



Transformación en la que puede *confiar.*

Cómo Pega Blueprint gestiona de forma
segura los datos, la privacidad y la IA.

● Seguridad y privacidad de Pega Blueprint™



Pega GenAI • Blueprint™

Dashboard

RETAIL BANKING • DP-206181

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](#)

Pega Blueprint™ Resumen de seguridad y privacidad

Creamos Pega GenAI Blueprint™ priorizando su privacidad y seguridad. Entendemos que sus procesos no son solo diagramas y flujos de trabajo, son su ventaja competitiva.



Acceso gestionado por su empresa

El acceso a Blueprint puede vincularse con el inicio de sesión único de su empresa.

- Blueprint gestiona el acceso a los datos mediante un control de acceso basado en roles, lo que garantiza que los Blueprints creados permanezcan privados para su creador, a menos que sean compartidos de forma explícita.
- Cuando un usuario deja de pertenecer a su organización, pierde el acceso a sus Blueprints en el momento en que su estado o sus roles se actualizan en el proveedor de inicio de sesión único (SSO) de la empresa.

Ninguna IA se entrena con los datos de su Blueprint

Los prompts, datos y diseños nunca se utilizan para entrenar modelos de inteligencia artificial.

- Blueprint aprovecha varios LLM en su funcionamiento interno, incluidos los modelos de Anthropic en AWS, Google Gemini y OpenAI en MS Azure.
- Todos los LLM están sujetos a una gobernanza continua, pruebas de rendimiento y aplican las prácticas recomendadas de los proveedores en materia de filtrado de contenido.

Los datos se mantienen confidenciales

Los detalles de sus Blueprints se almacenan en una base de datos cifrada en la nube.

- Implementado en la nube en la región que mejor se adapte a las necesidades de su empresa: Estados Unidos, Reino Unido, Asia- Pacífico o la Unión Europea.
- No se comparte ningún dato entre clientes o socios de Pega.
- Los Blueprints permanecen privados solo para su creador, a menos que sean compartidos de manera explícita.
- Solo el personal autorizado utiliza los datos de informes a nivel de actividad dentro de Pega (dirección de correo electrónico, fecha de creación, nombre de creador).

Seguridad en la nube de nivel empresarial

Sus datos de Blueprint reciben la misma protección sólida que nuestros entornos de producción de Pega Cloud, que incluye:

- Cifrado AES de 256 bits para datos en reposo y protección HTTPS/TLS para datos en tránsito.
- Supervisión continua con protección antivirus local y sistemas de prevención de intrusiones.
- Centros de operaciones de última generación que se toman muy en serio la seguridad física y ambiental.
- Protección integrada contra ataques DDoS y bloqueo automático de direcciones IP maliciosas conocidas.



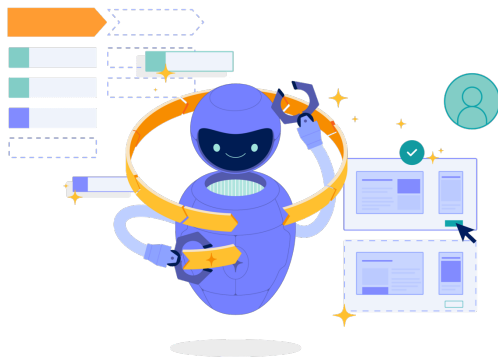
01

¿Qué es Pega Blueprint?



Combustible para la transformación

Pega Blueprint es una plataforma de desarrollo de flujos de trabajo empresariales impulsada por inteligencia artificial. Su objetivo es unir a las personas y la IA para acelerar la automatización e impulsar la transformación desde el primer momento.



Pega GenAI + Blueprint™

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](#)



¿Dónde encaja Blueprint en el ciclo de vida del desarrollo de software (SDLC)?

Diseño ágil para impulsar el desarrollo



Colaboración entre negocio y TI para acelerar el diseño inicial de flujos de trabajo con GenAI.

Configuración avanzada de integraciones, automatizaciones y otros elementos para convertir los Blueprints en aplicaciones completas

Procesos automatizados de DevOps que organizan la ruta hacia la puesta en producción, incluidas las pruebas, las aprobaciones, los análisis de seguridad y más

Experiencias seguras para los usuarios finales al acceder a los flujos de trabajo (protegidas mediante controles basados en roles y niveles de acceso)

Análisis de flujos de trabajo para detectar brechas en los procesos e ineficiencias operativas

Sin PII*

Sin PII*

Sin PII*

Potencialmente sensible

Potencialmente sensible

Operado de forma segura por Pega Cloud®

Implementación de clientes privados

Implementación de clientes privados

Implementación de clientes privados

Operado de forma segura por Pega Cloud®

*Basado en los casos de uso durante la fase de diseño, no se recomienda manejar información de identificación personal (PII) en estas etapas.

