

PEGA® Transformação com *confiança*.

Como o Pega Blueprint gerencia dados,
privacidade e IA com segurança.

— Segurança e privacidade do Pega Blueprint™



Pega GenAI • Blueprint™

Dashboard

RETAIL BANKING • BP-206781

Retail Loan Origination

Select the Case Type to define the workflow details: Secured Retail Loan Application

Case Lifecycle Case Data Model

This case type defines a secured Retail Loan application process, from submission, approval, and disbursement, ensuring efficient communication with applicants. This case type represents the process of handling and approving a secured retail lending products like vehicle loans.

Primary Steps:

Capture Applicant Inf...	Eligibility and Evaluat...	Additional Document...	Loan Amount and Te...	Loan Agreement and ...
- Collect Applicant Information - Collect Financial Information - Collect Collateral Information + Add Step	- Eligibility Check - Credit Check - Validate Financial Documentation - Check Collateral Type - Validate Guarantor's Financial Data - Retrieve Guarantor's Credit Score - Check Guarantor's Eligibility - Offer Risk Reducing Product to client + Add Step	- Additional Documentation Check - Collect Additional Documentation - Collect Collateral - Validate Collateral - Valuation of Collateral - Approve/Reject Loan + Add Step	- Loan Amount Check - Loan Terms Calculation - Loan Terms Approval + Add Step	- Prepare Loan Agreement - Review and Sign Agreement - Approve Loan Disbursement - Update Loan Account Information - Update Collateral Systems - Loan Disbursement - Notify Applicant for Loan Disbursement + Add Step

[Save & Close](#) [Next](#)

Resumo de segurança e privacidade do Pega Blueprint™

Criamos o Pega GenAI Blueprint™ priorizando sua privacidade e segurança. Entendemos que seus processos não são simples diagramas e fluxos de trabalho. São a sua vantagem competitiva.



Acesso gerenciado pela sua empresa

O acesso aos Blueprints pode ser conectado ao logon único da sua empresa.

- O Blueprint gerencia o acesso a dados com controle por função, garantindo que os Blueprints criados permaneçam privados para o criador – a menos que sejam compartilhados ativamente.
- Quando um usuário sai da sua organização, ele perderá acesso aos seus Blueprints quando o status ou as funções dele forem atualizados no provedor de SSO da sua organização.

Nenhuma IA é treinada com seus Blueprints

Prompts, dados e designs nunca usados para treinar modelos de IA.

- O Blueprint usa vários LLMs em seu sistema, inclusive modelos da Anthropic na AWS, o Google Gemini e da OpenAI no MS Azure.
- Todos os LLMs são continuamente controlados, têm seu desempenho testado e usam as melhores práticas do provedor para filtragem de conteúdo.

Os dados permanecem confidenciais

Os detalhes de seus Blueprints são armazenados em um banco de dados criptografado na nuvem.

- Implantado na nuvem na região que faz mais sentido para o seu negócio – EUA, Reino Unido, Ásia-Pacífico ou UE.
- Não compartilhamos nenhum dado entre clientes ou parceiros da Pega.
- O acesso aos Blueprints fica restrito ao seu criador, a menos que sejam voluntariamente compartilhados.
- Somente dados de relatórios em nível de atividade são utilizados pela Pega por pessoal autorizado (endereço de e-mail, horário de criação, nome de criação).

Segurança na nuvem de nível empresarial

Seus dados do Blueprint recebem a mesma proteção completa que nosso ambiente de produção do Pega Cloud, o que inclui:

- Criptografia AES de 256 bits para dados em repouso e proteção HTTPS/TLS para dados em trânsito.
- Monitoramento contínuo com sistemas de proteção contra vírus e prevenção de intrusão baseados em host.
- Centrais de operação de última geração, onde a segurança física e ambiental é levada a sério.
- Proteções integradas contra ataques DDoS e bloqueio automático de endereços IP perniciosos conhecidos.



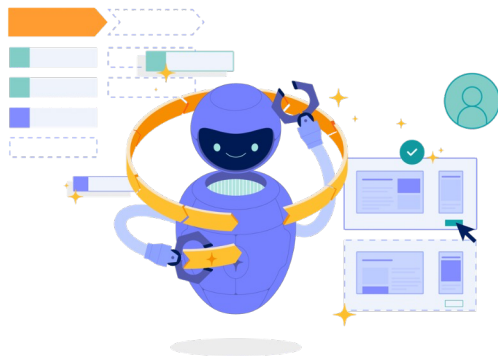
01

O que é o Pega Blueprint?



Combustível para a transformação

O Pega Blueprint desenvolve fluxos de trabalho corporativos com tecnologia de IA, reunindo pessoas e IA para acelerar a automação e turbinar a transformação.



