

Lo que debes saber de los asistentes virtuales a nivel de privacidad

Ten en cuenta que...



Estos dispositivos, al utilizarlos, generan un historial de información que pueden aprovechar las empresas para **mostrarte publicidad dirigida** en función de tus gustos, preferencias, rutinas, ubicación, etc.



Además, tienen **acceso a tu información personal aportada** y esta puede verse expuesta si no se configura de manera correcta el dispositivo.



Alexa, Siri, Cortana y el asistente de Google son ejemplos de asistentes virtuales que nos facilitan tareas en nuestro día a día. **¿Su uso conlleva riesgos para la privacidad?**

- 1 Lee la **política de protección de datos** para tener claro el uso que el asistente hará de tus datos e información
- 3 No facilites **datos sensibles** a través de tu asistente.
- 5 Limita los **permisos del asistente y de los usuarios** que pueden interactuar con él.
- 7 No actives ni vincules el asistente con **dispositivos que no están bajo tu control** o cuyas medidas de seguridad desconozcas.



2 **Comprueba las configuraciones** que permite y ajústalas a los niveles de privacidad que desees. Algunos ejemplos:

4 **Asegúrate de que el dispositivo está actualizado** para corregir las posibles vulnerabilidades que se hayan identificado y que puedan afectar a tu privacidad.

- Elimina las redes wifi guardadas.
- Borra las ubicaciones almacenadas en la aplicación.
- Elige los datos que permites compartir con otras empresas.
- Revisa el historial de búsquedas y reproducciones. Elimina aquello que no desees que se mantenga almacenado. Programa el borrado de información de manera automática.
- Cambia regularmente las contraseñas de tu cuenta asociada al asistente.

6 **Conecta siempre el dispositivo a una red wifi segura.**

8 **Desconecta el asistente cuando no lo estés usando.**

¿Cómo usarlos para garantizar una mayor privacidad?



Los ciberdelincuentes pueden obtener **información confidencial sobre ti**, haciendo uso del asistente, **falseando tu voz**.



Si el sistema operativo del dispositivo tiene una **vulnerabilidad**, o el propio asistente, podría **comprometer tu privacidad**.