SÉCURISATION DES USAGES DE L'IA en organisation

Une priorisation pragmatique
des premières mesures

Des mesures de sécurité IA activables, organisées selon trois situations types rencontrées par les RSSI et des responsables cyber :

➜ prise de poste dans une organisation peu mature sur l'IA
➜ explosion des usages et shadow IA
➜ situation d'urgence

CLUSIF

La généralisation rapide des usages de l'intelligence artificielle en organisation, combinée à la montée en puissance des outils grand public et des solutions « Shadow IA », expose les organisations à de nouveaux risques :

fuite de données sensibles
via les prompts,

non-conformité réglementaire
(RGPD, IA Act, droit international
et propriété intellectuelle),

dépendance à des fournisseurs
non maîtrisés,

vulnérabilités techniques spécifiques
(prompt injection, jailbreak, data poisoning,
fine tuning malveillant),

perte de maîtrise
des usages réels.

Ce document, volontairement très synthétique,
propose des premières mesures selon les différentes postures du RSSI

POSTURE 1

RSSI EN PRISE DE POSTE / PRISE EN MAIN DU SUJET

Contexte : maturité faible, volonté de construction pérenne

Dans un contexte de faible maturité, l'enjeu prioritaire n'est pas technique mais structurel, il faut :

- ➜ mettre en place une gouvernance IA claire,
- ➜ définir un cadre d'usage,
- ➜ créer une première visibilité sur les usages existants.

L'objectif est de poser rapidement des **fondations durables** permettant d'éviter l'ancrage de pratiques risquées, de préparer la conformité réglementaire (IA Act, RGPD, droit international) ou contractuelle et d'outiller progressivement la maîtrise des risques IA.

Logique de priorisation

Les mesures prioritaires sont organisées selon une séquence naturelle :

1. **Installer la gouvernance** (comité, charte, politique)
2. **Créer de la visibilité** (cartographie, inventaire)
3. **Évaluer les risques**
4. **Encadrer les usages et la conformité**
5. **Piloter dans la durée** (KPI, amélioration continue)

POSTURE 1 : RSSI EN PRISE DE POSTE / PRISE EN MAIN DU SUJET

Priorité	Catégorie	Mesure
1	Gouvernance IA	Mettre en place un comité de gouvernance IA incluant RSSI, DPO, juridique, achats, métiers clés
2	Gouvernance IA	Définir et formaliser une charte d'utilisation de l'IA et la communiquer immédiatement
3	Formation & Sensibilisation	Sensibiliser puis former les collaborateurs aux enjeux et risques de l'IA et du Shadow IA
4	Visibilité & Inventaire	Cartographier les systèmes d'IA (outils, données, agents, les usages et le propriétaire du système IA)
5	Gestion des risques IA	Évaluer les risques liés aux usages de l'IA
6	Veille & État de l'art	Mettre en place une veille réglementaire et technique IA / Shadow IT
7	Gouvernance IA	Définir et déployer une politique de sécurité de l'IA
8	Données & Confidentialité	Définir les règles d'usage des solutions d'IA (prompts, types de données)
9	Gouvernance IA	Assurer la conformité réglementaire (RGPD, IA Act, etc)
10	Gouvernance IA	Mettre en place des indicateurs IA (KPI / KRI)
11	Données & Confidentialité	Réviser les clauses contractuelles des fournisseurs IA

POSTURE 2

RSSI PRÉVENTION / SHADOW IA

Contexte : pression métier, explosion des usages, besoin de contrôle rapide

Dans cette posture, l'IA est déjà largement utilisée, souvent sans contrôle. Le risque principal est la **perte de maîtrise des usages réels** et l'exposition directe aux fuites de données et à la non-conformité.

L'objectif est de reprendre rapidement de la visibilité, canaliser les usages vers des solutions validées et instaurer des mécanismes de contrôle pragmatiques.

