Politique de gestion des vulnérabilités et des correctifs

Politique | Français · Modèle à adapter | v3.0 · 2026-10-16

Version du modèle : 3.0. Type : politique et procédure opérationnelle. Profil d'adaptation proposé : PME d'environ 80 personnes, avec parc utilisateur, services hébergés et exploitation éventuellement confiée à un infogérant. Le profil n'affirme rien sur votre entreprise. Un responsable interne doit garder les décisions de priorité, d'interruption, d'exception et d'acceptation du risque, même lorsque la découverte et le déploiement sont externalisés.

Après adaptation et adoption, les exigences exprimées par « doit » et les consignes ci-dessous s'appliquent au périmètre approuvé. Le propriétaire doit compléter les champs, confirmer moyens et contrats et obtenir une approbation nominative. Cette politique ne garantit ni conformité ni absence de vulnérabilité. Les calendriers proposés doivent être décidés localement ; aucun délai universel de correction n'est introduit.

1. Objet, périmètre et conditions d'adoption

La politique organise la découverte, la qualification, le traitement et la vérification des expositions. Elle concerne systèmes, applications, bibliothèques, équipements réseau, micrologiciels et services retenus dans l'inventaire. Le propriétaire doit distinguer ce que l'entreprise administre, ce que le fournisseur corrige et les paramètres qui restent à sa charge. Le mot « cloud » ne constitue pas une attribution de responsabilité suffisante.

Le périmètre doit préciser terminaux distants, équipements rarement connectés, postes d'administration, sauvegardes, services exposés et composants de développement utilisés. Les systèmes industriels ou sensibles suivent les méthodes approuvées par leurs responsables de sûreté. Une exclusion doit conserver actif, motif, propriétaire et traitement du risque. Aucun système ne doit être retiré de l'inventaire pour améliorer artificiellement un indicateur.

Décision d'adoption	Valeur locale	Autorité	Preuve
Services et actifs couverts	[À RENSEIGNER : inventaires, exclusions, frontières fournisseurs]	Direction technique et métier	Liste rapprochée des contrats
Responsables et remplaçants	[À RENSEIGNER : pilote, exploitation, sécurité, approbateurs]	Direction	Délégations et acceptation
Priorités et engagements	[À RENSEIGNER : niveaux, point de départ, échéances locales]	Autorité de risque	Justification selon exposition et moyens
Fenêtres et urgence	[À RENSEIGNER : cycles, autorisations, arrêt et retour]	Métiers et exploitation	Procédure testée
Version et revue	[À RENSEIGNER : version locale, effet, prochaine revue, signatures]	Propriétaire	Document approuvé et diffusé

Le propriétaire doit faire parcourir un avis jusqu'à sa clôture sur un service représentatif avant de déclarer le processus opérationnel. L'essai doit inclure un échec et une exception. Si l'infogérant ne peut fournir l'état réel de déploiement ou la couverture de l'inventaire, la limite doit être consignée et traitée avant de promettre un niveau de service.

2. Rôles et séparation des décisions

Fonction	Responsabilité	Décision réservée	Absence ou défaut
Propriétaire interne	Tenir périmètre, engagements, exceptions et reporting	Accepter la recette du processus	Suppléant nommé et accès au registre
Sécurité ou MSSP	Qualifier avis, exploitation plausible et priorité	Recommander, sans accepter seul le risque métier	Relais sécurité et escalade contractuelle
Infogérant ou exploitant	Vérifier versions, tester, déployer et rendre les preuves	Changement dans le mandat approuvé seulement	Opérateur autorisé de secours
Propriétaire métier	Évaluer interruption et vérifier service rendu	Accepter fenêtre et résultat fonctionnel	Remplaçant métier désigné
Autorité de risque	Arbitrer report, compensation et retrait	Accepter explicitement le risque résiduel	Délégation prévue, jamais tacite
Achats et gestion fournisseur	Rapprocher support, contrat et capacité annoncée	Engagement externe selon habilitation	Référent de remplacement

Le fournisseur doit recevoir pour chaque campagne actifs, action attendue, fenêtre, contraintes, critères de réussite et mode d'escalade. Le responsable interne doit obtenir l'acceptation de la tâche et des preuves attendues. Un accord commercial global ne dispense pas de vérifier qui peut intervenir sur une application, un équipement ou une dépendance sous contrat distinct.

