

ASISTENTES Y AGENTES DE IA

QUE LA IA ACTÚE POR TI, **NO SIN TI**

Decálogo para personas usuarias

1 ANTES DE DELEGAR, REVISA A QUIÉN LE DAS LAS LLAVES



Un asistente con acceso a tu correo, tu agenda, tus archivos o tus pagos **es una llave a buena parte de tu vida digital**. Revisa quién presta el servicio, qué hace con tus datos y qué controles te ofrece.

■ Elige **servicios claramente identificados** (que sepas qué empresa está detrás y cómo contactar con ella), que te permitan ejercer tus derechos y defenderlos legalmente en la UE, y que digan claramente adónde se envían tus datos.

■ Revisa las **opciones de privacidad, memoria e historial**, y si tus datos se usan para fines ajenos a tu interés, como el marketing. Si no quieres esos usos, desactívalos cuando el servicio lo permita. Ten en cuenta que, si permites que se usen tus datos para desarrollar modelos de IA, podría ser difícil eliminarlos después.

■ Desconfía de asistentes o agentes de **origen desconocido**, sean gratuitos o de pago, y especialmente de los que piden acceso a todo tu dispositivo o a información que no necesitan para su tarea.

■ Da prioridad a asistentes que procesen tus datos en tu propio dispositivo (móvil, ordenador...), **sin enviarlos a servidores externos**.

■ Elige un asistente **que te informe de qué datos guarda sobre ti** (incluidos los perfiles y los datos que deduce) y te permita consultarlos y eliminarlos, con herramientas del propio servicio o ejerciendo tus derechos. Y que te deje comprobar a qué ha accedido, cuándo y qué ha cambiado en cada tarea, y deshacer los cambios con los que no estés de acuerdo.

2 CONCEDE ACCESOS, NO CHEQUES EN BLANCO

Que pueda acceder a tu correo, tus contactos, tus fotos o tu ubicación no significa que lo necesite. Leer no es lo mismo que enviar, modificar o borrar. Y aceptar todos los permisos por cansancio no es tener el control.

■ Cuando el servicio te deje elegir, dale el acceso mínimo: que te pida permiso antes de abrir información que consideres delicada; que solo pueda leer, pero no modificar ni borrar sin tu visto bueno; y que acceda solo a lo necesario (una carpeta, un calendario), no a toda la cuenta ni a todo el dispositivo. Si no puedes limitarlo, valora si la tarea justifica conectar todo el servicio.

■ Revisa periódicamente qué tienes conectado, y de nuevo cuando el asistente o una aplicación incorporen funciones nuevas. Deshabilita y desconecta lo que no uses.

3 DALE LO MÍNIMO Y PROTEGE LO DELICADO

Cuanta más información tenga, mayor es el daño si se equivoca, si lo engañan o si alguien entra en tu cuenta. **Cuanto más delicados sean los datos** (salud, situación económica, identidad, contraseñas), **más limitado debe ser el acceso y la autonomía del agente.**

■ No escribas contraseñas, códigos de verificación ni números de tarjeta en la conversación. Cuando haya que identificarse o pagar, introduce tú esos datos en el formulario o espacio seguro destinado a ello.

■ Antes de darle un documento, elimina los nombres y los datos que no necesite para llevar a cabo la tarea.

4 DECIDE QUÉ PUEDE RECORDAR DE TI

La memoria hace al asistente más útil, pero construye poco a poco un perfil con tus gustos, relaciones, rutinas, preocupaciones o datos de las aplicaciones conectadas. Un dato trivial, sumado a muchos otros durante meses, acaba describiendo tu vida.

- Para eliminar información, **usa los controles de memoria**, historial y privacidad del servicio; no confíes solo en pedirselo en la conversación. Ten en cuenta que borrar un chat, borrar una memoria o eliminar una aplicación conectada no tienen el mismo efecto.
- Además de lo que *recuerda* para ayudarte, el servicio guarda tus datos para otros fines: seguridad, detección de abusos, registros técnicos, perfiles y puntuaciones sobre ti, avisos sobre tu actividad o datos de tu ubicación, entre otros. **Cada vez que lo usas puede generar datos nuevos sobre ti o deducirlos.** Estos datos también pueden estar en manos de empresas que trabajan para el proveedor o conservarse por orden judicial. Para conocer esa información, ejerce tu derecho de acceso; para eliminarla, tu derecho de supresión.