02

Arquitectura de Blueprint.



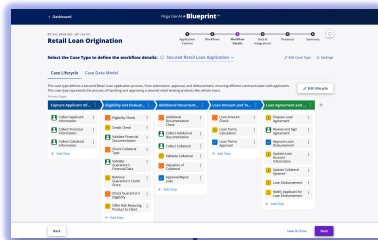
Arquitectura Pega Blueprint™

El Blueprint se ejecuta de forma segura en Pega Cloud® sobre AWS, administrado y operado conforme a los [principales estándares de la industria en servicios en la nube](#).

Arquitectura de alto nivel:

- La autenticación de Blueprint se conecta con el protocolo de inicio de sesión único (SSO) de su empresa.
- Pega ofrece servicios de residencia de datos segmentados geográficamente, específicos de su oferta de Pega Cloud. La región geográfica del Blueprint se basa en la ubicación de su empresa ([dentro de EE. UU. Este, Reino Unido o la Unión Europea](#)).
- El procesamiento del Blueprint se ejecuta sobre una aplicación Pega Infinity segura y confiable, totalmente respaldada por la fortaleza operativa de Pega Cloud Services, lo que garantiza [confiabilidad](#), [cumplimiento normativo](#), [seguridad](#) y [recuperación ante desastres](#) de nivel empresarial.
- Blueprint utiliza los LLM seleccionados según el caso de uso y el rendimiento. Utiliza principalmente modelos Claude que se ejecutan en [AWS Bedrock](#).
- Ninguna IA se entrena con los datos de su Blueprint.
- Los datos de Blueprint se [cifran en tránsito](#) mediante TLS.
- Asimismo, los datos del Blueprint se [almacenan de forma segura](#) y se [cifran en reposo](#).

Pega.com aplicación web front-end



Pega.com servicio de autenticación

Su SSO

Su empleado

{usuario}@{su-organización}.com



Totalmente aislado **por región**, distribuido entre:
EE. UU. - Reino Unido - Unión Europea



Aplicación Blueprint

Procesamiento central de solicitudes de usuario y funcionalidades del Blueprint

Desarrollado sobre Pega Infinity™



Servicio de conocimiento del sector

Servicio de generación aumentada de recuperación que proporciona a Blueprint información sobre las mejores prácticas en materia de flujo de trabajo y modelos de datos basándose en las solicitudes de los usuarios.

Desarrollado sobre Pega Knowledge Buddy™. Contiene propiedad intelectual del sector de Pega.
No almacena ningún dato de clientes ni de usuarios.



Servicio de orquestación de IA de Pega Cloud

Organiza llamadas a los LLM

Desarrollado sobre AWS. No almacena prompts, datos de clientes ni datos de usuarios.



AWS Bedrock
Proveedor principal de LLM
Claude Haiku y Sonnet



Google Gemini
Flash



Azure OpenAI
GPT

Diversos LLM se utilizan según el caso de uso y el rendimiento. Todo el procesamiento se realiza dentro de la región correspondiente. Ninguna IA se entrena con datos de usuarios ni de la empresa.



Almacenamiento seguro de datos

Cifrado de datos privados en reposo (DARE) para empresas

Todos los datos del cliente almacenados en volúmenes y bases de datos se cifran con un cifrado de 256 bits. De forma predeterminada, las claves de cifrado se rotan periódicamente y se almacenan de manera segura en un KMS conforme a FIPS 140-2.

Las claves de cifrado privadas de la empresa están disponibles previa solicitud.



Almacenamiento privado de archivos

Conéctese con su repositorio de Pega Cloud

Todos los archivos relacionados con la actividad de Blueprint, por ejemplo, la documentación y los videos cargados, se almacenan en una carpeta privada de Pega Cloud File Storage. De forma predeterminada, esta carpeta es administrada por Blueprint en nombre de la empresa.

Los archivos relacionados con Blueprint de los clientes de Pega Cloud se almacenan de forma predeterminada en su repositorio privado existente de Pega Cloud File Storage asociado a su instancia de Pega Cloud.

Residencia regional de datos Pega Blueprint™ (Unión Europea, Reino Unido, Estados Unidos)

Empresas ubicadas en Unión Europea

- Almacenamiento y cómputo: **AWS EU-Central (Fráncfort)**
- [Ejecución del modelo de IA](#)

	Proveedor	Modelo/ proveedor	Regiones de LLM
	AWS Bedrock Proveedor principal	Anthropic	AWS Bedrock: Unión Europea
	Google Cloud	Gemini	Google Vertex: Unión Europea
	Microsoft Azure	OpenAI GPT	Microsoft Azure: Unión Europea

Empresas ubicadas en Reino Unido

- Almacenamiento y cómputo: **AWS EU-Central (Fráncfort)**
- [Ejecución del modelo de IA](#)