Si une décision manque, le pilote doit solliciter le remplaçant et enregistrer l'attente. Les mesures préautorisées peuvent être exécutées dans leurs limites ; les autres exigent une décision explicite. Le propriétaire métier doit être informé d'une exposition persistante comme d'un risque d'interruption. L'urgence ne doit pas permettre au fournisseur d'accepter seul ces deux risques.

3. Découvrir et rapprocher les actifs

Le pilote doit rapprocher les inventaires disponibles : gestion des terminaux, annuaire, équipements réseau, hébergement, applications, licences et contrats. Il doit rechercher les actifs connus d'une source mais absents d'une autre. Le résultat doit montrer couverture, date d'observation et catégories non observables. Un actif éteint ou inaccessible ne doit pas être déclaré corrigé ni retiré silencieusement du périmètre.

Pour chaque actif, conserver identifiant stable, service, propriétaire, environnement, version observée, exposition et mode de maintenance. Une dépendance logicielle doit être liée à son application ou image en production. L'équipe doit distinguer version installée, paquet disponible et instance exécutée. Un inventaire déclaré par un outil doit être vérifié sur un échantillon adapté au risque avant d'être utilisé comme référence unique.

Écart de découverte	Action attendue	Preuve	Escalade
Actif sans propriétaire	Rechercher service et responsable ; maintenir visible	Identifiant, sources et tentatives	Direction technique
Versions contradictoires	Vérifier localement ou avec l'éditeur	Méthode et version effective	Sécurité si décision urgente
Terminal distant absent	Contacter son gestionnaire ; organiser retour ou contrôle autorisé	Dernière observation et restriction décidée	Responsable interne
Composant hors support	Confirmer support et options de traitement	Référence fournisseur et plan	Autorité de risque et métier

Les analyses actives doivent avoir un périmètre autorisé, une fenêtre et des consignes d'arrêt. Un système fragile doit utiliser une méthode approuvée par son exploitant. Les résultats doivent indiquer ce qui a été authentifié ou effectivement vérifié. Une analyse sans résultat ne permet pas de distinguer, à elle seule, absence de vulnérabilité, accès insuffisant ou couverture défaillante.

4. Qualifier un avis et décider la priorité

La sécurité doit suivre les avis des éditeurs, les avis du CERT-FR et les autres sources primaires retenues. Le pilote doit conserver référence, version de l'avis, date de consultation et applicabilité envisagée. Une publication révisée doit entraîner le réexamen des constats concernés ; une ancienne capture ne doit pas remplacer la lecture des instructions actuelles.

Le catalogue KEV de la CISA recense des vulnérabilités dont l'exploitation est connue et peut soutenir la priorité. Son absence ne prouve pas qu'une vulnérabilité n'est pas exploitée. Les échéances propres à des organismes ne sont pas automatiquement celles de l'entreprise. L'équipe doit combiner menace, exposition et conséquences, non recopier un délai sans examiner sa portée.

Situation	Qualification à effectuer	Décision proposée	Élément de contrôle
Exploitation observée ou crédible sur actif exposé	Applicabilité, accès, privilèges et signes de compromission	Traitement urgent et examen d'incident	Mesure protectrice et vérification nommées
Vulnérabilité applicable à un service critique	Chemin d'accès réel, protections et impact	Priorité élevée selon risque local	Fenêtre ou compensation explicitement décidée
Actif peu exposé mais défaut confirmé	Dépendances et possibilités de mouvement	Campagne planifiée justifiée	Échéance approuvée, pas oubli
Applicabilité inconnue	Version, configuration et conditions manquantes	Investigation bornée avec priorité conservatoire	Prochaine information, responsable et réexamen

La fiche de priorité doit expliquer pourquoi l'actif peut être atteint, ce que permettrait le défaut et quelles protections ont réellement été vérifiées. Un score technique ne suffit pas à décrire l'impact métier. La sécurité doit distinguer protection supposée et testée. Si l'information manque, le pilote doit choisir une mesure conservatoire ou accepter explicitement l'attente avec l'autorité compétente.

Les cibles locales doivent préciser leur point de départ : détection, confirmation d'applicabilité ou disponibilité d'un traitement. Le registre doit garder ces dates séparées. Une prolongation ne doit pas réinitialiser artificiellement l'ancienneté du constat. Un changement de menace ou d'exposition doit permettre une accélération, même lorsqu'une fenêtre ordinaire a déjà été approuvée.

