ORPALAB · Hermes Agent v0.21.5

# Preguntas frecuentes y seguridad de Hermes

Aprenda a revisar resultados y resolver errores. Sesión es una conversación; perfil reúne ajustes y accesos. Una aprobación depende de los ajustes de la empresa y no garantiza que el resultado sea correcto.

Abra el tema en el índice; la numeración corresponde a este PDF.


Qué hace solo y qué debe revisar 2

Contraseñas datos y privacidad 3

Revisar cálculos textos y entregas 4

Responder a errores frecuentes 5

Detener y reportar un incidente 6

Lo que no debe hacer 7

Cuide los datos personales y confidenciales 8

Glosario para usar Hermes 9


Los controles pueden variar según la versión y los permisos. Use los ajustes autorizados. Si su pantalla es distinta, pida ayuda al administrador de Hermes de su entidad.

Video: A14 – Cuidar los datos personales y confidenciales
Escanee el código o abra orpalab.com/formacion y busque A14

ORPALAB · Hermes Agent v0.21.5

# Qué hace solo y qué debe revisar

Hermes puede interpretar un pedido y utilizar herramientas habilitadas. Que una tarea parezca de solo lectura no significa que todas las herramientas tengan confirmación previa.

### ¿Pide permiso antes de cada acción?

No hay una garantía universal. El modo de aprobaciones, las herramientas, permisos y reglas de la instalación influyen. El modo off o YOLO (modo que omite algunas confirmaciones) puede omitir confirmaciones de comandos peligrosos. No los cambie para avanzar más rápido.

### ¿Qué conviene pedir primero?

Un plan, un borrador o una consulta con fuentes y pendientes. Para enviar, publicar, modificar un portal, pagar o borrar, haga que el administrador defina permisos y controles; no confíe solo en una frase de chat.

### ¿Qué reviso en una aprobación?

La acción exacta, destino, destinatarios, datos, archivos y efectos. Rechace si falta algo o no coincide con lo pedido. Apruebe una acción puntual; no dé permiso permanente por comodidad.

### ¿Aprobado significa recibido?

No. Una aprobación permite intentar una acción. Exija evidencia posterior de ejecución y, cuando corresponda, de recepción.

### ¿Puede decidir por mí?

La revisión de resultados y las decisiones del proceso siguen en el responsable autorizado. El agente puede equivocarse incluso si su redacción parece convincente.

**Para la formación:** solo datos ficticios; sin correos reales, publicaciones, pagos ni portales reales.

Video: A13 – Aprobaciones: cuándo pide permiso y cómo responder
Escanee el código o abra orpalab.com/formacion y busque A13

ORPALAB · Hermes Agent v0.21.5

# Contraseñas datos y privacidad

### ¿Dónde guardo una contraseña?

En Settings → Passwords & Logins, o en el campo protegido autorizado. Nunca en el chat, audio, adjunto ni captura.

### ¿La bóveda (lugar para accesos autorizados) protege todo?

Protege los secretos con mecanismos de cifrado y llenado limitado al sitio. No garantiza que el equipo o sitio sean seguros. Los nombres de usuario y dominios pueden ser metadatos visibles.

### ¿Qué datos puedo adjuntar?

Solo los necesarios y permitidos por su empresa. Quite contraseñas, información ajena y columnas innecesarias. Para practicar, use archivos ficticios.

### ¿Los datos siempre se quedan en el PC?

No debe asumirlo. Modelos, transcripción, navegación y herramientas pueden usar servicios externos. Consulte la configuración y política aprobadas antes de procesar datos reales.

### ¿Una sesión (conversación con su historial) nueva borra todo?

No. Cambia el hilo de conversación, pero puede existir memoria, historial, archivos o registros persistentes.

### ¿Qué hago si expuse una clave?

Detenga la tarea y active el procedimiento interno de revocación o rotación. Conserve solo la evidencia necesaria; no vuelva a copiar el secreto. Pedir que lo olvide no elimina necesariamente todas las copias.

### ¿Envío capturas al soporte?

Revise antes y oculte claves, otros chats, nombres, rutas personales, cuentas y documentos. Use únicamente el canal interno autorizado.

Video: A06 – Guardar la contraseña de un portal en la bóveda
Escanee el código o abra orpalab.com/formacion y busque A06

ORPALAB · Hermes Agent v0.21.5

# Revisar cálculos textos y entregas

### ¿Cómo sé si un cálculo está bien?

Compare hojas y filas usadas, filtros, sumas generales y por grupo. Revise duplicados, vacíos, unidades y período. Pida las fórmulas o el método, y recalcule lo necesario.

### ¿Puedo usar el oficio tal como sale?

Revise hechos, fecha, destinatario, cuantía, petición y firma. Los datos no suministrados deben quedar pendientes. Un borrador no es una actuación firmada o radicada.

### ¿Y una tabla extraída de una foto?

Compare cada campo crítico contra la fuente. El reconocimiento puede confundir caracteres, decimales y separadores. Lo ilegible se marca, no se completa.