Dashboard Pega GenAI + Blueprint™

RETAIL BANKING • BP-266181

Retail Loan Origination

Select the Case Type to define the workflow details: [Secured Retail Loan Application](#) [Edit Case Type](#) [Settings](#)

Case Lifecycle Case Data Model

This case type defines a secured Retail Loan application process, from submission, approval, and disbursement, ensuring efficient communication with applicants. This case type represents the process of handling and approving a secured retail lending products like vehicle loans. [Edit Lifecycle](#)

Primary Stages

Capture Applicant Inf...	Eligibility and Evaluat...	Additional Document...	Loan Amount and Te...	Loan Agreement and ...
- Collect Applicant Information - Collect Financial Information - Collect Collateral Information + Add Step	- Eligibility Check - Credit Check - Validate Financial Documentation - Check Collateral Type - Validate Guarantor's Financial Data - Retrieve Guarantor's Credit Score - Check Guarantor's Eligibility - Offer Risk Reducing Product to Client + Add Step	- Additional Documentation Check - Collect Additional Documentation - Collect Collateral - Validate Collateral - Valuation of Collateral - Approve/Reject Loan + Add Step	- Loan Amount Check - Loan Terms Calculation - Loan Terms Approval + Add Step	- Prepare Loan Agreement - Review and Sign Agreement - Approve Loan Disbursement - Update Loan Account Information - Update Collateral Systems - Loan Disbursement - Notify Applicant for Loan Disbursement + Add Step

[Save & Close](#) [Next](#)



Onde entra o Blueprint no SDLC?

Design rápido para acelerar o desenvolvimento



Pega Blueprint™	Pega Infinity™ Pega App Studio	Pega Infinity™ Pega Deployment Manager	Pega Infinity™ -	Pega Infinity™ Pega Process Mining
Colaboração de negócios e TI para acelerar o design inicial do fluxo de trabalho com GenAI.	Configuração detalhada de integração, automação e mais, para transformar Blueprints em aplicativos completos	Funis de DevOps automatizados orquestram o processo do início ao lançamento, incluindo testes, aprovações, verificações de segurança e muito mais	Experiência de usuário protegida para acesso aos fluxos de trabalho (bloqueios com controles baseados em função e acesso)	Análise os fluxos de trabalho para descobrir lacunas e ineficiências do processo
Sem PII*	Sem PII*	Sem PII*	Potencialmente sensível	Potencialmente sensível
Operado com segurança no Pega Cloud®	Implantação em cliente privado	Implantação em cliente privado	Implantação em cliente privado	Operado com segurança no Pega Cloud®

*Com base em casos de uso de tempo de design, não é aconselhável gerenciar PII nessas fases

02

Arquitetura do Blueprint



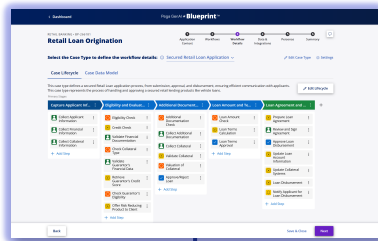
Arquitetura do Pega Blueprint™

O Blueprint é executado com segurança no Pega Cloud® na AWS, com gestão e operação baseadas nos [padrões de nuvem mais avançados](#).

Arquitetura de alto nível:

- A autenticação do Blueprint conecta-se ao protocolo de login único (SSO) da sua empresa.
- A Pega oferece serviços de residência de dados segmentados geograficamente específicos para os produtos Pega Cloud. A região geográfica do Blueprint é baseada na localização da sua empresa ([dentro dos EUA, Reino Unido, União Europeia, Austrália, Singapura ou Japão](#)).
- O processamento do Blueprint é executado em um aplicativo Pega Infinity seguro e confiável, totalmente respaldado pela força operacional dos serviços Pega Cloud, oferecendo [confiabilidade](#), [conformidade](#), [segurança](#) e [recuperação de desastres](#) de nível empresarial.
- O Blueprint usa LLMs de acordo com o caso de uso e desempenho. Principalmente modelos Claude rodando no [AWS Bedrock](#).
- Nenhuma IA é treinada com os dados de seus Blueprints.
- Os dados dos Blueprints são [criptografados em trânsito](#) com TLS.
- Os dados dos Blueprints são [armazenado com segurança](#) e [criptografados em repouso](#).

Pega.com/pt-br Aplicativo web de front-end



Pega.com/pt-br
Serviço de
autenticação

Seu
SSO

Seu funcionário
{usuário}@{sua-empresa}.com



Totalmente isolado **por região** para:
EUA – UE – AUS



Aplicativo Blueprint

Processamento central de solicitações de usuários e funções do Blueprint

Desenvolvido no Pega Infinity™



Serviço de conhecimentos do setor

Serviço de geração aumentada por recuperação (RAG), que fornece informações sobre as melhores práticas de fluxo de trabalho e modelo de dados com base nas solicitações dos usuários.

Desenvolvido no Pega Knowledge Buddy™. Contém PI setorial da Pega.
Não armazena nenhum dado de clientes ou usuários.



Serviço de orquestração de IA Pega Cloud

Orquestra chamadas para LLMs

Desenvolvido na AWS. Não armazena prompts, dados de clientes ou dados de usuários.