5. Valider le traitement et préparer un changement

L'exploitant doit confirmer produit, version, configuration, prérequis et dépendances avant de choisir le paquet ou la mesure. Il doit consulter les instructions de l'éditeur et vérifier la provenance et l'intégrité du traitement par les moyens disponibles. Les informations de téléchargement, la version visée et les restrictions connues doivent rester liées au ticket, sans joindre de secrets d'administration.

Le test doit utiliser un périmètre représentatif : service, authentification, accès applicatifs, tâche planifiée, sauvegarde et surveillance lorsque ces éléments sont concernés. L'opérateur doit prévoir les critères d'arrêt et un retour réaliste. Une sauvegarde déclarée réussie ne constitue pas à elle seule une démonstration de restauration. Un retour peut être impossible ou réintroduire la vulnérabilité ; ce risque doit être arbitré avant intervention.

Contrôle préparatoire	Responsable et entrée	Résultat attendu	Échec et décision
Applicabilité	Exploitant ; version et avis	Défaut confirmé ou exclusion motivée	Réexaminer la priorité, sans clôture vide
Provenance du traitement	Exploitant ; canal éditeur	Paquet et vérification identifiés	Arrêter l'installation suspecte

Contrôle préparatoire	Responsable et entrée	Résultat attendu	Échec et décision
Test technique	Opérateur ; environnement et critères	Résultats, version et effets relevés	Correction du plan ou compensation
Validation métier	Propriétaire ; opération représentative	Fonction attendue démontrée	Refus de déploiement large ou mode dégradé décidé

Le pilote doit obtenir un dossier de changement suffisamment précis pour être repris par un autre opérateur : cibles, ordre, durée estimée justifiée, conditions d'arrêt, contacts et contrôle de fin. Les estimations ne sont pas des garanties. Si les compétences nécessaires sont absentes, il doit prévoir le relais ou reporter sous décision de risque, plutôt qu'autoriser une improvisation.

6. Exécuter une campagne ordinaire

Le responsable doit regrouper les actifs selon leurs caractéristiques techniques, criticité et contraintes de maintenance. Les groupes proposés doivent être vérifiés : un ordinateur portable, un serveur métier et un équipement réseau ne partagent pas nécessairement la même méthode. Le pilote doit conserver la liste des membres au démarrage afin de mesurer ce qui a réellement été couvert.

L'opérateur doit commencer par le lot représentatif approuvé, vérifier le résultat puis élargir selon les critères. Les redémarrages, rechargements ou redéploiements nécessaires doivent être inclus dans le changement. Une bibliothèque remplacée dans un dépôt mais non déployée sur les instances actives doit rester un traitement incomplet. Les écarts doivent arrêter l'élargissement lorsque le risque n'est plus maîtrisé.

☐ Confirmer liste, propriétaires, dépendances et fenêtre.

☐ Vérifier accès opérateur, paquet et instructions actuelles.

☐ Confirmer les moyens de secours et les consignes d'arrêt.

☐ Informer les personnes concernées par les interruptions prévues.

☐ Exécuter le lot pilote et conserver résultats et erreurs.

☐ Vérifier version effective et fonction métier avant élargissement.

☐ Enregistrer les actifs réussis, échoués, exclus et non observés.

☐ Affecter les reprises et informer le pilote des réserves.

La fermeture de fenêtre doit produire un état explicite. Un actif éteint ou inaccessible reçoit une action de suivi, pas un succès présumé. Les changements non prévus doivent être expliqués et autorisés selon la procédure applicable. Si un retour a été utilisé, l'exposition résultante et la protection temporaire doivent être vérifiées et suivies séparément.

7. Urgence, exploitation suspectée et traitement sans correctif

En urgence, le pilote doit réunir sécurité, exploitation et métier pour choisir la protection disponible : correction accélérée, restriction d'accès, désactivation d'une fonction ou retrait du service. Il doit documenter menace, impact de la mesure et prochain contrôle. L'absence d'un test ordinaire complet doit être compensée par un test ciblé et une décision explicite, pas masquée.

Une exploitation suspectée doit déclencher la réponse aux incidents. La correction et l'enquête doivent être coordonnées pour préserver les éléments utiles et traiter les accès déjà obtenus. Corriger le défaut ne démontre pas que l'attaquant n'est plus présent. Le pilote doit vérifier qui recherche les traces, qui protège le service et qui autorise sa remise en fonctionnement.