	Proveedor	Modelo/ proveedor	Regiones de LLM
	AWS Bedrock Proveedor principal	Anthropic	AWS Bedrock: Unión Europea
	Google Cloud	Gemini	Google Vertex: Unión Europea
	Microsoft Azure	OpenAI GPT	Microsoft: Unión Europea

Empresas ubicadas en todo el mundo

- Almacenamiento y computación: **AWS US-East**
- [Ejecución del modelo de IA](#)

	Proveedor	Modelo/ proveedor	Regiones de LLM
	AWS Bedrock Proveedor principal	Anthropic	AWS Bedrock: Estados Unidos
	Google Cloud	Gemini	Google Vertex: Estados Unidos
	Microsoft Azure	OpenAI GPT	Microsoft Azure: Estados Unidos

Para socios de Pega

Defina en nombre de qué empresa está creando un Blueprint en el campo de nombre de organización de la página de descripción funcional del Blueprint. De este modo, dichos Blueprints se almacenarán y gestionarán automáticamente dentro de la región correspondiente, en nombre de esa empresa.

Determinación de la región en la que se almacena un Blueprint

Consulte el Id. del Blueprint, que incluirá un identificador regional si el Blueprint se encuentra almacenado y gestionado dentro de la Unión Europea, Australia, Reino Unido, Japón o Singapur.

Residencia de datos regional de Pega Blueprint™ (Asia-Pacífico)

Empresas ubicadas en

Australia

- Almacenamiento y cómputo: **AWS: Australia - Sydney**
- [Ejecución del modelo de IA](#)

Empresas ubicadas en

Japón

- Almacenamiento y cómputo: **AWS: Japón - Osaka**
- [Ejecución del modelo de IA](#)

Empresas ubicadas en

Singapur

- Almacenamiento e informática: **AWS: Singapur**
- [Ejecución del modelo de IA](#)

	Proveedor	Modelo/ proveedor	Regiones de LLM
	AWS Bedrock Proveedor principal	Anthropic	AWS Bedrock: Australia/Asia- Pacífico
	Google Cloud	Gemini	Google Vertex: Australia
	Microsoft Azure	OpenAI GPT	Microsoft Azure: Australia / Unión Europea

	Proveedor	Modelo/ proveedor	Regiones de LLM
	AWS Bedrock Proveedor principal	Anthropic	AWS Bedrock: Japón/Asia- Pacífico
	Google Cloud	Gemini	Google Vertex: Japón
	Microsoft Azure	OpenAI GPT	Microsoft Azure: Japón / Unión Europea

	Proveedor	Modelo/ proveedor	Regiones de LLM
	AWS Bedrock Proveedor principal	Anthropic	AWS Bedrock: Asia-Pacífico
	Google Cloud	Gemini	Google Vertex: Singapur
	Microsoft Azure	OpenAI GPT	Microsoft Azure: Unión Europea

Para socios de Pega

Defina en nombre de qué empresa está creando un Blueprint en el campo de nombre de organización de la página de descripción funcional del Blueprint. De este modo, dichos Blueprints se almacenarán y gestionarán automáticamente dentro de la región correspondiente, en nombre de esa empresa.

Determinación de la región en la que se almacena un Blueprint

Consulte el Id. del Blueprint, que incluirá un identificador regional si el Blueprint se encuentra almacenado y gestionado dentro de la Unión Europea, Australia, Reino Unido, Japón o Singapur.

03

Acceso y autenticación.



Pega Blueprint™

Acceso y autenticación

Configure el acceso al Blueprint mediante su inicio de sesión único (SSO).

Permitir que los usuarios se autenticuen mediante el proveedor de identidad (IDP) de su organización garantiza que solo los usuarios autorizados accedan a todos los sitios y aplicaciones de Pega, como Blueprint, My Support Portal, entre otros.

Cuando la autenticación federada está habilitada, al iniciar sesión, los usuarios no deberán ingresar una contraseña, sino que serán redirigidos para autenticarse a través de su proveedor de identidad.

Los responsables de TI de la organización cliente pueden colaborar con nuestro equipo de cuenta integrado para habilitar la autenticación federada.

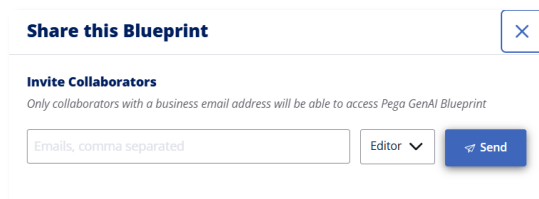
Qué necesitamos de usted: detalles de configuración de SAML 2.0 o de OAuth

Las siguientes aplicaciones utilizarán autenticación federada: Blueprint, Pega.com, community.pega.com, academy.pega.com, support.pega.com, docs.pega.com, partners.pega.com, saleshub.pega.com, partner-logo-generator.pega.com, My Support Portal, My Pega Cloud, My Pega, PDC, Deployment Manager y Pega Trials.