AWS Bedrock
Provedor de LLM principal
Claude Haiku & Sonnet



Google
Gemini
Flash



Azure
OpenAI
GPT

Vários LLMs adotados conforme o caso de uso/desempenho. Todo o processamento dentro da região.
Nenhuma IA treinada com dados de usuários ou da empresa.



Armazenamento seguro de dados

Criptografia de dados em repouso (DARE) privada corporativa

Todos os dados do cliente armazenados em volumes, bancos de dados criptografados com criptografia de 256 bits. Por padrão, as chaves de criptografia são alteradas regularmente e armazenadas com segurança em um KMS seguro compatível com FIPS 140-2.
Chaves de criptografia privadas corporativas disponíveis mediante solicitação.



Armazenamento privado de arquivos

Conecte seu repositório Pega Cloud

Todos os arquivos relacionados às atividades do Blueprint, como documentação e vídeos carregados, são armazenados em uma pasta privada da empresa no Pega Cloud File Storage. Por padrão, são gerenciados, em nome da empresa, pelo Blueprint. Os arquivos relacionados ao Blueprint de clientes do Pega Cloud são armazenados, por padrão, no repositório privado existente do Pega Cloud File Storage associado à instância do Pega Cloud deles.

Residência regional de dados do Pega Blueprint™ (UE, Reino Unido, EUA)

Empresas situadas na

União Europeia

- Armazenamento e computação: **AWS EU-Central (Frankfurt)**
- [Execução do Modelo de IA](#)

Empresas situadas no

Reino Unido

- Armazenamento e computação: **AWS EU-Central (Frankfurt)**
- [Execução do Modelo de IA](#)

Empresas situadas

em todo o mundo

- Armazenamento e computação: **AWS US-East**
- [Execução do Modelo de IA](#)

Fornecedor	Modelo/ provedor	Regiões LLM
 AWS Bedrock Provedor principal	Anthropic	AWS Bedrock: União Europeia
 Google Cloud	Gemini	Google Vertex: União Europeia
 Microsoft Azure	OpenAI GPT	Microsoft Azure: União Europeia

Fornecedor	Modelo/ provedor	Regiões LLM
 AWS Bedrock Provedor principal	Anthropic	AWS Bedrock: União Europeia
 Google Cloud	Gemini	Google Vertex: União Europeia
 Microsoft Azure	OpenAI GPT	Microsoft: União Europeia

Fornecedor	Modelo/ provedor	Regiões LLM
 AWS Bedrock Provedor principal	Anthropic	AWS Bedrock: Estados Unidos
 Google Cloud	Gemini	Google Vertex: Estados Unidos
 Microsoft Azure	OpenAI GPT	Microsoft Azure: Estados Unidos

Para Parceiros da Pega

Defina em nome de qual empresa você vai criar um Blueprint no campo de nome da organização, na página de descrição funcional do Blueprint. Esses Blueprints serão armazenados e gerenciados na região em nome dessa empresa, automaticamente.

Como saber em qual região um Blueprint está armazenado

Confira o ID do Blueprint: há um identificador regional que indica se ele está armazenado e gerenciado em UE, AU, Reino Unido, JP ou SG.

Residência Regional de Dados do Pega Blueprint™ (APAC)

Empresas situadas na

Austrália

- Armazenamento e computação: **AWS: Austrália - Sydney**
- [Execução do Modelo de IA](#)

Empresas situadas no

Japão

- Armazenamento e computação: **AWS: Japão - Osaka**
- [Execução do Modelo de IA](#)

Empresas situadas em

Singapura

- Armazenamento e computação: **AWS: Singapura**
- [Execução do Modelo de IA](#)

Fornecedor	Modelo/pr ovedor	Regiões LLM
 AWS Bedrock Provedor principal	Anthropic	AWS Bedrock: Austrália
 Google Cloud	Gemini	Google Vertex: Austrália
 Microsoft Azure	OpenAI GPT	Microsoft Azure: Austrália

Fornecedor	Modelo/pr ovedor	Regiões LLM
 AWS Bedrock Provedor principal	Anthropic	AWS Bedrock: Japão/APAC
 Google Cloud	Gemini	Google Vertex: Japan
 Microsoft Azure	OpenAI GPT	Microsoft Azure: Japão / União Europeia

Fornecedor	Modelo/pr ovedor	Regiões LLM
 AWS Bedrock Provedor principal	Anthropic	AWS Bedrock: APAC
 Google Cloud	Gemini	Google Vertex: Singapore
 Microsoft Azure	OpenAI GPT	Microsoft Azure: União Europeia

Para Parceiros da Pega

Defina em nome de qual empresa você vai criar um Blueprint no campo de nome da organização, na página de descrição funcional do Blueprint. Esses Blueprints serão armazenados e gerenciados na região em nome dessa empresa, automaticamente.

Como saber em qual região um Blueprint está armazenado

Confira o ID do Blueprint: há um identificador regional que indica se ele está armazenado e gerenciado na UE, AU, Reino Unido, JP ou SG.

