

DOCUMENTO TÉCNICO

Planton Genius

Plataforma de **inventário corporativo de emissões** de gases de efeito estufa. Como o sistema opera, onde roda, quem acessa, como o dado de cada empresa fica isolado e o que ele deliberadamente não faz.

01 Visão geral

O Planton Genius é uma aplicação web multiempresa. A equipe do cliente entra pelo navegador, informa os dados de atividade do período (energia, combustíveis, frota, resíduos, viagens, transportes, entre outras categorias), anexa os documentos comprobatórios e submete para revisão interna. A plataforma calcula as emissões com base de fatores versionada e devolve inventário, indicadores e relatórios.

Para a TI do cliente, o ponto de partida é este: **no modo padrão não há integração** — nenhum agente instalado na estação ou no servidor, nenhum coletor, nenhum túnel. Tudo entra pela tela, por pessoas nomeadas e autenticadas individualmente. Quando faz sentido alimentar a coleta a partir de um sistema do próprio cliente — ERP, gestão de frota, medição de energia, portal de faturas —, a integração **é possível hoje** e entra como escopo dedicado do projeto, desenhada caso a caso. Ver seção 04.

MODELO

Software como serviço (SaaS) multiempresa. Cada organização contratante é um inquilino isolado, com seus próprios usuários, unidades e inventários.

HOSPEDAGEM

Oracle Cloud Infrastructure (OCI), região Brasil Sudeste — São Paulo (`sa-saopaulo-1`). Processamento e armazenamento em território nacional.

ENTRADA DE DADOS

Preenchimento pelos usuários do cliente na própria plataforma, com anexo de documentos comprobatórios (contas, notas, extrações de relatório). Integração com sistemas do cliente é possível sob demanda, como escopo dedicado.

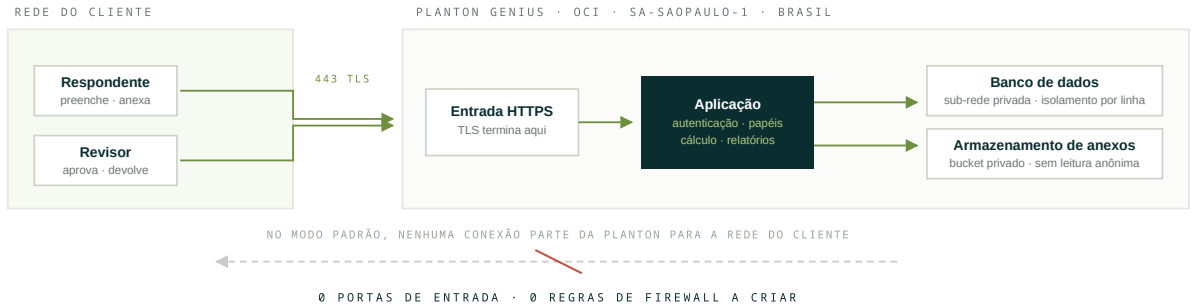
SAÍDA	Inventário por período e unidade, painéis de acompanhamento, relatórios e exportação em PDF e planilha.
AUTENTICAÇÃO	Login individual sem senha, com código de uso único enviado ao e-mail corporativo. Sem certificado digital, sem VPN, sem instalação na estação.
REQUISITO DE REDE	Saída HTTPS na porta 443 e recebimento de e-mail. Nenhuma porta de entrada aberta na rede do cliente.
CLIENTE INSTALADO	Nenhum. Navegador atual (Chrome, Edge, Firefox ou Safari) em desktop.

02 Ciclo de trabalho

Cinco etapas, do inventário configurado ao número publicado. Nenhum resultado é calculado antes de uma aprovação humana do lado do cliente.