Los Blueprints solo son visibles para su creador, a menos que se compartan de forma explícita.

De forma predeterminada, los Blueprints no son visibles para nadie más allá del usuario que los creó (el *propietario* del Blueprint).**

Los propietarios de un Blueprint tienen la posibilidad de compartirlo con otros interesados (por ejemplo, compañeros de equipo, socios, etc.). Pueden invitar a usuarios por correo electrónico con permisos de *editor* o *lector*.



Cuando un usuario deja la organización, sus Blueprints no se trasladan con él.

Si una empresa ha federado su inicio de sesión único (SSO) con las propiedades digitales de Pega (por ejemplo, Blueprint), solo los usuarios con acceso activo a su SSO podrán iniciar sesión en el Blueprint.

Si un usuario cambia el dominio registrado en su perfil de pega.com, por ejemplo, al cambiar de organización, los Blueprints que creó bajo su dominio anterior dejarán de ser visibles.

El acceso a esos Blueprints puede restablecerse para otros usuarios de la organización previa solicitud.

04

Privacidad de datos.



Pega Blueprint™

Gestión de datos

¿Qué se captura y cómo se gestiona?

#	Punto de datos	Formato	¿Procesado por LLM?	¿Se usa para entrenamiento de IA?	Almacenado en...	Visible para..
1	Información sobre el creador	Metadatos (nombre, correo electrónico, organización)	No	No	Almacenamiento de datos de Pega Cloud Totalmente cifrado*	Pega
2	Descripción de la aplicación	Metadatos (industria, nombre de la aplicación)	Sí, para informar sobre la plantilla inicial del Blueprint	No	Almacenamiento de datos de Pega Cloud Totalmente cifrado*	Pega
3	Descripción de la aplicación basada en texto	Texto cifrado	Sí, para informar sobre la plantilla inicial del Blueprint	No	Almacenamiento de datos de Pega Cloud Totalmente cifrado*	Solo creadores e invitados del Blueprint**
4	Documentación heredada	.PDF, .DOC, .DOCX	Sí, para informar sobre la plantilla inicial del Blueprint	No	Almacenamiento de archivos de Pega Cloud Cifrado en reposo*	Solo creadores e invitados del Blueprint**
5	Videos e imágenes heredados	.MOV, .MP4, .JPG, .PNG	Sí, para informar sobre la plantilla inicial del Blueprint	No	Almacenamiento de archivos de Pega Cloud Cifrado en reposo*	Solo creadores e invitados del Blueprint**
6	Diagramas de procesos	.BPMN	Sí, para informar sobre la plantilla inicial del Blueprint	No	Almacenamiento de archivos de Pega Cloud Cifrado en reposo*	Solo creadores e invitados del Blueprint**
7	Documentación de datos e integración	.YAML, .SQL, .DDL, .CRD	Sí, para informar sobre la plantilla inicial del Blueprint	No	Almacenamiento de archivos de Pega Cloud Cifrado en reposo*	Solo creadores e invitados del Blueprint**
8	Ediciones de Blueprint y diseños finales	Metadatos cifrados (exportados como archivo .Blueprint cifrado)	No	No	Almacenamiento de datos de Pega Cloud Totalmente cifrado*	Solo creadores e invitados del Blueprint**

*Los datos de Blueprint pueden eliminarse de forma permanente previa solicitud a través de Pega Support.

**Visible solo para el personal administrativo autorizado de Pega Cloud Operations.

05

Seguridad en la nube.





Pega Blueprint se ejecuta sobre los Pega Cloud® Services probados, lo que garantiza una seguridad de nivel empresarial.

- Monitoreo, gestión y soporte de operaciones 24/7
- Operaciones de arquitectura segura desde su diseño con estrictos controles de acceso y mecanismos de protección operativa, lo que minimiza la intervención humana mediante la automatización
- Cumplimiento normativo, tiempo de actividad, recuperación ante desastres y modelado de amenazas de nivel empresarial

Detalles

Accesso

Entorno regulado por controles operativos automatizados y estrictos protocolos de acceso

Detalles

Cumplimiento normativo

Cumplimiento estricto de más de 20 estándares del sector

Details

Recuperación ante desastres

Copia de seguridad integral de datos y servicios, conmutación por error y restauración.

Details

Modelado de amenazas

Sigue la metodología de Red Team basada en el OWASP Top 10

Details

Accesibilidad

La arquitectura aprovecha mecanismos integrados de alta disponibilidad y recuperación ante desastres para garantizar un tiempo de actividad prácticamente continuo.