03

Acesso e autenticação



Acesso e autenticação no Pega Blueprint™

Configure o acesso ao Blueprint com seu login único (SSO).

Ao permitir que os usuários se autentiquem no IDP da sua organização, você garante que apenas usuários autorizados acessem TODOS os sites e aplicativos da Pega, como Blueprint, My Support Portal, etc.

Quando a autenticação federada está ativada, no login, os usuários não precisam fornecer uma senha e são redirecionados para autenticação em seu provedor de identidade.

A área de TI da organização do cliente pode colaborar com nossa equipe de contas integradas para habilitar a autenticação federada.

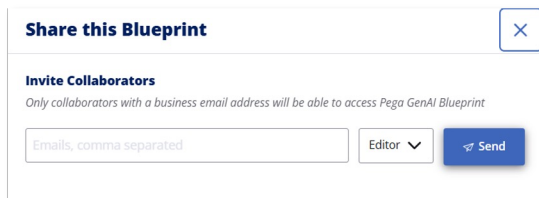
O que precisamos de você: **dados da configuração SAML 2.0** ou **dados da configuração do OAuth**

O login nos seguintes aplicativos será por autenticação federada: Blueprint, Pega.com, community.pegacom, academy.pegacom, support.pegacom, docs.pegacom, partners.pegacom, saleshub.pegacom, partner-logo-generator.pegacom, My Support Portal, My Pega Cloud, My Pega, PDC, Deployment Manager, Pega Trials

Os Blueprints são visíveis apenas para o criador, a menos que sejam compartilhados ativamente.

Por padrão, os Blueprints só podem ser vistos pelo usuário que os criou (o *proprietário* do Blueprint).**

Os proprietários de Blueprints podem compartilhar o Blueprint com outros interessados (colegas de equipe, parceiros, etc.). Eles podem convidar usuários por e-mail como *Editores* ou *Visualizadores*.



Quando um usuário sai da sua organização, seus Blueprints não saem com ele.

Se uma empresa tiver federado seu SSO com propriedades digitais da Pega (por exemplo, Blueprint), somente os usuários com acesso ativo ao SSO poderão acessar o Blueprint.

Se um usuário alterar o domínio registrado com seu perfil pega.com – por exemplo, mudar de organização –, os Blueprints que ele criou em seu domínio antigo não estarão mais visíveis.

O acesso a esses Blueprints pode ser restaurado para outros usuários dentro da organização mediante solicitação.

04

Privacidade de dados



Tratamento de dados no Pega Blueprint™

O que é capturado e como é tratado?

Nº	Dado	Formato	Processado por LLM?	Usado para treinamento de IA?	Armazenado em...	Visível para...
1	Dados do criador	Metadados (nome, e-mail, organização)	Não	Não	Armazenamento de dados Pega Cloud Totalmente criptografado*	Pega
2	Descrição do aplicativo	Metadados (setor, nome do aplicativo)	Sim – para informar o modelo inicial do Blueprint	Não	Armazenamento de dados Pega Cloud Totalmente criptografado*	Pega
3	Descrição em texto do aplicativo	Texto criptografado	Sim – para informar o modelo inicial do Blueprint	Não	Armazenamento de dados Pega Cloud Totalmente criptografado*	Apenas criadores e convidados do Blueprint**
4	Documentação legada	.PDF, .DOC, .DOCX	Sim – para informar o modelo inicial do Blueprint	Não	Armazenamento de arquivos Pega Cloud Criptografado em repouso*	Apenas criadores e convidados do Blueprint**
5	Vídeos e imagens legados	.MOV, .MP4, .JPG, .PNG	Sim – para informar o modelo inicial do Blueprint	Não	Armazenamento de arquivos Pega Cloud Criptografado em repouso*	Apenas criadores e convidados do Blueprint**
6	Diagramas de processo	.BPMN	Sim – para informar o modelo inicial do Blueprint	Não	Armazenamento de arquivos Pega Cloud Criptografado em repouso*	Apenas criadores e convidados do Blueprint**
7	Integração e documentação de dados	.YAML, .SQL, .DDL, .CRD	Sim – para informar o modelo inicial do Blueprint	Não	Armazenamento de arquivos Pega Cloud Criptografado em repouso*	Apenas criadores e convidados do Blueprint**
8	Edições de blueprint e designs finais	Metadados criptografados (exportados como arquivo .Blueprint criptografado)	Não	Não	Armazenamento de dados Pega Cloud Totalmente criptografado*	Apenas criadores e convidados do Blueprint**

*Os dados do Blueprint podem ser excluídos permanentemente mediante solicitação no suporte da Pega.

**Visível apenas para a equipe administrativa autorizada de operações de nuvem da Pega.

05

Segurança em nuvem





Acesse o Pega Cloud Trust Center para saber mais

Segurança em nuvem no Pega Blueprint™

O Pega Blueprint é operado pelos serviços confiáveis da Pega Cloud®, garantindo segurança de nível empresarial.