01	Configuração do inventário	PLANTON + CLIENTE
	Cadastro da estrutura organizacional (matriz, filiais, unidades), do período do inventário, da metodologia adotada e das categorias de emissão em escopo para cada unidade. Define também quem responde por quê.	
02	Coleta	USUÁRIOS DO CLIENTE
	Cada célula de coleta — categoria × unidade × competência — vira uma tarefa atribuída a um respondente nomeado, com prazo. O respondente preenche o formulário da categoria e anexa o documento comprobatório. O sistema valida unidade de medida, faixa e coerência do período no ato do preenchimento.	
03	Revisão e aprovação	CLIENTE
	O revisor da organização aprova ou devolve com comentário. Nada avança sem aprovação registrada, com autor e data. A devolução volta a tarefa para o respondente, mantendo o histórico da rodada anterior.	
04	Cálculo	PLATAFORMA
	A aprovação dispara o cálculo. Cada emissão guarda a memória de cálculo: o valor de atividade usado, o fator aplicado, a versão da base de fatores, a fonte do fator e a conversão de unidade. Recalcular é reproduzível e rastreável.	

Inventário consolidado por escopo, categoria, unidade e período; painéis de acompanhamento da coleta; exportação para uso externo e para verificação por terceira parte.



Todo o tráfego é iniciado pelo navegador do usuário, de dentro para fora. A seta inferior, riscada, é a conexão que não existe no modo padrão: a Planton não inicia comunicação com a rede do cliente — o que dispensa liberação de entrada, VPN e IP fixo. Integrações contratadas são desenhadas para preservar esse mesmo sentido de tráfego; ver seção 04.

03

Fronteiras do serviço

Boa parte de uma avaliação de risco se resolve sabendo o que o sistema não alcança. Salvo a primeira linha, as ausências abaixo são de projeto — a capacidade não existe, não é configuração desligada.

CAPACIDADE	DETALHE	EXISTE?
Integração com sistemas do cliente	Não vem ligada e não existe por padrão — mas é oferecida sob demanda, como escopo dedicado do projeto, com credencial exclusiva e recorte acordado. Nada é lido da operação sem acordo prévio. Ver seção 04.	SOB DEMANDA
Escrita de volta na operação	Mesmo com integração de entrada contratada, o fluxo é de mão única. Nenhum retorno para ERP, MES, PCP ou sistema de planta: o resultado vive na plataforma e sai por relatório ou exportação.	NÃO
Porta de entrada, VPN ou IP fixo	No modo padrão, nenhuma regra de firewall a criar do lado do cliente. Sem túnel, sem link dedicado. Integração contratada é desenhada para preservar isso.	NÃO
Certificado digital por usuário	Sem TLS mútuo. Nada a instalar, distribuir ou renovar nas estações.	NÃO
Acesso de uma empresa ao dado de outra	O isolamento é aplicado no banco de dados, não apenas na tela. Ver seção 05.	NÃO

CAPACIDADE	DETALHE	EXISTE?
Uso do dado para treinar modelos	O dado é usado apenas na finalidade contratada: coleta, cálculo, revisão e reporte do inventário daquela organização.	NÃO
Decisão automática sem revisão humana	Nenhum número entra no inventário sem aprovação nominal de um revisor da própria organização.	NÃO

04 Infraestrutura e rede

Aplicação web em nuvem, sem componente instalado no parque do cliente. Hospedagem na Oracle Cloud Infrastructure, região Brasil Sudeste — São Paulo. Processamento e armazenamento em território nacional, o que dispensa o enquadramento de transferência internacional de dados na LGPD.

Arquitetura de contêineres em Kubernetes gerenciado, com entrega por GitOps: imagens publicadas em registro privado e aplicadas ao ambiente por controlador de sincronização.

Nenhuma alteração entra em produção por acesso manual a servidor — toda mudança passa por versionamento e fica registrada. A exposição externa acontece por um único ponto de entrada HTTPS; o banco de dados e o armazenamento de anexos não têm endereço público.