Details

[Page Sites](#)
[Platform](#)
[Solutions](#)
[Customers](#)
[Learn](#)
[Services & Partners](#)
[Events](#)
[About Us](#)

[Try Pega](#)

[Apache Log4j vulnerability update](#)
[Learn what steps Pega is taking to address it](#)

Pega 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 more about Pega's security features:](#)

- [Security](#)
- [Privacy](#)
- [Compliance](#)
- [VPA's](#)
- [Service reliability](#)

Security

Our security policies provide a framework for safeguarding against unauthorized access and preventing/mitigating attacks that compromise performance and availability.

[View security bulletins](#)

Authorization & access

Manage user and system data access with role-based controls to Pega Cloud Environment(s). Simplify native identity access management and integration with leading single sign-on technologies, including SAML, OAuth, and Active Directory.

Client-based access control

Client-based access control rules define where and how customer data is stored and accessed. We associate personal data with actual people, not abstract entities such as businesses.

Network protection

Our network architecture is designed to meet a range of security control requirements. Gain secure operation of your Pega Cloud Environment(s) isolated from fellow Pega clients and internal services thanks to our network firewalls and access controls.

Data encryption

Encryption is critical to the protection of data whether it is in transit or at rest. Pega Cloud employs encryption across all Pega Cloud Environment(s) that meet or exceed client and regulatory requirements. When data is at rest, AES 256-bit encryption is the standard. For data in transit, Pega Cloud offers TLS 1.2 and TLS 1.3.

Secure system integration

We offer multiple secure and private ways for Pega Cloud Environment(s) to integrate with systems in enterprise environments.

Supporting security documents

Pega maintains a set of documents and white papers that allow our clients to better understand our overall security posture from software development through service delivery.

Resources	Last updated (YYYY-MM-DD)	Assessment scope
Digital Security Policies	2024-12-27	Pega Cloud AWS, GCP
Veracode Statements	N/A	Pega Cloud AWS, GCP
Penetration Test Summaries	2024-09-17	Pega Cloud AWS, GCP
Business Continuity Plan Summary	2024-05-03	Pega Cloud AWS, GCP
Disaster Recovery Test Results	2024-12-09	Pega Cloud AWS, GCP

Privacy

Use our services to enable you to implement your own privacy and compliance strategies. We continually evolve our platform to provide the features and security measures that you may need to support your security and privacy strategy.

[Read Pega's privacy notice](#)

Compliance certifications, attestations, and accessibility

When evaluating the services listed under each compliance standard it should be noted that Pega relies on a common set of controls for the purposes of adherence. These common controls exist across the Pega Platform, the underlying infrastructure, and the operations, administration and management provided by Pega in Pega Cloud. Pega applications developed within the Pega Platform inherit these controls which are attested to in the current scope of Pega Cloud certifications

APRA	
CISA	
CSA STAR	
Cyber Essentials	
Cyber Essentials Plus	
CyberGRC	
CyberEvals	
FISMA	

06

Governanza de IA.





Pega Blueprint™ utiliza una combinación de modelos innovadores para impulsar una transformación rápida y eficiente.

Todos los modelos se gestionan e integran de forma segura en el producto, para lograr un equilibrio entre eficacia y rendimiento.

A partir del tercer trimestre de 2025

Si bien Pega evalúa continuamente los LLM para garantizar el uso del modelo más adecuado para cada tarea, a continuación se enumeran los modelos actualmente utilizados en la plataforma:

Hiperescaladores	Proveedor de LLM	Región del Blueprint	Región del LLM
 AWS Proveedor principal	Anthropic	AMS (EE. UU.)	AWS Bedrock: Estados Unidos
		UE	AWS Bedrock: Unión Europea
		Reino Unido	AWS Bedrock: Reino Unido
 Google Cloud	Google Gemini	AMS (EE. UU.)	Google Vertex: Estados Unidos
		UE	Google Vertex: Unión Europea
		Reino Unido	Google Vertex: Reino Unido
 Microsoft Azure	OpenAI - GPT	AMS (EE. UU.)	Microsoft Azure: Estados Unidos
		UE	Microsoft Azure: Unión Europea
		Reino Unido	Microsoft Azure: Reino Unido

Todos los acuerdos con hiperescaladores incluyen compromisos de que ni el hiperescalador ni el proveedor de LLM tendrán acceso a las solicitudes ni a los datos enviados por Pega o los clientes.