Transformação com confiança.

- Monitoramento, gerenciamento e suporte de operações 24 horas
- Operações de arquitetura protegidas por padrão com rígidos controles de acesso e proteções operacionais, minimizando intervenção humana com automação
- Conformidade, disponibilidade, recuperação de desastres e modelagem de ameaças de nível empresarial

Operações

Monitoramento, suporte ao ambiente e resposta proativa 24 horas
[Detalhes](#)

Acesso

Ambiente com controles operacionais automatizados e rígidos protocolos de acesso
[Detalhes](#)

Conformidade

Mais de 20 padrões setoriais estritamente seguidos
[Detalhes](#)

Recuperação de desastres

Backup, failover e restauração total de dados e serviços
[Detalhes](#)

Modelagem de ameaças

Siga a metodologia de red teams dos top 10 da OWASP
[Detalhes](#)

Disponibilidade

A arquitetura aproveita a alta disponibilidade interna e a recuperação de desastres para oferecer disponibilidade quase contínua.
[Detalhes](#)

Pega Cloud Trust Center
Secure. Reliable. Compliant. Pega Cloud empowers the world's biggest brands to meet - and exceed - the challenges of today and tomorrow. Learn how.

Learn how about Pega's security solutions

Security

Our security policies provide a framework for configuring applications to meet industry standards, preventing misconfigurations that compromise performance and availability.

Your security solution

Authorization & access
Manage user and system data access with role-based access control (RBAC) in Pega Cloud. Securely manage user access, manage user roles, and manage user roles. Role-based access control (RBAC) is a security model that uses roles to manage access to resources. Roles are assigned to users, and users are assigned to resources. Roles are assigned to users, and users are assigned to resources.

Network protection
Our network and cloud is designed to protect your data and services. We use a combination of firewalls, intrusion detection and prevention systems, and other security technologies to protect your data and services. We use a combination of firewalls, intrusion detection and prevention systems, and other security technologies to protect your data and services.

Secure system integration
Our system integration is designed to protect your data and services. We use a combination of firewalls, intrusion detection and prevention systems, and other security technologies to protect your data and services. We use a combination of firewalls, intrusion detection and prevention systems, and other security technologies to protect your data and services.

Data encryption
Encryption is a key part of the protection of data. Pega Cloud uses a combination of hardware and software encryption technologies to protect your data and services. We use a combination of hardware and software encryption technologies to protect your data and services.

Supporting security documents

Pega Cloud has a number of documents that describe our security practices. These documents are available in the Pega Cloud Trust Center.

Resources

Resource	Last updated (YYYY-MM-DD)	Assessment scope
Policy of Information Security	2024-01-01	Pega Cloud: AWS, GCP
Privacy Policy	2024-01-01	Pega Cloud: AWS, GCP
Security Policy	2024-01-01	Pega Cloud: AWS, GCP
Incident Response Plan	2024-01-01	Pega Cloud: AWS, GCP

Privacy

Pega Cloud is committed to protecting your privacy. We use a combination of hardware and software encryption technologies to protect your data and services. We use a combination of hardware and software encryption technologies to protect your data and services.

Compliance certifications, attestations, and accessibility

Pega Cloud is committed to providing a secure and reliable environment for your applications. We use a combination of hardware and software encryption technologies to protect your data and services. We use a combination of hardware and software encryption technologies to protect your data and services.

Pega Cloud certifications

Certification	Status
APRA	✓
CS	✓
CSA STAR	✓
Cyber Essentials	✓
Cyber Essentials Plus	✓
CyberGEX	✓
Cyberark	✓

06

Governança de IA





O Pega Blueprint™ usa uma combinação de modelos de vanguarda para promover transformação acelerada

Os modelos são todos gerenciados com segurança e incorporados ao produto para equilibrar eficácia e desempenho.

No 3º trimestre de 2025

A Pega está sempre avaliando os LLMs para garantir que estamos usando o modelo certo para o trabalho certo, mas estes são os modelos que usamos no momento:

Plataforma	Provedor de LLM	Região do Blueprint	Região do LLM
 AWS Provedor principal	Anthropic	AMS (EUA)	AWS Bedrock: Estados Unidos
		UE	AWS Bedrock: União Europeia
		Reino Unido	AWS Bedrock: Reino Unido
 Google Cloud	Google Gemini	AMS (EUA)	Google Vertex: Estados Unidos
		UE	Google Vertex: União Europeia
		Reino Unido	Google Vertex: Reino Unido
 Microsoft Azure	OpenAI - GPT	AMS (EUA)	Microsoft Azure: Estados Unidos
		UE	Microsoft Azure: União Europeia
		Reino Unido	Microsoft Azure: Reino Unido

Todos os contratos com plataformas contêm cláusulas estabelecendo que nenhum prompt ou dado enviado pela Pega ou pelos clientes será acessado pela plataforma nem pelo provedor de LLM.