Portas e sentido do tráfego

ORIGEM	DESTINO	PORTA	SENTIDO	NECESSÁRIO?
Navegador do usuário	Domínio da plataforma	443/TCP (TLS)	Saída	SIM
Estação do usuário	Resolução DNS pública	53	Saída	SIM
Servidor de e-mail	Caixa corporativa do usuário	e-mail comum	Entrada de e-mail	SIM
Planton (nuvem)	Qualquer host do cliente	—	Entrada na rede do cliente	NENHUMA
Sistema do cliente	API da plataforma	443/TCP (TLS)	Saída	SÓ SE HOUVER INTEGRAÇÃO

A última linha só se aplica a quem contrata integração. Ela mantém o sentido das demais: quem inicia a conexão é o cliente, para fora.

Integração com sistemas do cliente (sob demanda)

O modo padrão é sem integração: o dado entra pela tela. Quando o cliente prefere alimentar a coleta a partir de um sistema próprio — ERP, gestão de frota, medição de energia, portal de

faturas, base de logística —, a integração é possível e entra como escopo dedicado do projeto, desenhada em conjunto com a TI do cliente antes de qualquer implantação.

- **O cliente envia; a Planton não busca.** O arranjo preferencial é o sistema do cliente enviar os dados para a API da plataforma, por HTTPS, sempre de dentro para fora. Nesse formato a rede do cliente continua sem porta de entrada aberta, sem VPN e sem IP fixo — o quadro da seção anterior permanece válido.
- **Alternativa quando o envio não é viável.** Área de arquivo acordada — SFTP ou repositório do próprio cliente — de onde a plataforma lê em janela combinada. O sentido do tráfego, as credenciais e eventuais liberações de rede são definidos no escopo da integração e registrados por escrito antes da implantação.
- **Credencial própria, escopo mínimo.** Cada integração recebe credencial exclusiva daquele cliente, restrita às unidades e categorias acordadas. Nunca é a credencial de uma pessoa, nunca é um acesso amplo, e é revogável isoladamente — revogá-la não afeta o acesso dos usuários.
- **Nada é descoberto sozinho.** Não há varredura, inventário automático de sistemas nem leitura fora do recorte contratado e configurado. O que a integração enxerga é exatamente o que foi acordado.
- **Mesmo rastro, mesma aprovação.** O dado que chega por integração é marcado como tal, com origem, lote e horário, e segue para a mesma revisão e aprovação humana das demais categorias. Integração não pula etapa de aprovação.

PONTO DE ATENÇÃO PARA A TI

O código de login e as notificações de prazo chegam por e-mail. Recomenda-se liberar o domínio remetente da Planton no filtro anti-spam antes do início da coleta — é a causa número um de "não consigo entrar" no primeiro acesso.

05 Identidade e acesso

A autenticação é sem senha. O usuário informa o e-mail corporativo e recebe um código de uso único de seis dígitos, digitado na própria tela. O fluxo é conduzido pelo provedor de identidade central da Planton, por OIDC. É um fator de posse no ato do login: o acesso depende da caixa corporativa, controlada pelo próprio cliente. **Não há senha para vaziar, reutilizar ou envelhecer.**

A sessão é mantida em cookie `httpOnly` e `Secure`, com validade limitada e horizonte máximo absoluto, encerrada no logout. Toda operação de escrita exige um cabeçalho próprio da aplicação, o que fecha a superfície de CSRF — um site de terceiros não consegue disparar uma ação em nome do usuário logado.

Regras de acesso

- **Identidade individual, nunca compartilhada.** Cada pessoa tem o próprio login, vinculado ao e-mail corporativo. Não existe usuário genérico de área.
- **Papel por escopo.** O papel é concedido sobre um escopo — a organização inteira ou uma unidade específica — e vale para os nós abaixo dele na hierarquia. Quem responde pela Filial SP não enxerga a Filial RJ.