Branche d'urgence	Action minimale	Vérification	Escalade
Correctif disponible et testable	Tester les fonctions essentielles, déployer progressivement si possible	Version et service réels	Échec vers métier et sécurité

Branche d'urgence	Action minimale	Vérification	Escalade
Aucun correctif	Vérifier la mesure de réduction d'exposition proposée	Accès ou fonction effectivement restreints	Risque accepté, échéance et suivi éditeur
Service impossible à arrêter	Définir une exploitation dégradée ou une protection adaptée	Contrôle compensatoire observable	Autorité de risque, pas fournisseur seul
Indice de compromission	Ouvrir incident et coordonner collecte/confinement	Étendue connue et inconnue consignées	Pilote d'incident

Les mesures temporaires doivent avoir un propriétaire et une condition de remplacement. Dès qu'un traitement durable est disponible, le pilote doit décider quand l'appliquer et retirer la compensation devenue inutile. Retirer une restriction sans vérifier le correctif peut réintroduire le risque ; conserver indéfiniment une mesure d'urgence peut aussi dégrader le service.

8. Actifs anciens, exceptions et risque accepté

Un actif hors support ou non corrigeable doit avoir un dossier spécifique : usage indispensable, propriétaire, dépendances, options de remplacement et exposition. L'exploitant doit expliquer pourquoi la correction est impossible et ce qui a été testé. Le métier doit examiner une réduction d'usage ou un remplacement ; « application critique » n'est pas, seul, un argument d'exception suffisant.

Fiche d'exception	Exemple fictif rempli	Valeur vierge	Validation
Actif et contrainte	Passerelle de test ancienne ; logiciel métier incompatible	[À RENSEIGNER]	Propriétaire et preuve
Compensation	Accès limité à un réseau autorisé ; journaux vérifiés	[À RENSEIGNER]	Test et opérateur
Risque accepté	Défaillance de la restriction ou usage hors périmètre	[À RENSEIGNER]	Autorité interne nominative
Sortie et expiration	Remplacement lié au projet métier ; revue avant expiration décidée	[À RENSEIGNER]	Responsable et décision suivante

L'expiration doit être une date locale réelle, à compléter avant approbation. Aucun exemple ne dispense de cette décision. Le propriétaire doit vérifier la compensation à la fréquence approuvée et après changement de menace. À l'échéance, il doit apporter correction, retrait ou nouvelle justification. Le renouvellement tacite et l'acceptation par le seul opérateur sont exclus.

9. Vérifier et clôturer avec des preuves

L'opérateur doit relier chaque actif au constat, au changement et au contrôle effectué. La sécurité doit examiner si la preuve répond au défaut : version active, état de configuration, redémarrage ou analyse autorisée. La clôture doit distinguer correction confirmée, protection temporaire, risque accepté, non-applicabilité démontrée et inconnu. Ces états ne sont pas des succès interchangeables.

Résultat	Preuve requise	Action suivante	Autorité de clôture
Corrigé	Contrôle de l'effet sur la cible réelle	Surveillance des effets secondaires	Propriétaire du processus
Échec	Erreur et état actuel conservés	Reprise ou compensation décidée	Pilote, avec métier si impact

Résultat	Preuve requise	Action suivante	Autorité de clôture
Non applicable	Version ou configuration vérifiée et justification	Réexamen si changement	Sécurité et propriétaire
Inconnu	Absence de contrôle clairement indiquée	Obtenir accès ou autre preuve	Aucune clôture comme corrigé
Protégé temporairement	Mesure vérifiée et limites	Correctif ou retrait planifié	Autorité de risque

Un tableau fournisseur indiquant « installé » doit être rapproché de la population prévue. Le pilote doit rechercher les lignes absentes, doublons et changements de version contradictoires. Les erreurs ne doivent pas être effacées lors d'une nouvelle tentative. L'historique doit permettre de comprendre combien de temps l'actif est resté exposé, sans inventer une date de protection.

10. Scénario fictif de bout en bout

La PME fictive Atelier Rivage utilise un portail distant administré par un infogérant. Un avis primaire concerne une version peut-être présente. Le MSSP signale une exposition plausible ; l'inventaire du fournisseur est ancien. Le pilote interne refuse de traiter l'ancienne liste comme une preuve et demande une observation actuelle. Il s'agit d'un exercice, pas d'un résultat client.

