Skyseat · Folha de segurança

Para responsáveis de TI e de segurança · Última revisão: 1 de novembro de 2026
skyseat.app/pt/confianca

A Skyseat permite a uma empresa ter funcionários IA, cada um com o seu computador na nuvem, as suas permissões e uma pessoa responsável. A Skyseat está em acesso antecipado. Esta folha diz o que existe hoje e, na caixa vermelha, o que não existe.

ONDE ESTÃO OS DADOS

- Plataforma, base de dados e cofre: Hetzner, **Helsínquia, Finlândia**. Computadores dos funcionários IA: Hetzner, Alemanha. A Hetzner tem ISO 27001; nós não operamos centros de dados.
- Existe uma **região dos EUA** construída atrás de um interruptor; será criada quando o primeiro cliente dos EUA precisar.
- Os dados de cada empresa estão separados. Um teste automático tenta cada rota do painel com dados de outra empresa (todas devolvem «não encontrado»); as rotas novas entram sozinhas.
- O modelo de IA (Claude, da Anthropic) e os fornecedores de voz e telefone estão nos **EUA** seja qual for a região; os subcontratantes são públicos, com 30 dias de aviso de alterações.

CIFRAGEM E CHAVES

- HTTPS/TLS em todo o tráfego para a plataforma.
- Credenciais dos serviços ligados: AES-256-GCM num cofre; a chave fica fora da base de dados. O computador de um funcionário IA nunca as vê: a plataforma faz a chamada, verifica a permissão e regista-a.
- Palavras-passe: scrypt, com as palavras-passe comuns rejeitadas. Ninguém define a palavra-passe de outra pessoa (ligações de convite de utilização única).
- Sem chaves geridas pelo cliente (BYOK), HSM nem rotação automática de chaves.

APROVAÇÃO HUMANA

- Por funcionário IA: pergunta antes de tudo, antes do que é sensível ou nunca. Em todos os níveis continuam ativas três salvaguardas: limite de gasto, aviso de IA a terceiros e registo.
- **Quatro olhos:** os pagamentos acima de um valor, as eliminações, os envios em massa ou as alterações de permissões podem exigir duas pessoas diferentes, nenhuma delas a que atribuiu a tarefa. Nunca se autoaprovam nem se aprovam em bloco; uma rejeição bloqueia. Ainda não cobre: alterações de permissões feitas à mão no painel.
- Tudo o que se pede por telefone aguarda a aprovação de uma pessoa.

REGISTO DE ATIVIDADE VERIFICÁVEL

- Registam-se as ações de pessoas e funcionários IA; a base de dados impede editar e apagar. Exportação de qualquer período em PDF, CSV ou JSON, **assinada com Ed25519 e com linhas encadeadas por hash**.
- Um auditor pode verificar uma exportação com um script independente, sem a Skyseat. Prova que o ficheiro não foi alterado depois de exportado; por si só não prova que a base de dados não foi tocada antes.
- A retenção é definida por cada empresa; se for limitada, nunca desce de 2 anos, e cada eliminação fica registada.

IDENTIDADE E ACESSO

- **SSO:** OIDC e SAML 2.0 (Okta, Microsoft Entra ID, Google Workspace, ADFS e outros). Só domínios de email verificados por DNS; pode tornar-se obrigatório.
- Aprovisionamento **SCIM 2.0**: o fornecedor cria, atualiza e remove pessoas; os grupos definem a função (nunca administrador).
- **Verificação em dois passos** (app TOTP + 10 códigos de recuperação de utilização única), exigível a toda a empresa; sempre obrigatória para os operadores da Skyseat. Os códigos errados têm limite por pessoa.
- Funções por empresa (administrador, responsável, só leitura) mais permissões por funcionário IA, verificadas com varrimentos automáticos. Limites de tentativas de acesso por email, por IP e no total.
- Sessões: quem administra define a duração máxima (de 8 h a 30 dias; por predefinição, 30 dias que se prolongam com o uso) e pode terminar as de todos. Cada entrada fica no Registo da empresa. Quem administra vê e revoga cada chave de API que chega à empresa.

CÓPIAS E RECUPERAÇÃO

- Cópia diária cifrada (AES-256) e outra antes de cada implementação, guardadas noutro centro de dados (Falkenstein): 14 diárias + 8 semanais. Teste de restauro automático todas as semanas.
- RPO até 24 h. **Simulacro de desastre de 31 de outubro de 2026:** servidor novo reconstruído só com a cópia externa em 4 min 18 s, com todos os dados legíveis; 20–30 min realistas de ponta a ponta.
- Um servidor de plataforma numa região (ainda sem reserva em funcionamento). Página de estado e monitorização a partir de 4 regiões. **Sem SLA contratual.**

COMO USAMOS A IA

- Cada tarefa envia ao modelo só o que precisa. O que se lê em emails, páginas web ou ficheiros é tratado como informação, não como ordens; as ações sensíveis precisam de aprovação. Não afirmamos que a injeção de instruções esteja totalmente impedida.
- A plataforma (não o funcionário IA) acrescenta o aviso de IA ao email, ao chat, às chamadas e às reuniões; a empresa pode reformulá-lo, mas não retirá-lo.
- **Sem treinar com os seus dados.** A API comercial da Anthropic não treina com o que recebe. A plataforma passará a uma API comercial ou a um plano empresarial antes da disponibilidade geral.

OS SEUS DADOS

- Descarregue-os todos quando quiser; ao encerrar a conta são todos apagados após 30 dias. O acordo de tratamento de dados (art. 28.º do RGPD e um anexo de leis estaduais dos EUA) está redigido e pendente de revisão jurídica; aviso de violação em 48 horas após a detetarmos, para que tenha 72 horas perante a autoridade (rascunho).

O QUE AINDA NÃO TEMOS

- **Nem SOC 2, nem ISO 27001, nem HIPAA, nem PCI, nem FedRAMP.** Está previsto o SOC 2 Type I; não contratámos um auditor e **não há data confirmada**. Existem um mapa de controlos e rascunhos de políticas.
- **Nenhum pentest externo.** Fazemos as nossas próprias revisões de segurança (falhas corrigidas, cada uma com o seu teste) e um teste ligeiro a partir de fora dos nossos domínios públicos; não são independentes.
- As políticas são rascunhos. Sem programa formal de segurança de RH, revisões formais de acessos, DPO nem MDM. Previstas as cópias contínuas de WAL e a reserva em funcionamento. Ainda sem caixa `security@` nem `security.txt`: comunique qualquer falha a partir do painel (Ajuda e suporte, resposta em 1 dia útil).
- Algumas integrações (telefone, email próprio dos funcionários, WhatsApp, Microsoft 365, Google Workspace) continuam em modo de teste. Sem VPAT nem auditoria formal de acessibilidade.

A Skyseat ainda não está constituída; os dados da entidade legal constarão dos documentos do contrato. Esta folha descreve controlos, não é uma declaração de conformidade legal. Um questionário de segurança preenchido (estilo CAIQ / SIG Lite) está disponível a pedido.