

Política de Privacidad de LibreChat

Versión: 1.0

Ámbito: Personal autorizado de la Pontificia Universidad Católica del Perú
Administración funcional y técnica: Oficina de Transformación Digital (OTD)
Contacto: txdigital@pucp.edu.pe

1. Objeto, alcance y marco aplicable

1.1. Objeto

La presente Política de Privacidad tiene por objeto informar sobre el tratamiento de información y datos personales que puede producirse durante el acceso y utilización de **LibreChat**, plataforma institucional de inteligencia artificial generativa de la Pontificia Universidad Católica del Perú.

Esta Política establece las condiciones generales aplicables al tratamiento de información mediante LibreChat, incluyendo el uso de modelos de inteligencia artificial, archivos, agentes, herramientas, conectores y servicios externos.

Esta Política tiene carácter informativo y de transparencia y **no sustituye la obtención del consentimiento del titular de los datos personales cuando este resulte exigible conforme a la normativa aplicable.**

Debe interpretarse conjuntamente con las **Condiciones de uso de LibreChat** y las demás disposiciones institucionales y legales aplicables.

1.2. Alcance y administración de LibreChat

LibreChat está dirigido exclusivamente al personal autorizado de la PUCP, incluyendo principalmente:

- personal administrativo;
- personal docente;
- personal que desarrolla labores de investigación;
- otros miembros del personal a quienes la Universidad otorgue expresamente acceso.

LibreChat no está destinado al acceso o uso por estudiantes.

No obstante, en el desarrollo de sus funciones, los usuarios autorizados podrían tratar mediante LibreChat, cuando corresponda y se encuentre permitido, información relacionada con estudiantes, trabajadores, investigadores, participantes de investigaciones u otras personas.

La **Oficina de Transformación Digital (OTD)** es responsable de la administración funcional y técnica de LibreChat y de la aplicación de las medidas operativas y tecnológicas correspondientes a la plataforma.

El uso de LibreChat no modifica las responsabilidades, obligaciones ni niveles de protección aplicables a la información de acuerdo con su naturaleza y procedencia.

1.3. Marco normativo e institucional

El tratamiento de información mediante LibreChat deberá observar, según corresponda:

1. La **Ley N.º 29733, Ley de Protección de Datos Personales**.
2. El **Decreto Supremo N.º 016-2024-JUS**, Reglamento de la Ley N.º 29733.
3. El **Reglamento de Protección de Datos Personales de la PUCP**.
4. La **Ley N.º 31814**, Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país.
5. El **Decreto Supremo N.º 115-2025-PCM**, Reglamento de la Ley N.º 31814.

6. Los **Lineamientos para el uso de herramientas IA generativas** de la Dirección de Tecnologías de Información (DTI).
7. Los **Lineamientos sobre el uso académico de la Inteligencia Artificial** de la Dirección de Asuntos Académicos (DAA), cuando LibreChat sea utilizado en actividades vinculadas con la docencia.
8. Las demás políticas y disposiciones institucionales relacionadas con protección de datos personales, seguridad de la información, confidencialidad, ética, investigación y uso responsable de recursos tecnológicos.

El Reglamento de la Ley N.º 29733 regula expresamente el tratamiento de datos personales en entornos digitales, incluido el tratamiento mediante servicios tecnológicos tercerizados y los flujos internacionales de datos. El Reglamento de la Ley N.º 31814 establece, a su vez, principios y restricciones relacionados con privacidad, seguridad y gestión de riesgos en el uso de inteligencia artificial.

2. Principios, información tratada y finalidades

2.1. Principios aplicables

El tratamiento de información mediante LibreChat deberá observar los principios establecidos por la normativa vigente y las disposiciones institucionales aplicables.

En particular:

- la información deberá utilizarse para finalidades determinadas y legítimas;
- se tratará únicamente la información pertinente y necesaria para cada finalidad;
- deberá protegerse la confidencialidad de la información;
- deberán aplicarse medidas técnicas y organizativas de seguridad;
- se procurará minimizar la exposición innecesaria de información a terceros;
- los usuarios deberán poder conocer cuándo utilizan funcionalidades que implican procesamiento externo;
- la OTD mantendrá el control funcional y técnico de LibreChat y aplicará las medidas correspondientes para la protección de la información tratada mediante la plataforma.