*A partir de junio de 2025

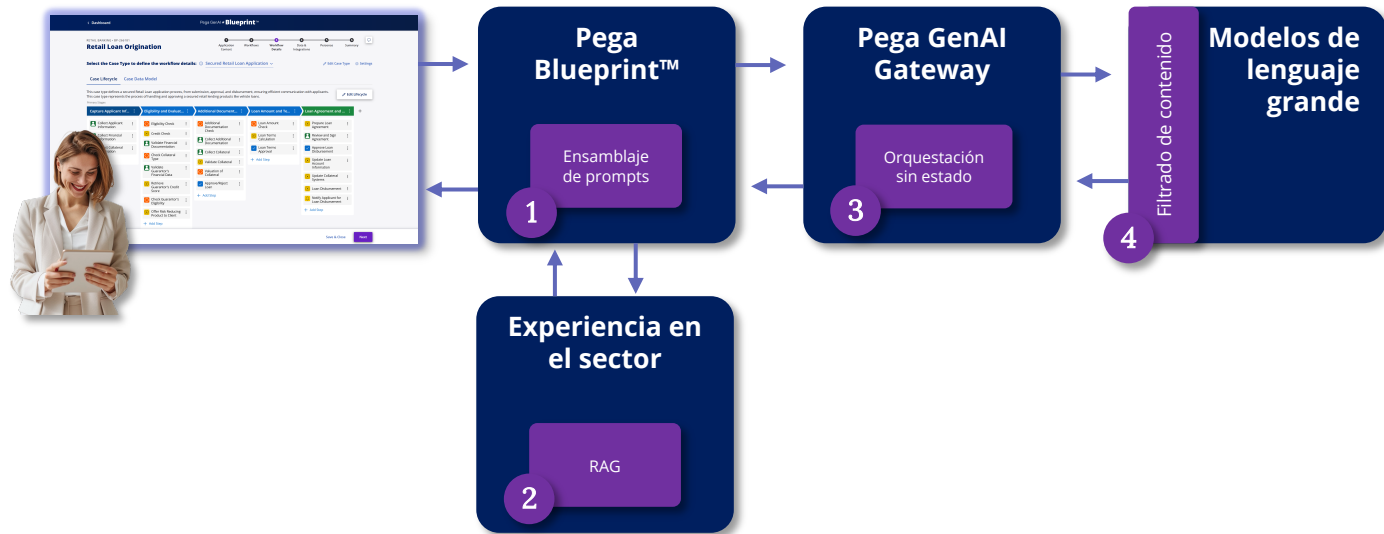
**Siempre actualizado en pegacom.com

Flujo de datos de IA

Pega Blueprint™

Gestión segura y confiable de la IA:

1. Pega Blueprint **genera prompts** que describen la aplicación en función de la información ingresada por el usuario.
2. Pega Blueprint recurre a la base de conocimientos sobre **experiencia en el sector** de Pega, administrada por Pega Knowledge Buddy, para sintetizar las prácticas recomendadas de la industria según el caso de uso definido en Blueprint y enriquecer tanto los prompts de los LLM como la creación del propio Blueprint.
3. Todas las llamadas a los LLM se gestionan a través de **Pega GenAI Gateway Service** en Pega Cloud. Este servicio proporciona una capa confiable de seguridad, segmentación y escalabilidad para la comunicación con los proveedores de modelos de lenguaje de gran tamaño.
4. Al enviar un prompt cifrado a un LLM seguro, se aplica un **filtrado de contenido** destinado a detectar y prevenir contenido dañino tanto en los prompts como en las respuestas.



Enfoque de filtrado de contenido

Pega confía en los proveedores de modelos de lenguaje grande más reconocidos para ofrecer sus capacidades basadas en inteligencia artificial generativa. Cada modelo incorpora sólidos mecanismos de filtrado de contenido diseñados para mitigar la posibilidad de respuestas dañinas, poco éticas o tóxicas. Si bien estas capacidades son avanzadas, constituyen solo medidas de mitigación, por lo que sigue existiendo la posibilidad de un “jailbreak” (evasión de las protecciones del modelo). Además, cada proveedor de modelos adopta un enfoque diferente para lograr el mismo objetivo de una IA responsable y ética.

Esto significa que los modelos de clasificación, los umbrales y las categorías de detección pueden diferir entre proveedores. Cuando se utilizan distintos modelos, se aplican diferentes métodos de clasificación y filtrado de contenido. Por lo tanto, los clientes que empleen Pega GenAI Connect deben ser conscientes de estas posibles diferencias y realizar pruebas de validación para confirmarlas.