### ¿Qué verifico en un dashboard (panel de indicadores)?

Pruebe filtros, totales, unidades y etiquetas. Compruebe que abre en el entorno autorizado. Un HTML local no acredita publicación ni actualización automática.

### ¿Qué le pido como evidencia?

Fuente, fecha de corte, archivos usados, acciones confirmadas, método, faltantes y error exacto. Ajuste esa evidencia a la tarea; no añada datos sensibles innecesarios.

> Antes de cerrar, indique la fuente, el período, los totales de control, qué revisó y qué no pudo verificar. Entregue la versión vigente y conserve el original.

### Regla de aceptación

El resultado debe poder comprobarse. Si no hay evidencia suficiente, manténgalo como borrador y pida revisión humana.

Video: A15 – Verificar lo que responde Hermes
Escanee el código o abra orpalab.com/formacion y busque A15

ORPALAB · Hermes Agent v0.21.5

# Responder a errores frecuentes

| Lo que ocurre | Qué hacer |
|---|---|
| No responde o pierde conexión | Anote hora y error. Revise su conexión; consulte soporte. No reinicie gateways (servicios de conexión entre canales) por su cuenta. |
| No active task o no hay tarea activa | No había una tarea que detener. No demuestra que stop falle ni que una operación anterior se revirtió. |
| Comando desconocido o sin permiso | Revise comando con /, canal y catálogo. Consulte al administrador; no cambie de cuenta para eludir el bloqueo. |
| Archivo no encontrado | Confirme que se adjuntó; una ruta puede pertenecer a otro equipo. Solicite adjunto o descarga. |
| Respuesta incompleta | Pida archivo o resumen y confirme la cobertura. No use cifras parciales. |
| Autenticación o cuota agotada | Conserve el error y consulte soporte. No copie claves ni cambie a un proveedor no aprobado. |
| Datos o totales incorrectos | Señale la celda o campo, adjunte la fuente vigente y pida corrección con método. |

### No repita a ciegas

Antes de /retry, compruebe si hubo una acción externa. Si el estado es desconocido, pida confirmar qué ocurrió en el destino; no lance otro envío.

> Indique qué recibió, qué intentó, qué quedó confirmado y el error exacto. No reintente ni cambie ajustes. Deje lo pendiente para revisión.

Video: A16 – Cuando algo no funciona
Escanee el código o abra orpalab.com/formacion y busque A16

ORPALAB · Hermes Agent v0.21.5

# Detener y reportar un incidente

1. Si hay riesgo en el trabajo activo, use **/stop**. No lo interprete como una reversión de todo lo ocurrido.
2. Pida un estado: acciones confirmadas, archivos cambiados y operaciones pendientes. Si no sabe si se envió, compruebe el destino antes de repetir.
3. Conserve hora, sesión (conversación con su historial), mensaje de error e identificadores necesarios, sin copiar secretos.
4. Informe al responsable interno según el procedimiento de su empresa. No publique registros ni use **/debug** para subirlos por su cuenta.
5. Corrija mediante el procedimiento aprobado. No borre evidencia ni cambie registros para ocultar el incidente.

### ¿Qué hace undo?

Retrocede turnos del diálogo. No garantiza deshacer archivos ni comunicaciones. La restauración de archivos requiere una función específica y revisión; no restaura por sí sola un sistema externo.

### ¿Qué hace new?

Abre una conversación nueva. No cancela necesariamente tareas programadas ni elimina memoria y archivos.

### ¿Qué reporto?

Qué quería hacer, qué pasó, hora, fuente, estado confirmado, impacto conocido y pendientes. Si el impacto no se conoce, dígalo. No invente que todo quedó restaurado.

> Detenga el trabajo. Separe lo confirmado de lo desconocido. Muestre qué evidencia puedo conservar sin datos sensibles. No borre ni revierta nada externo sin un plan aprobado.

### Continuidad

Si el agente no está disponible, use el procedimiento alterno de su empresa y mantenga registro de qué hizo manualmente.



Video: A09 – Los 3 básicos: /new, /status y /stop
Escanee el código o abra orpalab.com/formacion y busque A09

ORPALAB · Hermes Agent v0.21.5

# Lo que no debe hacer

- No envíe contraseñas, tokens ni códigos de verificación en el chat.
- No use un bot desconocido ni comparta documentación en chats de personas o grupos no autorizados.
- No cambie aprobaciones, YOLO (modo que omite algunas confirmaciones), proveedores, claves, gateways (servicios de conexión entre canales) ni herramientas para resolver una tarea urgente.
- No apruebe un envío sin revisar destinatarios, adjuntos y contenido.
- No use resultados no comprobados como cifras oficiales.
- No ejecute macros, programas o enlaces sospechosos porque el agente lo sugiera.
- No enseñe una habilidad con secretos o datos reales innecesarios.
- No deje tareas de prueba, accesos ficticios o habilidades de práctica activos al terminar.
- No confunda la edición del contenido de un documento con su firma, envío o radicación.

