- **Soporte automatizado**
    - El software será fácil de usar y autónomo, lo que reducirá la necesidad de intervención directa. Sin embargo, los usuarios aún podrían tener preguntas o problemas ocasionales.
    - Base de conocimientos (FAQ): Crear una sección de preguntas frecuentes en tu sitio web, que cubra los problemas comunes que los usuarios puedan encontrar.
    - Tutoriales y guías interactivas: Incluir tutoriales dentro del software para guiar a los usuarios en la instalación y el uso, asegurando que se aprovechen al máximo las funciones de protección.
- **Atención al cliente**
    - Correo electrónico de soporte: Ofrecer un canal de atención al cliente por correo electrónico donde los usuarios puedan realizar consultas sobre el software.
    - Chat en vivo o soporte por tickets: Aunque el software sea autónomo, siempre es útil tener un canal de soporte técnico que pueda resolver problemas más complejos o proporcionar asistencia a empresas que puedan tener dudas.
- **Comunidad de usuarios**
    - Crear una comunidad en línea (en redes sociales, foros o a través de un blog) donde los usuarios puedan intercambiar experiencias, consejos y soluciones sobre problemas comunes relacionados con la ciberseguridad.
    - Fomentar la participación de los usuarios en redes sociales mediante contenido educativo sobre ciberseguridad, creando una red de personas que recomienden y apoyen el producto
- **Actualizaciones y mantenimiento**
    - Aunque el software sea autónomo, es probable que se necesiten actualizaciones periódicas para adaptarse a nuevas amenazas de ciberseguridad. Notificar a los clientes sobre nuevas versiones y mejoras es clave para mantener la relación.
    - Boletines informativos: A través de correos electrónicos o notificaciones dentro del software, puedes mantener a los usuarios informados sobre nuevas actualizaciones, características y consejos de ciberseguridad.
- **Seguimiento postventa**
    - En el caso de clientes empresariales, podría ser útil realizar seguimientos periódicos para asegurarse de que el software siga siendo adecuado para sus necesidades, especialmente si hay cambios en su infraestructura o en las amenazas que enfrentan.