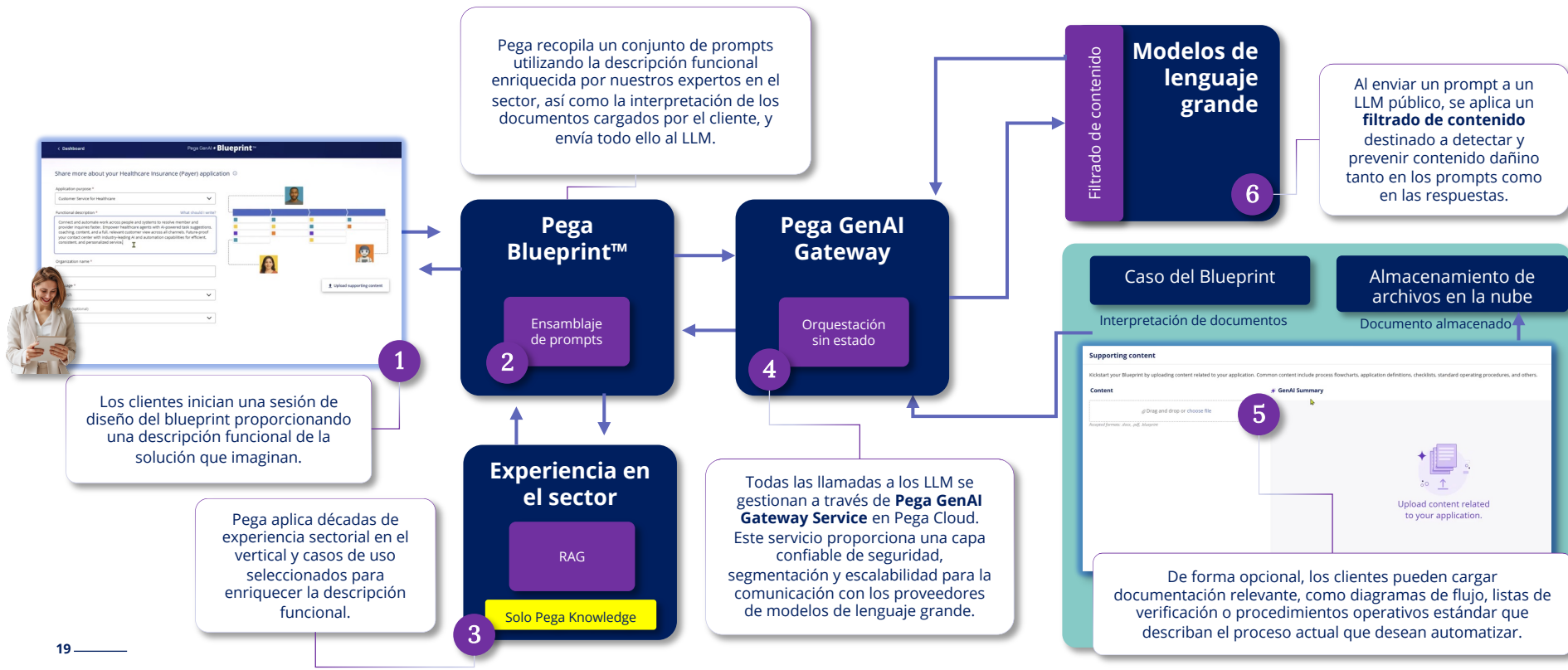
Flujo de datos de IA

Pega Blueprint™

Enfoque de filtrado de contenido

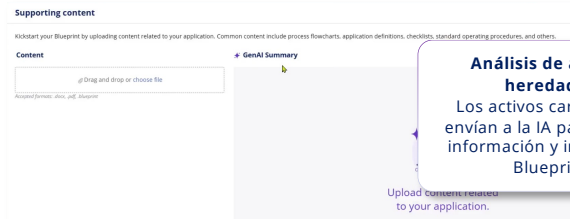
Pega confía en los proveedores de modelos de lenguaje grande más reconocidos para ofrecer sus capacidades basadas en inteligencia artificial generativa. Cada modelo incorpora sólidos mecanismos de filtrado de contenido diseñados para mitigar la posibilidad de respuestas dañinas, poco éticas o tóxicas. Si bien estas capacidades son avanzadas, constituyen solo medidas de mitigación, por lo que sigue existiendo la posibilidad de un "jailbreak" (evasión de las protecciones del modelo). Además, cada proveedor de modelos adopta un enfoque diferente para lograr el mismo objetivo: una IA responsable y ética.

Esto significa que los modelos de clasificación, los umbrales y las categorías de detección pueden diferir entre proveedores. Cuando se utilizan distintos modelos, se aplican diferentes métodos de clasificación y filtrado de contenido. Por lo tanto, los clientes que empleen Pega GenAI Connect deben ser conscientes de estas posibles diferencias y realizar pruebas de validación para confirmarlas.