2.2. Información tratada por LibreChat

Dependiendo de las funcionalidades utilizadas, LibreChat puede tratar las siguientes categorías de información:

- datos asociados a la cuenta institucional del usuario;
- prompts, preguntas e instrucciones;
- respuestas generadas por los modelos;
- historial y contexto de las conversaciones;
- archivos cargados;
- fragmentos e información procesada mediante File Search;
- configuraciones y archivos asociados a agentes;
- consultas realizadas mediante herramientas o conectores;
- información recuperada desde sistemas integrados;
- registros técnicos y de seguridad;
- información relacionada con el uso de modelos y consumo de créditos.

Los usuarios deberán proporcionar únicamente la información necesaria para realizar sus actividades y verificar que cuentan con autorización para utilizar información perteneciente a terceros.

2.3. Finalidades del tratamiento

La información tratada mediante LibreChat podrá utilizarse, según corresponda, para:

- proporcionar las funcionalidades de conversación e inteligencia artificial;

- procesar las solicitudes realizadas por los usuarios;
- permitir la consulta y análisis de documentos;
- mantener el historial y continuidad de las conversaciones;
- permitir la creación y utilización de agentes;
- ejecutar las herramientas y servicios habilitados por el usuario;
- administrar cuentas y permisos;
- gestionar el consumo de créditos y recursos;
- mantener la operación técnica de la plataforma;
- diagnosticar y solucionar errores;
- proteger la seguridad de LibreChat;
- investigar incidentes de seguridad;
- cumplir obligaciones institucionales y legales.

La información no deberá utilizarse para finalidades incompatibles con aquellas que justificaron su recopilación o tratamiento.

3. Infraestructura, modelos y procesamiento externo

3.1. Infraestructura de LibreChat

La infraestructura principal de LibreChat se encuentra desplegada en servicios de **computación en la nube bajo un modelo de Infraestructura como Servicio (IaaS)**, con recursos de procesamiento ubicados en **Estados Unidos**, y es administrada por la OTD.

En consecuencia, el procesamiento realizado directamente por la infraestructura de LibreChat se efectúa físicamente fuera del territorio peruano, aun cuando dicha infraestructura se encuentre bajo administración de la OTD.

3.2. Modelos locales

Para efectos de esta Política, se denomina “**modelo local**” a aquel cuya inferencia se realiza dentro de la infraestructura de LibreChat administrada por la OTD, sin que sea necesario enviar el contenido de la solicitud al proveedor externo del modelo para realizar dicha inferencia.

La denominación “local” hace referencia al **control y administración de la infraestructura**, y no a su ubicación geográfica.

Cuando se utiliza un modelo local, los prompts y el contexto utilizados para realizar la inferencia permanecen dentro de la infraestructura administrada por la OTD y no requieren ser transmitidos a un proveedor adicional del modelo.

Por ello, cuando la capacidad del modelo resulte suficiente y la confidencialidad sea un criterio relevante, se recomienda privilegiar el uso de modelos locales.

El uso de un modelo local no implica necesariamente que toda la interacción permanezca dentro de la infraestructura administrada por la OTD si se utilizan simultáneamente herramientas o servicios externos.

3.3. Modelos procesados por proveedores externos

LibreChat también permite utilizar modelos cuya inferencia se realiza en infraestructura de proveedores externos.

En estos casos, la información necesaria para atender la solicitud puede ser transmitida al proveedor correspondiente, incluyendo, según la interacción:

- prompts;
- instrucciones;

- partes relevantes del historial;
- contenido incorporado mediante archivos;
- fragmentos recuperados mediante File Search;
- resultados obtenidos mediante herramientas.

El uso de estos modelos implica la intervención de un proveedor adicional en el procesamiento de la información.

3.4. Proveedores externos y procesamiento internacional

Además de la infraestructura de LibreChat administrada por la OTD, determinados modelos, herramientas y servicios pueden requerir el envío de información a proveedores externos.

En consecuencia, el procesamiento de información mediante LibreChat puede producirse:

- dentro de la infraestructura de LibreChat administrada por la OTD;
- en la infraestructura de proveedores externos utilizados mediante LibreChat;
- mediante una combinación de ambos escenarios.

En el ámbito de LibreChat, la **OTD aplicará las disposiciones correspondientes al tratamiento mediante servicios tecnológicos tercerizados y al procesamiento internacional de datos personales conforme a la normativa vigente.**

Cuando se utilicen proveedores externos, la OTD procurará emplear configuraciones y condiciones de servicio que reduzcan la exposición innecesaria de información y que resulten compatibles con los niveles de protección requeridos.

4. Archivos, agentes, herramientas y conectores

4.1. File Search

File Search permite procesar e indexar documentos y recuperar los fragmentos relevantes para responder las consultas mediante mecanismos de recuperación aumentada o RAG (*Retrieval-Augmented Generation*).

