une analyse d'impact identifiant les conséquences des modifications sur les procédures et standards existants, les besoins de communication et de resensibilisation des collaborateurs et les éventuels investissements techniques nécessaires. Le suivi des révisions et de l'historique des versions est assuré par le système de gestion documentaire du SMSI. La PSSI doit être facilement accessible à tous les collaborateurs via l'intranet de l'organisation et intégrée dans le parcours d'intégration des nouveaux arrivants. La conformité aux prescriptions de l'ENISA pour NIS 2 impose cette rigueur documentaire.

Faut-il adapter la PSSI aux spécificités sectorielles ?

L'adaptation de la PSSI aux spécificités sectorielles est non seulement recommandée mais souvent obligatoire pour les organisations soumises à des réglementations verticales. Le secteur financier doit intégrer les exigences de DORA en matière de résilience opérationnelle numérique et les recommandations de l'ACPR et de l'AMF. Le secteur de la santé doit couvrir les exigences HDS pour l'hébergement des données de santé et les recommandations de l'ANS. Le secteur de la défense et de l'armement doit intégrer les exigences de la LPM et de l'instruction générale interministérielle sur la protection du secret.

L'approche recommandée consiste à construire un **socle commun** de PSSI aligné sur ISO 27001 et NIS 2, puis à ajouter des annexes sectorielles couvrant les exigences spécifiques de chaque réglementation verticale applicable. Cette modularité facilite la maintenance de la politique et

évite la duplication des règles communes tout en garantissant la couverture exhaustive des obligations sectorielles. La PSSI doit être cohérente avec l'ensemble du dispositif de gestion des vulnérabilités et de continuité d'activité.

À retenir : La PSSI est le document fondateur de votre dispositif de cybersécurité et doit être traitée comme tel : validée par la direction, rédigée de manière sobre et accessible, déployée avec un programme de sensibilisation continu, maintenue à jour et contrôlée régulièrement. Une PSSI efficace tient en 30 à 50 pages, est comprise par tous les collaborateurs et se décline en procédures opérationnelles concrètes pour chaque domaine de sécurité.

Sources et références : ANSSI · CERT-FR

Comment contrôler l'application effective de la PSSI ?

Le contrôle de l'application effective de la PSSI est le complément indispensable du déploiement initial, car sans mécanisme de vérification régulier, les règles de sécurité se dégradent progressivement sous la pression des contraintes opérationnelles et de la rotation des équipes. Le programme de contrôle doit combiner des contrôles automatisés continus via les outils de sécurité existants (vérification du déploiement des correctifs, conformité des configurations, activation du MFA), des audits internes périodiques ciblant les domaines à plus haut risque identifiés par l'analyse de risques, et des audits de conformité externes conduits par des tiers indépendants au moins annuellement dans le cadre du SMSI ou de la certification ISO 27001.

Les résultats des contrôles doivent alimenter un processus formalisé de gestion des non-conformités incluant l'analyse des causes racines, la définition d'actions correctives avec des responsables et des échéances, et le suivi de la mise en œuvre jusqu'à la clôture de chaque non-conformité. Le tableau de bord du RSSI doit intégrer des indicateurs de conformité à la PSSI permettant d'identifier les domaines de faiblesse récurrents et d'adapter les actions de sensibilisation en conséquence. La remontée des non-conformités significatives au COMEX démontre la rigueur du dispositif de contrôle et justifie les investissements nécessaires à l'amélioration continue de la posture de sécurité globale de l'organisation.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr