Piloter plus vite.
Analyser mieux.
Décider avec recul.

PRAESIDIUM, votre plateforme IA locale et sécurisée, capable de rechercher, analyser et synthétiser la documentation technique, administrative et financière.

PROJET PILOTE · 90 JOURS · BANQUE PRIVEE - RESPONSABLE SÉCURITÉ PHYSIQUE

Seeger Consulting
Expertise en sécurité physique, opérationnelle et IT,
enrichie par l'intelligence artificielle locale et responsable.

Le constat terrain

Un chef de la sécurité physique d'une banque privée fait face à un défi structurel : non pas le manque d'information, mais la difficulté à l'exploiter rapidement, proprement et en toute confidentialité.

Procédures dispersées

Des référentiels hétérogènes, des versions non synchronisées, multilingues, une lisibilité documentaire insuffisante.

Mains courantes sous-exploitées

Des données événementielles précieuses, des signaux faibles rarement analysées de façon systématique ou croisée.

Inventaires techniques fragmentés

Équipements, contrats, documentation — éclatés entre services, formats variés, interlocuteurs différents.

Dépendance à la mémoire individuelle

Le savoir opérationnel repose trop souvent sur des personnes clés, sans capitalisation structurée. Rédaction documentaire fastidieuse.

Préparation budgétaire chronophage

Consolider les données techniques, financières et contractuelles prend un temps disproportionné. Pas de visibilité sur plusieurs années.

Cloisonnement entre fonctions

Terrain, technique, gouvernance et direction peinent à partager une vision documentaire commune.

Pourquoi agir maintenant

Dans un environnement bancaire suisse, les exigences de confidentialité, de traçabilité et de justification des choix sont croissantes.

L'IA ne peut y avoir sa place que si elle est locale, gouvernée et strictement contrôlée.

Les enjeux spécifiques à votre contexte

· Confidentialité absolue des informations sensibles
· Risque réputationnel élevé
· Traçabilité des décisions
· Justification budgétaire devant la Direction
· Gestion de l'obsolescence des équipements
· Coordination entre sécurité physique, IT, cybersécurité et conformité.
· Réponse aux audits internes et externes
· Gestion du Plan de Continuité des Activités (PCA)

Le principe fondateur

Une IA locale n'est pas un outil autonome. C'est un système d'analyse au service du responsable sécurité — qui accélère le traitement de l'information, structure les données et soutient la décision.

La décision reste humaine. L'IA sert à accélérer et mieux structurer.

Aucun traitement en cloud public. Aucune exposition externe. Données conservées dans un environnement entièrement maîtrisé.

La solution proposée

Une plateforme d'assistance IA locale et sécurisée, déployée dans votre environnement informatique maîtrisé, conçue pour traiter la documentation sensible sans exposition externe.

LLM privé

Modèle de langage déployé localement — aucune donnée ne quitte l'environnement maîtrisé.

RAG documentaire

Recherche augmentée dans vos propres documents — procédures, contrats, rapports, inventaires. Base de connaissances locale.

Assistants métier

Interfaces spécialisées par profil : sécurité physique, conformité, direction, IT sécurité.

Gestion stricte des accès

Droits par rôle, journalisation complète, séparation des environnements, sources citées à chaque réponse.

Validation humaine

Chaque synthèse, résumé ou analyse reste soumis à validation. L'IA propose, l'humain décide.

Export structuré

Notes de synthèse, rapports d'analyse, comparatifs — produits en format exploitable pour la direction.

Cas d'usage prioritaires du pilote

Six cas d'usage concrets, sélectionnés pour leur impact immédiat sur le quotidien du responsable sécurité physique en banque privée.

Révision des procédures SOPs

Situation : Documents dispersés, versions multiples, multilingues.
Apport : Identification des écarts, consolidation, synthèse des révisions.
Bénéfice : Conformité documentaire accélérée, traçabilité garantie.

Analyse des mains courantes

Situation : Données événementielles peu exploitées.
Apport : Détection de tendances, regroupement thématique, alertes récurrentes.
Bénéfice : Pilotage proactif, rapport d'activité structuré.

Consolidation du parc technique

Situation : Inventaires fragmentés, obsolescence non détectée.
Apport : Consolidation automatisée, signalement des équipements en fin de vie.
Bénéfice : Anticipation des renouvellements, budgets mieux justifiés.

Préparation budgétaire

Situation : Synthèse chronophage de données hétérogènes.
Apport : Extraction et mise en forme des données contractuelles et techniques.
Bénéfice : Gain de temps significatif, scénarios comparatifs prêts pour la direction.

Recherche dans les contrats fournisseurs

Situation : Notices, SLA et conditions dispersées dans des PDF multiples.
Apport : Recherche sémantique instantanée avec citation des sources.
Bénéfice : Réponse rapide aux questions opérationnelles et contractuelles.

Synthèses pour la direction

Situation : Préparation longue et peu standardisée des rapports.
Apport : Génération de synthèses structurées à partir de la documentation existante.
Bénéfice : Communication direction plus fluide, positionnement sécurité renforcé.

Réponse aux audits internes et externes

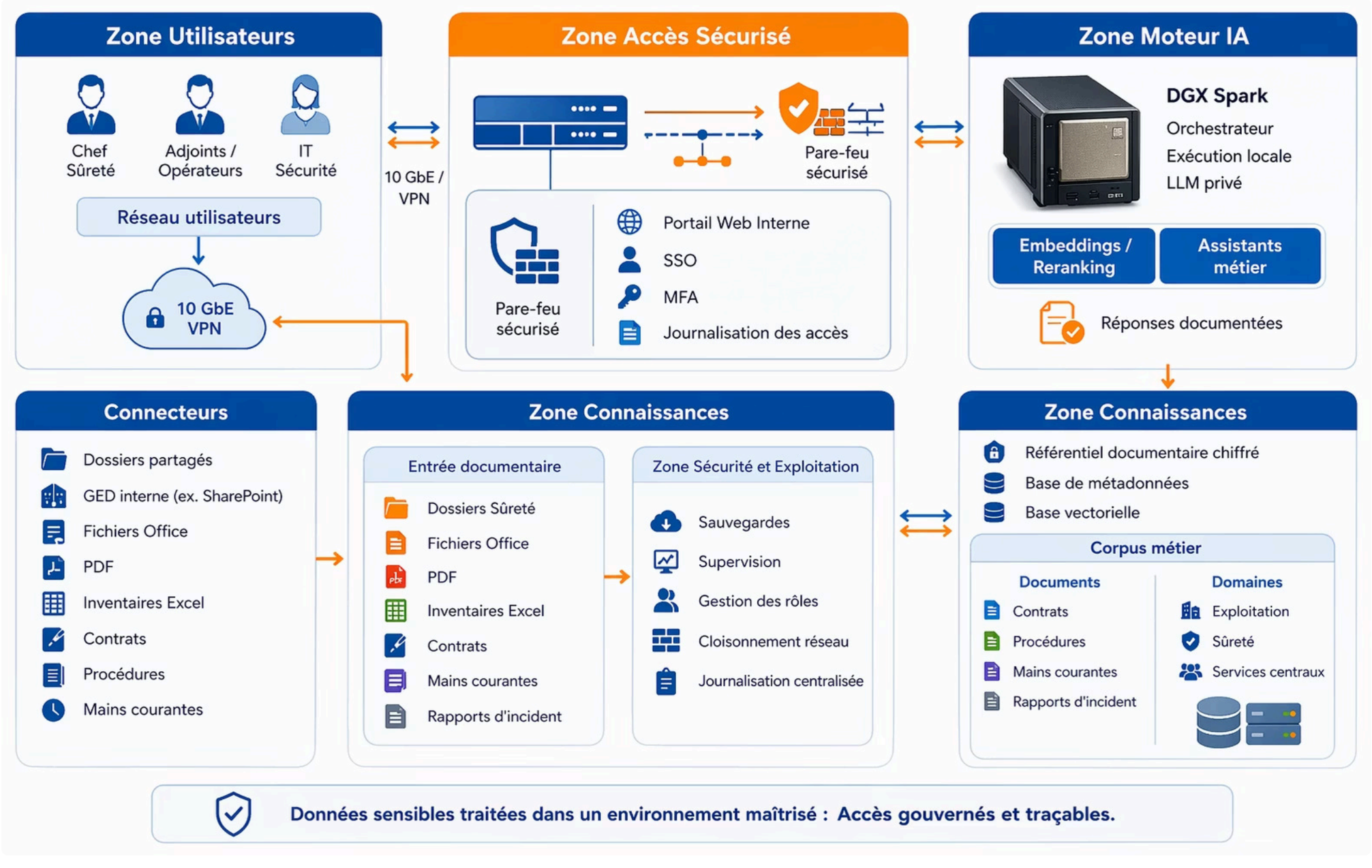
Situation : Préparation chronophage, documents épars, difficultés à retrouver les preuves de conformité.
Apport : Recherche instantanée dans la documentation, génération de synthèses de conformité, traçabilité des actions correctives.
Bénéfice : Réponse aux auditeurs accélérée, dossiers de preuve structurés, crédibilité renforcée.

Plan de Continuité des Activités (PCA)

Situation : Plans PCA volumineux, peu accessibles en situation de crise, difficiles à maintenir à jour.
Apport : Accès rapide aux procédures de crise, identification des écarts entre versions, aide à la mise à jour documentaire.
Bénéfice : Réactivité améliorée en situation d'urgence, conformité PCA maintenue, coordination facilitée.

Architecture cible | Environnement maîtrisé

Une architecture entièrement locale, cloisonnée par zones réseau, sans exposition vers Internet. Chaque flux est journalisé. Chaque accès est géré.



Sécurité, gouvernance et maîtrise du risque

Une IA utile en sécurité physique n'est pas un gadget. C'est une capacité d'analyse intégrée dans un cadre de gouvernance exigeant.

Traitement local strict

LLM déployé sur infrastructure interne. Chiffrement des données au repos et en transit. Aucune dépendance cloud public.

Droits par profil

Accès strictement limités selon les rôles définis. Séparation entre utilisateurs, administrateurs et équipes IT.

Journalisation complète

Traçabilité de chaque action, chaque requête, chaque export. Piste d'audit disponible pour la conformité et la direction.

Sauvegardes et reprise

Plan de sauvegarde défini, procédures de reprise testées, supervision continue de l'environnement.

Validation humaine systématique

L'IA ne décide jamais seule. Chaque analyse, synthèse ou recommandation est soumise à validation explicite.

Gouvernance partagée

Pilotage conjoint entre sécurité physique, IT, cybersécurité et conformité — pour une maîtrise collective du dispositif.

Mise en place sur 90 jours

Un calendrier structuré en quatre phases, conçu pour garantir une montée en puissance maîtrisée, sans perturbation des opérations courantes.

Phase 1 · J1–J15

1

Cadrage

Sélection des cas d'usage · Définition du corpus documentaire · Cartographie des accès · Validation de la gouvernance

Livrable : Cahier de cadrage signé

Phase 2 · J16–J35

2

Architecture & Installation

Déploiement de l'environnement · Sécurisation réseau · Préparation des flux documentaires · Mise en place des accès

Livrable : Environnement opérationnel et sécurisé

Phase 3 · J36–J65

3

Configuration & Tests

Ingestion des documents · Configuration du RAG · Déploiement des assistants métier · Tests qualité et sécurité

Livrable : Plateforme configurée et validée

Phase 4 · J66–J90

4

Pilotage réel

Utilisation sur périmètre limité · Mesure des gains · Ajustements · Restitution et recommandation pour passage à l'échelle

Livrable : Rapport de pilote · Décision de déploiement

Chaque phase fait l'objet d'un point de validation formel avec le responsable sécurité physique et les parties prenantes IT et conformité.

Offre commerciale | Projet pilote

Périmètre du pilote

- **Objectif :** Valider la pertinence métier et la solidité technique de la solution dans votre environnement réel.
- **Périmètre :** 4 à 5 cas d'usage sélectionnés conjointement, corpus documentaire défini et limité.
- **Livrables :** Environnement déployé · Assistants configurés · Rapport de pilote · Recommandations de passage à l'échelle.
- **Critères de succès :** Définis conjointement en phase de cadrage (qualité des réponses, gain de temps, conformité sécurité).
- **Gouvernance :** Comité de pilotage bimensuel · Responsable désigné côté client · Interlocuteur dédié Seeger Consulting.

Conditions de réussite

Disponibilité d'un interlocuteur IT · Accès au corpus documentaire initial · Validation de la gouvernance par la direction · Engagement sur la durée des 90 jours.

Investissement

Forfait pilote 90 jours

CHF 35'000.-

Inclus : cadrage complet, 3 à 4 cas d'usage, structuration documentaire, assistants métier, gouvernance, suivi projet renforcé, restitution + roadmap

Extension possible

À l'issue du pilote validé : déploiement étendu à l'ensemble des périmètres documentaires · nouveaux cas d'usage · gouvernance consolidée · support continu.

Conditions à définir conjointement après restitution du pilote.

Rôle de Seeger Consulting

Chef de projet · Formateur

Rôle de l'Intégrateur externe expert en IA

· Architecte solution · Développement · Intégration

Lancer un pilote ciblé, discret et maîtrisé en 90 jours.

Valeur métier immédiate	Maîtrise totale du risque	Compatible banque privée
Gains concrets sur vos cas d'usage prioritaires dès les premières semaines.	Environnement local, données protégées, gouvernance rigoureuse, validation humaine systématique.	Confidentialité, traçabilité et conformité au cœur du dispositif, dès la conception.

PRAESIDIUM

Transformer les faits en décisions opérationnelles

Seeger Consulting · Votre interlocuteur : **Pascal Seeger | pascal@seegerconsulting.online | 022 575 32 50**
Genève · Expertise sécurité physique, opérationnelle et IT · Assistance IA locale et gouvernée