Étape	Décision fictive	Preuve attendue	Critère de réussite
Découverte	Confirmer actif et version effective	Observation liée à l'identifiant du portail	Avis applicable ou exclusion motivée
Priorité	Exposition justifie traitement urgent	Chemin d'accès et limites décrits	Autorité et prochain contrôle nommés
Traitement	Restriction temporaire puis correctif testé	Test de restriction et résultat pilote	Aucun « protégé » sans contrôle
Déploiement	Un nœud réussit, un autre reste inaccessible	Deux états distincts	Campagne non déclarée entièrement réussie
Clôture	Nœud restant vérifié après reprise autorisée	Version active et opération métier	Historique conservé, compensation retirée sous décision

L'exercice est accepté si un remplaçant peut expliquer pourquoi le second nœud n'était pas corrigé, retrouver le risque accepté pendant l'attente et démontrer le contrôle final. Il doit refuser un pourcentage favorable calculé en excluant le nœud inaccessible. Il doit aussi distinguer le traitement de la vulnérabilité et l'enquête sur une exploitation possible.

11. Registres de travail et recette

Constat à compléter	Informations nécessaires	Responsable	Contrôle de fin
Identification	[À RENSEIGNER : avis, révision, actif, version, service]	[À RENSEIGNER]	Applicabilité et couverture
Décision	[À RENSEIGNER : exposition, impact, priorité, échéance]	[À RENSEIGNER]	Justification approuvée
Changement	[À RENSEIGNER : test, fenêtre, ordre, arrêt, retour]	[À RENSEIGNER]	Accord et résultats

Constat à compléter	Informations nécessaires	Responsable	Contrôle de fin
Vérification	[À RENSEIGNER : méthode, date, effet, réserves]	[À RENSEIGNER]	Statut explicitement qualifié
Exception	[À RENSEIGNER : compensation, risque, décideur, expiration]	[À RENSEIGNER]	Revue et sortie

Le propriétaire doit faire tester un avis applicable, un faux positif de version, un actif distant, un échec et un actif ancien. Le remplaçant doit retrouver les décisions et relancer la tâche fournisseur. Toute capacité manquante doit être documentée avant l'adoption. Un outil supplémentaire ne remplace pas l'attribution des responsabilités et la vérification des changements.

12. Assurance, application et révision

Le pilote doit présenter à [À RENSEIGNER : instance et cadence] couverture, constats échus, actifs non observés, exceptions expirantes et traitements non vérifiés. Chaque indicateur doit préciser période, population et source. Les écarts doivent conduire à une correction affectée ou à un risque accepté. Les rapports doivent rendre les inconnues visibles, même lorsqu'elles dégradent l'apparence du résultat.

Une intervention hors autorisation, une fermeture sans preuve ou une exception expirée doit être examinée par le propriétaire. Celui-ci doit définir la protection immédiate, les conséquences opérationnelles et le suivi avec les personnes compétentes. La politique ne crée aucune sanction automatique ; les suites doivent respecter les règles internes et obligations applicables. Le fournisseur doit être associé aux corrections de ses propres écarts.

La révision doit être déclenchée après incident, échec significatif ou changement de technologie, fournisseur ou responsabilités. Auteur, motif, approbation et version remplacée doivent être conservés dans [À RENSEIGNER : dépôt, droits et durée]. Les opérateurs doivent recevoir les nouvelles règles. Les échéances et fréquences doivent être confirmées selon les risques réels, pas simplement reconduites d'un ancien document.

Sources et limites

Le NIST SP 800-40 révision 4, avril 2022, notamment §2.2–2.3 et §3.2–3.6, traite inventaire, réponse au risque, déploiement, vérification, groupes de maintenance et exceptions. Le NIST SP 800-61 révision 3 apporte le contexte de réponse lorsque l'exploitation est suspectée.

Les matrices, rôles, exemples et exigences locales sont une proposition Seculogik, non une reprise normative de ces sources. Les instructions de l'éditeur et contraintes de sûreté doivent être vérifiées au moment d'agir. Aucun outil, prestataire ou pourcentage ne garantit l'absence de défaut ni la disparition d'un accès hostile préexistant.