Logique de priorisation

La priorisation repose sur trois axes :

1. **Voir :** identifier les outils et usages existants
2. **Canaliser :** référencer et communiquer les solutions autorisées
3. **Contrôler :** mettre en place une gouvernance et un monitoring léger mais efficace

POSTURE 2 : MESURES PRIORITAIRES « PRÉVENTION / SHADOW IA »

Priorité	Catégorie	Mesure
1	Visibilité & Inventaire	Réaliser l'inventaire des IA utilisées et fournies (interne / externe)
2	Veille & État de l'art	Mettre en place une veille spécifique Shadow IA / Shadow IT
3	Données & Confidentialité	Identifier et référencer les solutions IA validées par l'entreprise
4	Formation & Sensibilisation	Sensibiliser puis former les collaborateurs aux enjeux et risques IA
5	Données & Confidentialité	Réviser les clauses contractuelles / CGU des fournisseurs IA qui peuvent provoquer des difficultés ou limiter les impacts en cas d'incident (support, urgence, astreintes, langue parlée, horaires, SLA, etc.)
6	Gouvernance IA	Suivre l'utilisation réelle des outils IA (prévention des dérives) et bloquer les utilisations non autorisées
7	Gouvernance IA	Déployer une politique de sécurité de l'IA
8	Gouvernance IA	Mettre en œuvre une démarche d'amélioration continue IA
9	Gouvernance IA	Communiquer les solutions IA acceptables pour l'usage professionnel
10	Sécurité technique	Mettre en place des contrôles des entrées / sorties des IA

POSTURE 3

RSSI *POMPIER*

Contexte : crise IA, incident en cours, urgence opérationnelle

Dans un contexte de crise, la priorité n'est plus la structuration mais la **réduction immédiate de l'impact** : stopper les fuites, comprendre rapidement les usages à risque, sécuriser les flux ou organiser la communication et le retour d'expérience.

Logique de priorisation

La séquence suit une logique de gestion de crise cyber classique :

1. **Contenir** (contrôles des flux IA)
2. **Qualifier** (évaluation rapide des risques)
3. **Organiser la réponse** (plan d'incident, communication)
4. **Durcir techniquement** (tests, sécurisation)
5. **Capitaliser** (RETEX)

POSTURE 3 : MESURES PRIORITAIRES « RSSI POMPIER »

Priorité	Catégorie	Mesure
1	Sécurité technique	Mettre en place des contrôles des entrées et sorties des IA
2	Gestion des risques IA	Mettre en place une évaluation rapide des risques pour les usages urgents
3	Sécurité technique	Couper les accès IA concernés, puis collecter et faire analyser les éléments d'investigation
4	Données & Confidentialité	Réviser en urgence les clauses contractuelles des fournisseurs IA
5	Sécurité technique	Mettre en place un plan de réponse à incident IA
6	Communication de crise	Communiquer et sensibiliser sur la crise auprès des parties prenantes
7	Sécurité technique	Réaliser des tests de sécurité IA (pentest, prompt injection, jailbreak)
8	Gouvernance IA	Réaliser le RETEX de la crise

À PROPOS DU CLUSIF

Le Clusif est l'association de référence des professionnels de la cybersécurité et de la sécurité de l'information. Reconnue d'utilité publique, l'association propose à ses adhérents des groupes de travail, espace d'échanges et publications.

Le groupe de travail Utilisation sécurisée de l'IA

Fondé fin 2025, ce GT regroupe des RSSI, juristes, consultants, risks managers… et produit des livrables liés à la sécurisation de l'usage de l'intelligence artificielle en organisation (évaluation des solutions et des implémentations, sensibilisation des collaborateurs, gouvernance de l'IA…)

Animation du groupe de travail :
Alia Saadi (Excube), Quentin Bédéneau (Sanofi), Sabrina M'Hidi (Suez)

Le Clusif adresse ses plus vifs remerciements aux membres du groupe ainsi qu'aux adhérents ayant relu le présent livrable

Pour contribuer aux groupes de travail et aux activités de l'association, rejoignez-nous ! :

clusif.fr

Document à télécharger
et présentation complète

CLUSIF