- **Menor privilégio, verificado a cada operação.** Permissão de leitura, preenchimento, revisão e administração são distintas. Escrever no dado de uma coleta exige designação explícita naquela campanha, não basta ter o papel.
- **Administração pelo próprio cliente.** Um administrador nomeado pela organização convida, designa e revoga acessos na própria plataforma, sem depender da Planton. Toda mudança de acesso fica registrada com autor e data.
- **Revogação imediata.** Revogar o acesso encerra o vínculo; a sessão em curso perde validade no próximo ciclo de renovação, medido em minutos.

Opções sob demanda

Por padrão o acesso é possível de qualquer lugar, sempre com o código de uso único a cada login — configuração que preserva quem está em home office, viagem ou rede móvel. Controles adicionais entram como escopo de configuração:

OPÇÃO	O QUE FAZ	A CONSIDERAR
Lista de IPs permitidos	Aceita conexões apenas das faixas informadas pelo cliente, bloqueando no ponto de entrada, antes da aplicação.	Acesso fora das faixas passa a falhar, inclusive rede móvel e home office sem VPN. Exige responsável por comunicar mudanças de faixa.
Federação com o provedor de identidade do cliente	Login pelo diretório corporativo do cliente (Entra ID, Google Workspace ou outro provedor OIDC/SAML), aproveitando o MFA já em uso.	Depende de configuração conjunta com a TI do cliente e de um responsável técnico dos dois lados. Avaliado caso a caso.

06 Isolamento entre empresas

A plataforma é multiempresa: várias organizações contratantes convivem na mesma aplicação. O isolamento não depende de o código lembrar de filtrar — ele é **aplicado pelo banco de dados**.

- **Filtragem no banco, por linha.** Toda transação roda com a identidade e a organização do usuário fixadas no contexto da conexão. Políticas no próprio banco de dados restringem, linha a linha, o que aquela transação enxerga. Uma consulta sem contexto válido não devolve dado de outra empresa: ela falha.
- **A organização não vem do cliente.** O vínculo entre usuário e organização é resolvido no servidor a partir da identidade autenticada. Um cabeçalho ou parâmetro manipulado no navegador não muda a empresa em cujo dado a requisição opera.
- **Separação por contexto.** Cada domínio funcional — organização, acessos, inventários, coleta, cálculo — vive em esquema próprio no banco, com fronteiras explícitas entre eles.
- **Anexos com o mesmo recorte.** Documentos comprobatórios ficam em armazenamento de objetos privado, sem leitura anônima. Todo download passa pela aplicação e é autorizado com as mesmas regras da tela.

- **Acesso da equipe Planton.** O suporte técnico tem acesso nominal, individualmente identificado e explicitamente marcado no registro de auditoria — nunca anônimo, nunca em rotina automática de fundo, e restrito às pessoas alocadas no projeto.

07 Proteção do dado

Plano contratual

A confidencialidade é coberta por cláusula específica no contrato de prestação de serviço, com anexo de proteção de dados (LGPD). A cláusula fixa: dados do cliente são confidenciais; uso restrito à finalidade contratada; sem compartilhamento fora da relação de subprocessadores declarada; sem uso dos dados para treinamento de modelos; devolução ou eliminação ao fim do contrato.

Do ponto de vista da LGPD, o dado tratado é predominantemente operacional (consumo, produção, logística). O dado pessoal envolvido se limita ao necessário para operar o acesso — nome, e-mail corporativo e registro de ações do usuário.

Plano técnico

- **Em trânsito.** HTTPS obrigatório com TLS moderno em todo o caminho externo; a terminação acontece no ponto de entrada e o tráfego interno não sai do perímetro da nuvem.
- **Em repouso.** Volumes de banco e de armazenamento de objetos cifrados pela plataforma de nuvem, com chaves geridas pelo provedor.
- **Sem exposição de rede.** Banco e armazenamento vivem em sub-rede privada, sem endereço público e sem rota de entrada da internet. O único caminho até eles é a aplicação.
- **Segredos.** Credenciais e chaves ficam em cofre de segredos do cluster, nunca no código nem em imagem de contêiner, e são rotacionáveis sem alteração de aplicação.
- **Ambientes separados.** Homologação e produção são ambientes distintos, com bancos distintos. Dado real de cliente existe apenas em produção.