El documento no necesita incorporarse íntegramente al contexto en cada consulta.

Cuando se utiliza File Search:

- con un modelo local, los fragmentos recuperados pueden procesarse dentro de la infraestructura administrada por la OTD;
- con un modelo externo, los fragmentos necesarios para responder pueden ser enviados al proveedor de dicho modelo.

Por ello, File Search no implica por sí mismo que todo el procesamiento posterior permanezca dentro de la infraestructura administrada por la OTD.

4.2. Upload as Text

La opción **Upload as Text** incorpora el contenido textual extraído del archivo al contexto de la conversación.

Si posteriormente se utiliza un modelo externo, el contenido necesario para generar la respuesta podrá formar parte de la información enviada al proveedor correspondiente.

4.3. Upload to Provider

La opción **Upload to Provider** transmite directamente el archivo al proveedor externo del modelo para utilizar las capacidades nativas de procesamiento que dicho proveedor ofrece.

En esta modalidad, el archivo es tratado mediante la infraestructura del proveedor externo.

No deberá utilizarse esta opción con información cuya transferencia a terceros no se encuentre autorizada.

4.4. Agentes y Marketplace

LibreChat permite crear agentes que pueden almacenar instrucciones, configuraciones, archivos, fuentes de conocimiento y referencias a herramientas necesarias para su funcionamiento.

Cuando un agente sea publicado en el **Marketplace institucional**, su configuración no deberá exponer datos personales, información confidencial, credenciales u otra información cuyo acceso deba permanecer restringido.

La publicación de agentes deberá realizarse conforme a las Condiciones de uso de LibreChat y en coordinación con la OTD cuando corresponda.

4.5. Herramientas, Web Search, conectores y servidores MCP

LibreChat puede integrarse con herramientas, servicios de búsqueda web, conectores, servidores MCP y otros sistemas institucionales o externos.

El uso de estas funcionalidades puede requerir que determinada información sea transmitida al servicio correspondiente.

Por ello, **la utilización de un modelo local no significa necesariamente que toda la interacción permanezca dentro de la infraestructura administrada por la OTD** si se utilizan simultáneamente servicios externos.

La OTD aplicará a las integraciones con terceros las disposiciones y medidas que correspondan conforme a la normativa aplicable y las condiciones de los servicios utilizados.

5. Tratamiento de información protegida y usos especiales

5.1. Datos sensibles y tratamientos de especial riesgo

Como política institucional de carácter conservador, **los usuarios no deberán incorporar datos sensibles a LibreChat.**

Esto comprende, entre otros, datos relacionados con:

- salud;
- biometría;
- origen racial o étnico;
- convicciones políticas, religiosas, filosóficas o morales;
- información económica personal cuando tenga naturaleza sensible;
- características físicas, emocionales o familiares pertenecientes a la esfera íntima;
- otras categorías consideradas sensibles por la normativa aplicable.

Excepcionalmente, el tratamiento de datos sensibles mediante LibreChat podrá realizarse cuando exista una finalidad institucional o de investigación legítima y previamente definida, el tratamiento se encuentre autorizado conforme a la normativa de protección de datos personales y **el caso de uso haya sido previamente evaluado y autorizado por las instancias institucionales competentes.**

No podrá autorizarse mediante LibreChat ningún tratamiento que constituya un **uso indebido de inteligencia artificial** conforme a la normativa vigente.

Los casos que puedan corresponder a **usos de riesgo alto** deberán ser previamente evaluados institucionalmente y estarán sujetos a los controles que resulten aplicables. El Reglamento de la Ley N.º 31814 distingue entre usos indebidos, de riesgo alto y de riesgo aceptable y establece restricciones específicas para determinadas aplicaciones de inteligencia artificial.

Cuando resulte posible alcanzar la finalidad sin identificar a las personas, deberán utilizarse previamente mecanismos de anonimización o disociación.

Cuando un tratamiento excepcional de datos sensibles haya sido autorizado y pueda realizarse adecuadamente mediante un modelo local, deberá privilegiarse esta modalidad para reducir la intervención de proveedores externos adicionales.

5.2. Información académica

Cuando el personal docente utilice LibreChat deberá observar adicionalmente los lineamientos establecidos por la **Dirección de Asuntos Académicos (DAA)**.

Deberá evitarse incorporar innecesariamente:

- datos personales de estudiantes;
- calificaciones identificables;
- información académica confidencial;
- trabajos de estudiantes que contengan información personal;
- información cuya divulgación pueda afectar la privacidad de miembros de la comunidad universitaria.