*Dados de junho de 2025

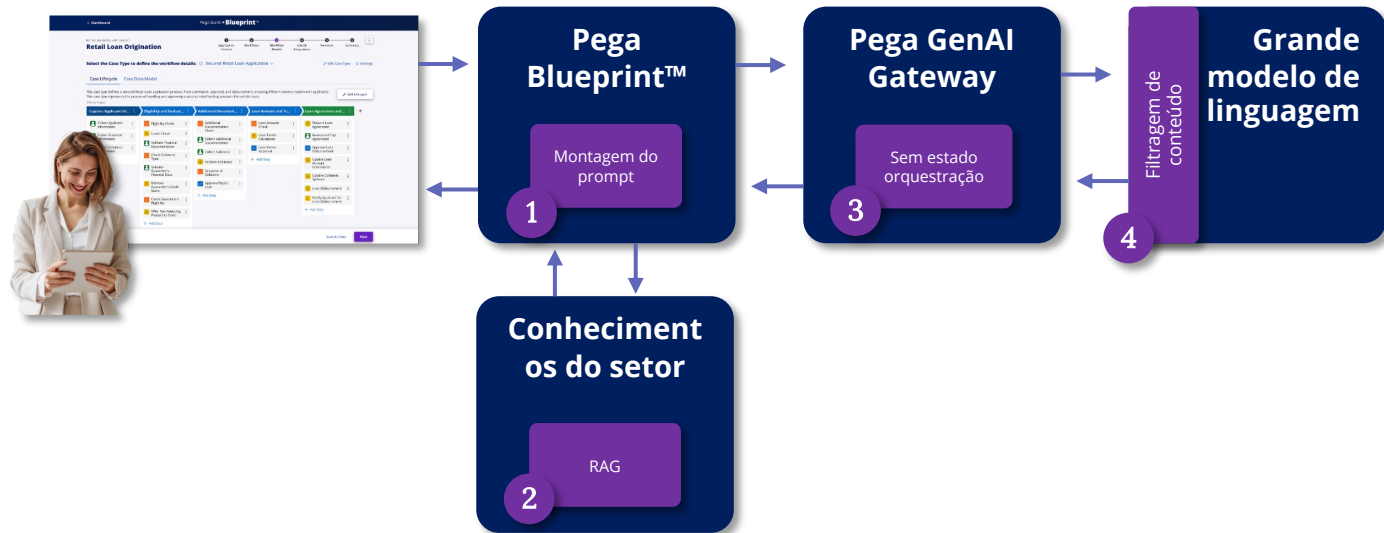
**Atualização continua em pega.com/pt-br

Fluxo de dados de IA

Pega Blueprint™

Gestão segura de IA:

1. O Pega Blueprint **cria prompts** que descrevem o aplicativo com base nas informações inseridas pelo usuário.
2. O Pega Blueprint aplica a base de conhecimentos de **experiência setorial** da Pega operada no Pega Knowledge Buddy para sintetizar as melhores práticas do setor para o caso de uso do Blueprint e enriquecer os prompts do LLM e a criação do Blueprint.
3. Todas as chamadas de LLM são intermediadas pelo **Serviço de gateway da Pega GenAI** na Pega Cloud. Esse serviço fornece uma camada confiável de segurança, segmentação e escala para comunicação com provedores de grandes modelos de linguagem.
4. Ao enviar um prompt criptografado para um LLM seguro, é aplicada a **filtragem de conteúdo** para detectar e bloquear conteúdo nocivo em prompts e resultados.



Abordagem de filtragem de conteúdo

A Pega conta com os provedores de grandes modelos de linguagem mais comprovados para a entrega de recursos da Pega que dependem de IA generativa. Dentro de cada modelo, há recursos robustos de filtragem de conteúdo que reduzem a probabilidade de respostas prejudiciais, antiéticas ou tóxicas. Embora os recursos sejam avançados, são apenas mitigações, e ainda existe a possibilidade de um jailbreak. Além disso, cada provedor tem a sua abordagem para atingir o mesmo resultado de uma IA responsável e ética.

Isso significa que os modelos de classificação, limites e categorias de detecção podem ser diferentes. Quando diferentes modelos são usados, diferentes classificações e filtros de conteúdo são aplicados. Quando os clientes usam o Pega GenAI Connect, eles devem estar cientes dessas possíveis diferenças e realizar testes para validá-las.

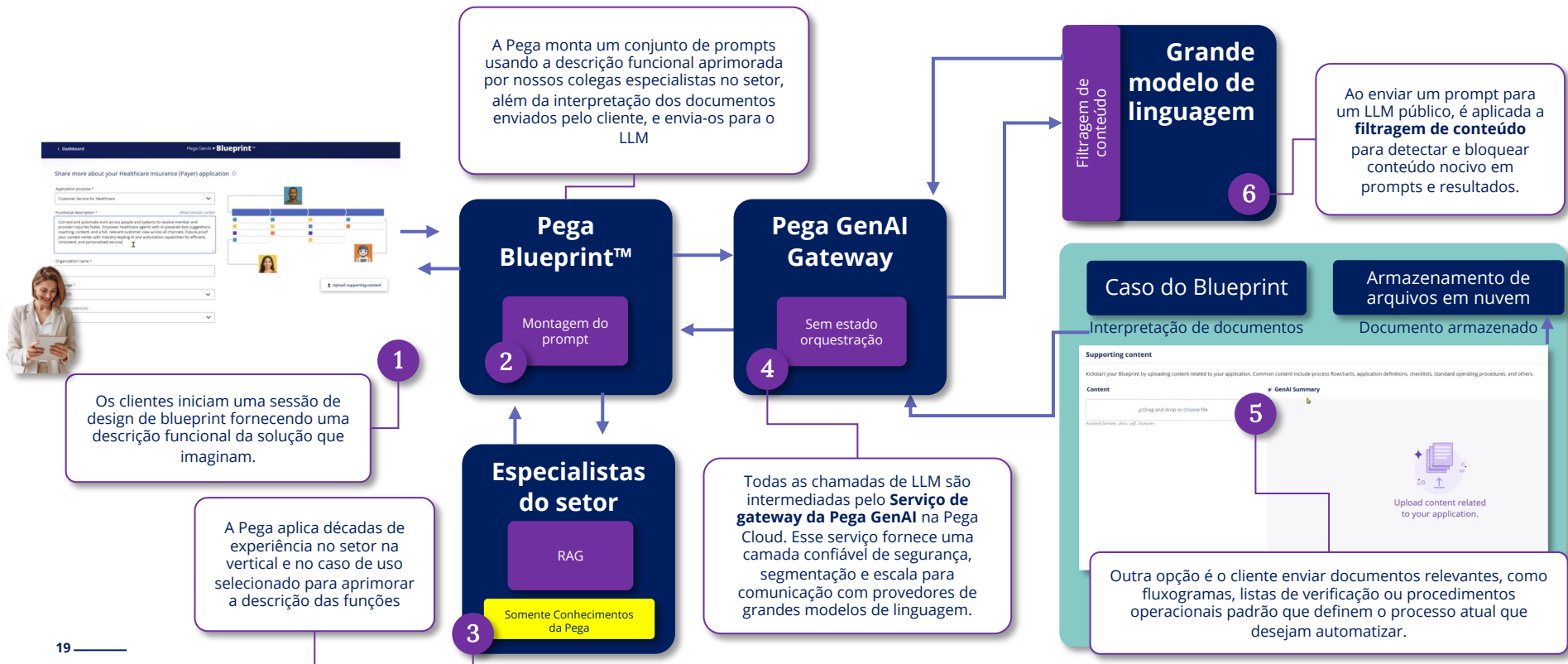
Fluxo de dados de IA

Pega Blueprint™

Abordagem de filtragem de conteúdo

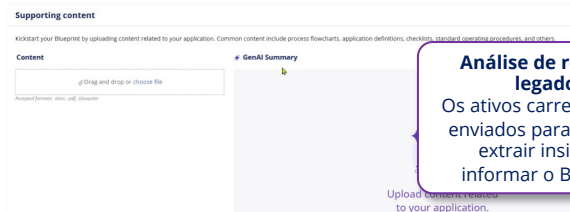
A Pega conta com os provedores de grandes modelos de linguagem mais comprovados para a entrega de recursos da Pega que dependem de IA generativa. Dentro de cada modelo, há recursos robustos de filtragem de conteúdo que reduzem a probabilidade de respostas prejudiciais, antiéticas ou tóxicas. Embora os recursos sejam avançados, são apenas mitigações, e ainda existe a possibilidade de um jailbreak. Além disso, cada provedor tem uma abordagem própria para atingir o mesmo resultado de uma IA responsável e ética.

Isso significa que os modelos de classificação, limites e categorias de detecção podem ser diferentes. Quando diferentes modelos são usados, diferentes classificações e filtros de conteúdo são aplicados. Quando os clientes usam o Pega GenAI Connect, eles devem estar cientes dessas possíveis diferenças e realizar testes para validá-las.



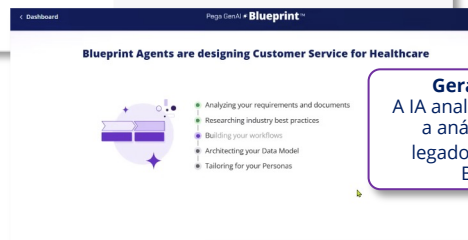
Fluxo de dados de IA

Pega Blueprint™



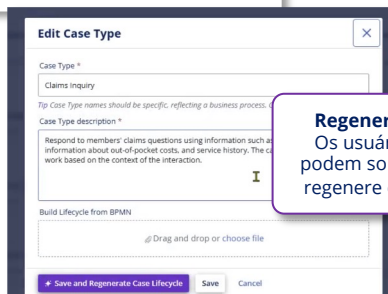
Análise de recursos legados

Os ativos carregados são enviados para a IA para extrair insights e informar o Blueprint