- Cuando tu asistente usa **servicios de terceros** para hacer tus tareas (por ejemplo, una web de reservas o una tienda online), o accede a ellos con fines de marketing, la información que queda guardada en esos servicios queda al margen de la gestión del asistente. Para eliminarla, dirígete a cada uno de ellos.
- Usa conversaciones temporales para asuntos delicados y, cuando el servicio lo haga posible, **separa los usos personal, familiar y profesional** en cuentas, perfiles o espacios distintos.
- Revisa **dónde se hacen las copias de seguridad** de tus datos y que estén protegidas con una clave elegida por ti.

5 DILE TAMBIÉN LO QUE NO DEBE HACER

Un agente puede hacer algo más que ejecutar una **instrucción puntual**: perseguir un objetivo, dividirlo en pasos y decidir cómo realizarlos. “Organiza la cena” o “revisa mi correo y encárgate de todo” equivale a darle carta blanca.

■ **Di qué quieres y también qué no**: a quién puede escribir, cuánto puede gastar, qué no debe tocar y cuándo debe parar y preguntarte. Empieza por tareas pequeñas y reversibles.

■ Evita reunir en una misma tarea **contenido procedente de desconocidos, acceso a tu información privada y capacidad de actuar en tu nombre**. Si necesitas combinarlas, exige tu confirmación antes de cualquier acción externa. Los límites que escribas en la instrucción orientan al agente, pero no sustituyen a los permisos y las confirmaciones.



G CONFIRMA LO IMPORTANTE



Cuando el asistente solo responde, un error es una respuesta equivocada. Cuando actúa, es un correo enviado, un archivo compartido, una compra, un contrato o un consentimiento dado en tu nombre.

■ Recuerda que **puedes ser responsable** de las acciones que has permitido ejecutar a tu agente.

■ Cuando el servicio lo permita, activa la **confirmación previa** para enviar, publicar, compartir, borrar, pagar, contratar o aceptar condiciones. No concedas autorizaciones permanentes para actuar sin preguntarte (“permitir siempre”) salvo que sean realmente necesarias y comprendas su alcance.

■ **Lee de verdad lo que apruebas**: destinatario, importe, fecha, adjunto. Un resumen puede ocultar lo esencial. No pulses “aprobar todo” para que deje de preguntar.

■ **No dejes que ejecute sin tu revisión** decisiones con consecuencias legales (como firmar o aceptar un contrato), económicas o de salud, ni las que afecten seriamente a otra persona. Los asistentes pueden equivocarse y presentar una respuesta incorrecta con apariencia de seguridad.

7 DESCONFÍA TAMBIÉN DE LO QUE LEE

Una web, un correo, un PDF o una invitación de calendario pueden contener instrucciones ocultas, incluso invisibles para ti (texto blanco sobre fondo blanco), para que el agente haga algo distinto de lo que le pediste, como enviar tus datos, abrir un enlace o aprobar algo. Ninguna medida elimina por completo este riesgo; por eso la mejor protección es limitar lo que el agente puede hacer si consigue ser engañado. Cuanto más contenido ajeno maneje (correos, webs, documentos de otros), menos acceso y capacidad de actuar debe tener sobre tus datos y tus cuentas.

■ Evita las tareas en las que el agente resuma o gestione contenido de desconocidos (correos, archivos o webs) y, a la vez, tenga acceso a tu información privada y pueda actuar en tu nombre. Por ejemplo: “resume mis correos nuevos y responde a todos”. Si necesitas combinarlas, haz que te pida confirmación antes de cualquier acción hacia fuera (como enviar, compartir, pagar o publicar).

■ Si te pide una contraseña o un código, te urge a aprobar algo, visita sitios inesperados o propone un enlace, detén la tarea y revísala antes de continuar.

■ Configura, acepta o crea limitaciones sobre servicios externos a los que pretende acceder el agente.



8 PROTEGE TAMBIÉN LOS DATOS DE LOS DEMÁS

En tu correo, tu agenda, tus contactos, tus fotos y tus chats **hay información de familiares, amigos, compañeros, clientes o pacientes que no han decidido relacionarse con esa inteligencia artificial.** Si das autorización al agente para que acceda a esas fuentes, podrá tratar la información de terceros. Que tú lo autorices no te da vía libre para utilizar la información de los demás.

- Antes de conectar una fuente de datos, **piensa quién más está en ella y limita el alcance cuando puedas.** No lo uses para reunir o deducir información delicada de otras personas (salud, ideología, situación económica...) ni para tomar decisiones que les afecten sin pensar antes si es apropiado y si la ley lo permite.
- Si se comunica con otras personas en tu nombre, **evita que se confundan sobre quién está actuando** (tú o el asistente) y extrema la precaución si utiliza tu voz, tu imagen o tu identidad.
- En **dispositivos compartidos**, usa perfiles separados. Si lo usan menores, crea también perfiles para ellos y acompáñalos mientras lo usan.