Cuando resulte necesario utilizar información relacionada con estudiantes para una actividad autorizada, deberá minimizarse la información utilizada y, cuando resulte posible, aplicarse mecanismos de anonimización o disociación.

5.3. Información utilizada en investigación

Cuando LibreChat sea utilizado en actividades de investigación deberán respetarse:

- las condiciones bajo las cuales fueron obtenidos los datos;
- los consentimientos que correspondan;
- los protocolos de investigación;
- las obligaciones de confidencialidad;
- las disposiciones de los comités de ética que resulten aplicables;
- las condiciones establecidas por financiadores, colaboradores o terceros.

La autorización para utilizar LibreChat no constituye por sí misma autorización para tratar datos personales o sensibles procedentes de una investigación.

Siempre que resulte posible deberán utilizarse datos anonimizados o disociados.

6. Registros, conservación y seguridad

6.1. Registros técnicos y de seguridad

Con la finalidad de proteger la plataforma, administrar su funcionamiento y diagnosticar problemas, LibreChat y los componentes tecnológicos asociados generan registros técnicos o **logs**.

Estos pueden incluir, dependiendo del componente:

- fecha y hora de las operaciones;
- identificadores técnicos;
- información sobre el modelo o herramienta utilizada;
- errores;
- eventos de autenticación;
- eventos de seguridad;
- información técnica necesaria para investigar incidentes.

La información registrada se limita a la necesaria para las finalidades operativas y de seguridad correspondientes.

Los registros relacionados con el tratamiento de datos personales se conservan durante los **plazos establecidos por la normativa aplicable y las disposiciones institucionales correspondientes**.

La OTD administra estos registros como parte de la operación y seguridad de LibreChat.

6.2. Conservación y eliminación de información

La información tratada mediante LibreChat se conservará durante el tiempo requerido para cumplir las finalidades institucionales correspondientes y de acuerdo con las disposiciones legales e institucionales aplicables.

Los periodos de conservación pueden variar según se trate de:

- datos de cuenta;
- conversaciones;
- archivos;
- información de File Search;
- agentes;
- registros de uso y consumo;
- logs;
- copias de respaldo.

Cuando corresponda, la información podrá ser eliminada mediante las funcionalidades disponibles para el usuario o a través de los procedimientos institucionales aplicables.

La eliminación desde la interfaz de LibreChat podrá requerir procesos adicionales para completar la eliminación en sistemas auxiliares o respaldos, de acuerdo con las políticas técnicas y de conservación aplicables.

6.3. Seguridad y confidencialidad

La OTD aplicará medidas técnicas y organizativas orientadas a proteger la información tratada mediante LibreChat.

Estas comprenden, según corresponda:

- autenticación;
- control de acceso;
- administración de permisos;
- protección de infraestructura;
- registros técnicos y de seguridad;
- respaldo de información;
- actualización y mantenimiento de componentes;
- monitoreo;
- mecanismos para prevenir accesos no autorizados.

Los usuarios que tengan acceso a datos personales o información confidencial deberán mantener su reserva conforme a las disposiciones institucionales y legales aplicables.

Las medidas de seguridad de la plataforma no sustituyen las obligaciones del usuario respecto de la información a la que tiene acceso en el ejercicio de sus funciones.

7. Incidentes y consultas

Los usuarios deberán comunicar oportunamente cualquier incidente relacionado con LibreChat que pueda comprometer:

- datos personales;
- datos sensibles;

- información confidencial;
- credenciales;
- sistemas institucionales;
- seguridad de la información;
- derechos de personas o terceros.

También deberá reportarse el ingreso accidental de información protegida en un proveedor o servicio externo cuando exista riesgo de tratamiento no autorizado.

Las consultas e incidentes relacionados con LibreChat podrán comunicarse a:

Oficina de Transformación Digital (OTD)

txdigital@pucp.edu.pe

La OTD gestionará el incidente y, cuando corresponda, coordinará o derivará su atención a las instancias institucionales competentes conforme a los procedimientos y obligaciones aplicables.

8. Actualización de la Política

Esta Política podrá actualizarse cuando se produzcan cambios relevantes en:

- la normativa aplicable;
- la arquitectura o infraestructura de LibreChat;
- los modelos de inteligencia artificial disponibles;
- los proveedores externos;
- las herramientas, conectores o integraciones;
- las condiciones de tratamiento, conservación o seguridad de la información;
- las disposiciones institucionales aplicables.

La versión vigente de esta Política deberá mantenerse disponible para los usuarios de LibreChat.

La interpretación y aplicación de esta Política se realizará conforme al marco normativo e institucional señalado en la sección 1.3.