Flujo de datos de IA

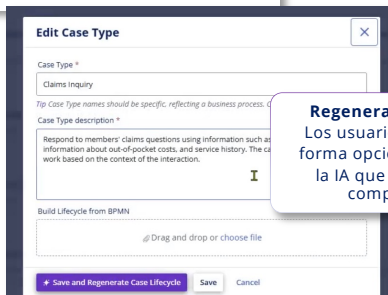
Pega Blueprint™



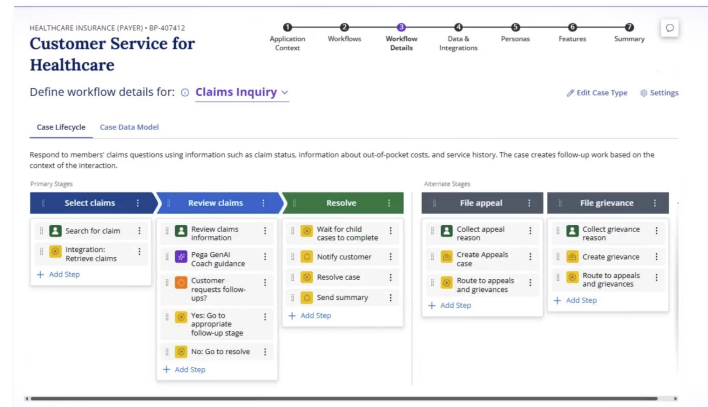
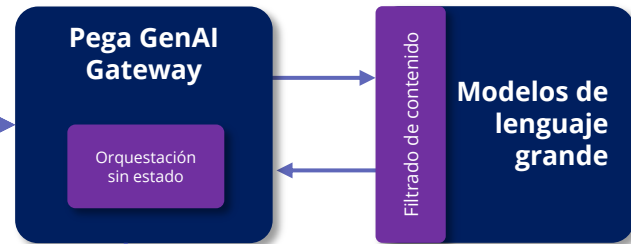
Análisis de activos heredados
Los activos cargados se envían a la IA para extraer información y informar al Blueprint



Generación inicial
La IA analiza la descripción funcional y los activos heredados para generar el Blueprint



Regeneración de la IA
Los usuarios pueden, de forma opcional, solicitar a la IA que regenere los componentes



Gobernanza de IA en Pega

Supervisión de principio a fin

La junta de Gobernanza de IA de Pega está dirigida por el equipo de Seguridad en la Nube y supervisa toda la utilización de IA en los productos de Pega.

Reúne a expertos y responsables de producto, seguridad en la nube, operaciones en la nube, TI, asuntos legales y comercialización para garantizar que toda implementación de IA en Pega sea segura, responsable y confiable.

Alianzas estratégicas

Para satisfacer las necesidades específicas de sus clientes empresariales, Pega ha establecido relaciones estratégicas y acuerdos generales con AWS, Google Cloud y Microsoft, con el fin de impulsar iniciativas conjuntas en materia de IA.

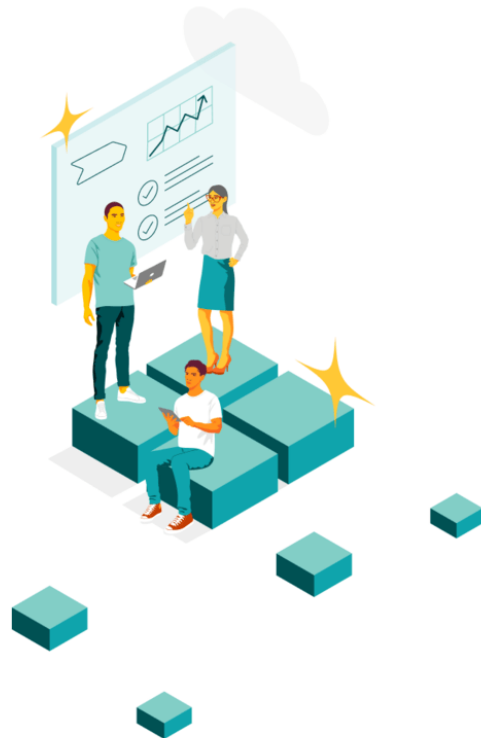
Pega y sus proveedores de servicios de LLM en la nube se reúnen periódicamente para revisar las opciones de modelos, el rendimiento, la seguridad y las incidencias.

La seguridad como prioridad

La junta de Gobernanza de IA de Pega organiza y ejecuta evaluaciones de seguridad continuas en todas las capacidades impulsadas por IA, incluido Pega Blueprint.

Las evaluaciones de seguridad que se ejecutan incluyen:

1. ISO 42001
2. Metodología Microsoft AI Red Team
3. Prácticas recomendadas de seguridad de OpenAI
4. Medidas de mitigación requeridas por Microsoft
5. OWASP Top 10 para aplicaciones con LLM
6. OWASP Top 10 para seguridad en aplicaciones nativas en la nube





Pega es la empresa líder en transformación empresarial que ayuda a las organizaciones a construir para el cambio (Build for Change®) con la toma de decisiones de IA empresarial y la automatización del flujo de trabajo. Muchas de las empresas más influyentes del mundo confían en nuestra plataforma para resolver sus retos más urgentes, desde la personalización del engagement hasta la automatización del servicio o la optimización de las operaciones. Desde 1983, hemos desarrollado nuestra arquitectura escalable y flexible para ayudar a las empresas a satisfacer las demandas de los clientes de hoy mientras se transforman continuamente para el mañana. Para más información acerca de Pega (NASDAQ: PEGA), consulte <http://www.pega.com/es>