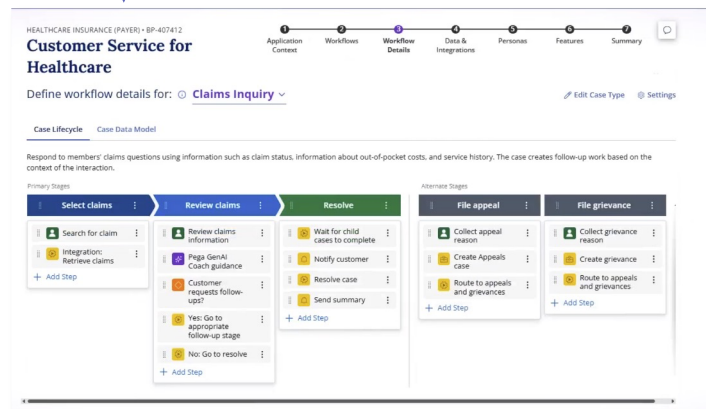
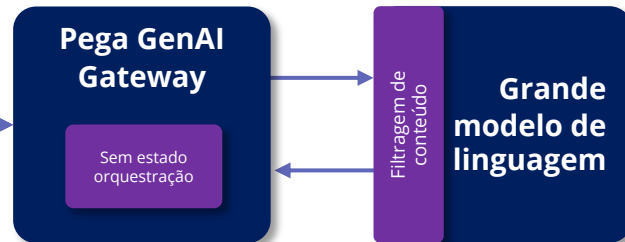
Geração inicial

A IA analisa a descrição e a análise de ativos legados para gerar o Blueprint



Regeneração por IA

Os usuários também podem solicitar que a IA regenere componentes



Governança de IA na Pega

Supervisão de ponta a ponta

O conselho de governança de IA da Pega é administrado pela equipe de segurança na nuvem e supervisiona toda a utilização de IA nos produtos da Pega.

Ele reúne especialistas e proprietários das áreas de produto, segurança na nuvem, operações na nuvem, TI, jurídico e entrada no mercado para garantir que toda a utilização da IA na Pega seja segura e responsável.

Parcerias estratégicas

Para atender às necessidades exclusivas de seus clientes corporativos, a Pega formou relacionamentos estratégicos e amplos contratos com AWS, Google Cloud e Microsoft para promover iniciativas de IA compartilhadas.

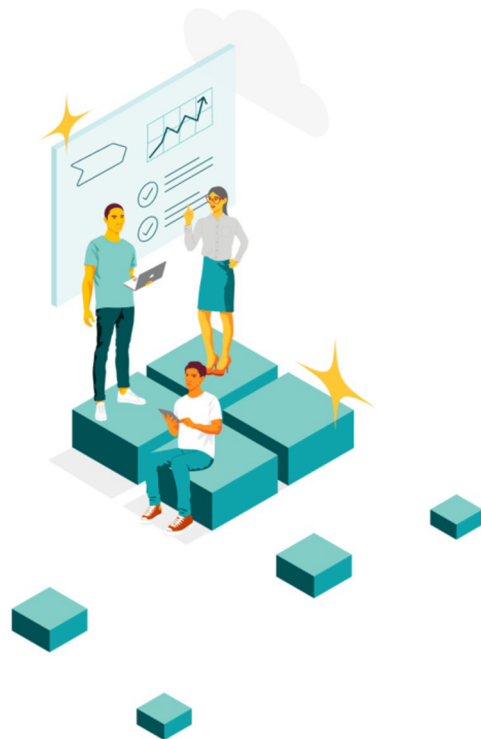
A Pega e seus provedores de serviços de LLM em nuvem se reúnem regularmente para analisar opções de modelos, desempenho, segurança e problemas.

Segurança em primeiro lugar

O conselho de governança de IA da Pega organiza e executa avaliações contínuas de segurança de todos os recursos baseados em IA, inclusive o Pega Blueprint.

Avaliações de segurança executadas:

1. ISO 42001
2. Metodologia Red Team de IA da Microsoft
3. Melhores práticas de segurança da OpenAI
4. Mitigações obrigatórias da Microsoft
5. Top 10 da OWASP para aplicações LLM
6. Top 10 da OWASP para Segurança de aplicativos nativos da nuvem





A Pega é a principal empresa de transformação empresarial que ajuda organizações no propósito Build for Change® com IA empresarial e automação de fluxo de trabalho. Muitas das empresas mais influentes do mundo confiam na nossa plataforma para resolver seus desafios mais urgentes, desde personalizar o engajamento até automatizar o atendimento e otimizar as operações. Desde 1983, construímos nossa arquitetura escalável e flexível para ajudar empresas a atender às demandas dos clientes de hoje, ao mesmo tempo em que se transformam para o amanhã. Para mais informações sobre a Pega (NASDAQ: PEGA), visite

<http://www.pegacom/pt-br>