Rastreabilidade

Autenticações, mudanças de acesso e ações sobre o dado ficam registradas com identidade, horário e origem, em registro estruturado com identificador único de requisição. No plano do conteúdo, cada célula de coleta carrega o histórico completo — quem preencheu, quem enviou, quem aprovou ou devolveu, com que comentário e quando — e cada emissão calculada guarda a metodologia, a versão da base de fatores e o fator exato aplicado.

Continuidade

O banco de dados tem rotina de backup automática com retenção definida, e o ambiente é reconstruível a partir do repositório de configuração: como a entrega é por GitOps, o estado desejado da infraestrutura está versionado, não depende de servidor montado à mão.

08 Uso de inteligência artificial

A plataforma tem um assistente que apoia o preenchimento: lê os documentos anexados pelo próprio usuário, sugere os valores encontrados e responde dúvidas sobre a categoria em questão. É apoio de digitação e conferência, não uma fonte de verdade.

- **O usuário decide.** Toda sugestão do assistente é apresentada para conferência e pode ser editada ou descartada. O que entra no inventário é o que a pessoa confirmou, e a aprovação continua sendo de um revisor humano.
- **Escopo do dado.** O que trafega para o modelo é o conteúdo dos documentos e do formulário daquela coleta, no momento em que o usuário aciona o assistente. Não há varredura em segundo plano da base do cliente.
- **Fornecedor.** Os modelos de linguagem são consumidos por API corporativa de fornecedor terceiro, sob acordo comercial que veda o uso do conteúdo enviado para treinamento de modelos. O fornecedor consta da relação de subprocessadores do contrato.
- **Rastro.** Cada ação do assistente que altera dado fica registrada como ação do usuário que a acionou, com horário — o rastro de auditoria não distingue-se em qualidade de uma digitação manual.
- **Opcional.** O uso do assistente é habilitado por organização e pode ser mantido desligado sem prejuízo das demais funções.

09 Operação e mudanças

- **Entrega versionada.** Toda alteração de código e de configuração passa por revisão, testes automatizados e esteira de integração contínua antes de chegar a produção. Não há alteração aplicada manualmente em servidor.
- **Homologação antes de produção.** Mudanças relevantes são validadas em ambiente de homologação, com dado fictício, antes da promoção.
- **Observabilidade.** Métricas, registros e alertas centralizados, com painel de erros acompanhado pela equipe. Falhas de aplicação são detectadas por monitoramento, não por aviso do usuário.
- **Suporte e incidentes.** Canal de suporte definido em contrato, com registro de chamados. Incidentes de segurança relevantes são comunicados ao responsável nomeado pelo cliente, conforme o acordado no anexo de proteção de dados.

10 O que a Planton precisa do cliente

ITEM	POR QUÊ	ÁREA TÍPICA
Responsável nomeado para pedir e revogar acessos	É o controle que garante que só a equipe autorizada entra	TI

ITEM	POR QUÊ	ÁREA TÍPICA
Relação de pessoas, com e-mail corporativo e papel	Provisionamento das identidades individuais e da designação por unidade e categoria	TI + área técnica
Liberação do domínio remetente no filtro de e-mail	O código de login e os avisos de prazo chegam por e-mail; sem isso o primeiro acesso falha	TI
Estrutura organizacional e período do inventário	Define as unidades, as categorias em escopo e as competências a coletar	Sustentabilidade
Interlocutor técnico para integração, se houver interesse	Define o sistema de origem, o recorte do dado, o sentido do tráfego e a credencial	TI + área técnica
Definição sobre lista de IPs permitidos	Opcional; se houver interesse, entra como escopo de configuração	Segurança da informação
Interesse em federação com o IdP corporativo	Opcional; muda o fluxo de login e exige configuração conjunta	Segurança da informação