### ¿Las habilidades son permisos?

No. Una habilidad carga instrucciones de trabajo; no concede por sí sola autorización. Algunas habilidades presentes en esta instalación son específicas de un sector o requieren herramientas adicionales.

### ¿Puedo pedir cualquier portal?

Solo dentro de su autorización y de las herramientas aprobadas. Para aprender, use un portal local ficticio. No use la guía para experimentar con una plataforma real.

### ¿Puedo distribuir esta formación?

Distribuya solo la formación aprobada por su entidad. Para funciones técnicas, pida ayuda al administrador de Hermes de su entidad.

Video: A14 – Cuidar los datos personales y confidenciales
Escanee el código o abra orpalab.com/formacion y busque A14

ORPALAB · Hermes Agent v0.21.5

# Cuide los datos personales y confidenciales

Hermes trabaja mejor con información, pero no toda debe entrar al chat. Son confidenciales los datos personales (cédula, dirección, teléfono), los de salud (historias clínicas, diagnósticos) y los accesos (contraseñas, códigos de verificación). Un texto pegado o un archivo adjunto puede ser procesado por servicios configurados fuera del equipo.

1. Antes de pegar o adjuntar, pregúntese si Hermes necesita ese dato para la tarea. Si no lo necesita, quítelo: nombres, números de documento, columnas completas.
2. Practique con datos de ejemplo, como un archivo ficticio. Use datos reales solo si su empresa lo autorizó para esa tarea concreta.
3. Guarde las contraseñas únicamente en la bóveda (lugar para accesos autorizados). No las escriba en el chat ni dicte los códigos de verificación que le lleguen por mensaje.
4. Si pegó un dato que no debía, deje de escribir. No intente borrarlo a escondidas ni pida a Hermes que lo «olvide»: eso no elimina las copias. Avise a sistemas con la hora, la conversación y el tipo de dato, sin repetir el dato.

> Use solo las columnas Sede, Fecha y Valor del archivo adjunto. No repita nombres ni números de documento en la respuesta. No envíe nada.

### Qué verá

Una respuesta que usa solo lo que le indicó. Compruebe que no repite datos personales; si lo hace, avise a sistemas.

> **Recuerde.** Ante la duda, pregunte antes de pegar. Un dato enviado puede quedar en el historial y en los servicios configurados.



Video: A14 – Cuidar los datos personales y confidenciales
Escanee el código o abra orpalab.com/formacion y busque A14

ORPALAB · Hermes Agent v0.21.5

# Glosario para usar Hermes

Consulte esta página cuando una palabra de la pantalla le resulte desconocida.

**Sesión:** Una conversación con sus mensajes y archivos. Use una por tema.

**Contexto:** La información que Hermes tiene a mano para responder: mensajes, archivos y decisiones.

**Perfil:** El conjunto de ajustes, accesos e instrucciones de un agente. Use el asignado por su empresa.

**Modelo:** El servicio de inteligencia artificial que interpreta su pedido y prepara una respuesta.

**Esfuerzo:** Cantidad de razonamiento solicitada al modelo; puede tardar más y no garantiza acierto.

**Herramienta:** Una función para leer un archivo, calcular o usar una aplicación.

**Después de una herramienta:** Cuando termine la siguiente operación que el agente haya iniciado; una corrección puede esperar hasta entonces.

**Skill o habilidad:** Una receta de instrucciones reutilizable. Las instaladas varían entre empresas.

**Toolset:** Un grupo de herramientas. Activarlo no demuestra que tenga los accesos necesarios.

**MCP:** Forma de conectar herramientas de otro servicio con Hermes. Lo configura sistemas.

**Gateway:** Servicio que comunica Hermes con canales como Telegram. Lo administra sistemas.

**Terminal o CLI:** Ventana donde se escriben órdenes técnicas. TUI es una interfaz de texto de esa ventana.

**Bóveda:** Lugar de la aplicación para guardar accesos autorizados sin pegarlos en el chat.

**YOLO:** Modo que omite confirmaciones para ciertos comandos peligrosos. No lo active.

**Artifacts:** Galería de referencias de 30 sesiones recientes. No es un respaldo ni asegura que el archivo siga existiendo.

**Dashboard:** Panel de indicadores para comparar cifras y ver gráficos.

**Memoria:** Notas breves que Hermes guarda para conversaciones futuras, como una preferencia de trabajo. No guarde datos confidenciales.

**Aprobación:** Permiso que Hermes pide antes de una acción delicada. Lea la acción exacta antes de aceptar; depende de los ajustes de su empresa.

**Tarea programada (cron):** Tarea que Hermes ejecuta sola a una hora fijada, incluso con la ventana cerrada. La autoriza sistemas.

**Conversación nueva (/new):** Comando que abre una conversación en blanco. No borra archivos ni deshace acciones; la memoria se conserva.

Video: A02 – Hermes Desktop: dónde está cada cosa
Escanee el código o abra orpalab.com/formacion y busque A02