9 PROTEGE TU CUENTA Y TU DISPOSITIVO: SON LA LLAVE DE TODO LO DEMÁS

La cuenta del asistente da acceso a todo lo que tiene conectado. Quien la controle, o quien logre que instales un complemento malicioso, puede leer tu correo, suplantarte o gastar tu dinero.

■ Usa una contraseña única y segura, activa la verificación en dos pasos (o una llave de acceso, passkey) y los avisos de inicio de sesión. No dejes sesiones abiertas en dispositivos que utilizan otras personas y revisa periódicamente dónde tienes iniciada sesión.

■ Instala solo complementos (extensiones que añaden funciones al asistente) y conectores (que lo enlazan con otras aplicaciones) de origen conocido, y comprueba qué permisos piden.

■ Si el agente controla un navegador o tu ordenador, ten presente que podría acceder a las páginas en las que hayas iniciado sesión y procesar lo que aparezca en pantalla. Para tareas delicadas, usa cuando sea posible un perfil o una sesión separados y elimina después las sesiones, cookies o accesos que ya no necesites.

■ Si tienes en el dispositivo información que consideres muy sensible, guárdala cifrada y descífrala solo cuando el agente esté desactivado.



10 SUPERVÍSALO, APRENDE A PARARLO Y RETIRA SUS ACCESOS

■ **Delegar no es desentenderse.**

Averigua cómo detener el agente y cómo retirarle los accesos antes de necesitarlo. Prepárate para cuando tus datos o tu dispositivo se vean comprometidos (por ejemplo, por un acceso no autorizado o un programa malicioso).

■ Comprueba que las actualizaciones del agente no cambian tu configuración ni amplían lo que hace con tus datos más allá de lo que te interesa.

■ Revisa el **historial de actividad** que ofrezca el asistente y comprueba también en las aplicaciones afectadas qué mensajes se han enviado, qué archivos se han compartido, qué compras se han hecho o qué cambios se han producido.

■ En los servicios a los que pueda acceder el agente y en los que un problema podría afectarte seriamente, **configura avisos** que te alerten cuando haya actividad en ellos.

■ Presta especial atención a las tareas programadas, periódicas o que siguen funcionando sin que estés presente: limita cuánto duran, qué datos y servicios usan y qué pueden hacer sin preguntarte, y elimina las que ya no necesitas.

■ Si algo falla, deténlo, desconecta las aplicaciones afectadas, cambia las contraseñas, comprueba qué se ha enviado y avisa a quien pueda verse afectado (en el trabajo, a tu organización). Los datos que el servicio conserve sobre ti están sujetos a la normativa de protección de datos: puedes **ejercer los derechos** que correspondan, como acceso, rectificación o supresión, y reclamar ante la AEPD si consideras que no se han respetado.

■ Mantén **copias de tus datos** en otro dispositivo que te permita seguir haciendo las tareas más importantes si el principal falla, lo pierdes o tienes que bloquearlo.



SI LO USAS EN EL TRABAJO

Utiliza solo los **asistentes autorizados por tu organización y conecta únicamente las cuentas, aplicaciones y datos que esta haya autorizado**. Que puedas usar una herramienta en tu ámbito personal no significa que sea adecuada para uso profesional.

No instales agentes por tu cuenta en el equipo de trabajo ni conectes el correo o los documentos profesionales a una cuenta personal de IA. Los datos de clientes, pacientes, alumnos o ciudadanos siguen siendo responsabilidad de tu organización, y tú lo eres del uso que haces de ellos. Ante la duda, consulta a la persona delegada de protección de datos (DPD) de tu organización.

LO QUE PUEDES ESPERAR DEL PROVEEDOR DEL SERVICIO

La responsabilidad de los asistentes y agentes de IA no puede recaer solo en la persona usuaria.

Quien ofrece asistentes capaces de actuar por ti debería ofrecer también controles suficientes: permisos comprensibles que distingan consultar de actuar, confirmación configurable para las acciones de mayor impacto, un historial de lo que el agente ha hecho en nombre de la persona usuaria, una forma inmediata de detenerlo, gestión y borrado de la memoria, información clara sobre a quién se envían los datos y si se usan para entrenar la IA, y una vía sencilla para ejercer los derechos.

Si un servicio no te ofrece estos controles, tenlo en cuenta al decidir qué le confías.





WWW.AEPD.ES



[AEPD_ES](https://twitter.com/AEPD_ES)



[AEPD](https://www.linkedin.com/company/AEPD)



[@AEPD.ES](https://www.instagram.com/AEPD.ES)