- **Desarrollo de software**
    - Creación y mejora continua del software: La actividad principal será el desarrollo del software de ciberseguridad. Esto incluirá el diseño, programación y pruebas del producto, así como la implementación de nuevas características para adaptarse a las amenazas cibernéticas emergentes.
    - Desarrollo de algoritmos de IA: Específicamente, desarrollar algoritmos de inteligencia artificial que detecten y neutralicen amenazas impulsadas por IA, como hacking automatizado, phishing inteligente y malware autoaprendible, será esencial para el éxito del producto.
    - Pruebas de calidad y seguridad: Antes de cada lanzamiento, se deben realizar pruebas exhaustivas para garantizar que el software funcione correctamente, sea seguro y esté libre de vulnerabilidades.
- **Actualizaciones y mantenimiento**
    - Monitoreo constante de amenazas: Estar al tanto de las nuevas amenazas cibernéticas que surjan y actualizaciones tecnológicas es crucial. Esto permitirá ajustar el software y mantener la seguridad de los usuarios.
    - Actualización de bases de datos de amenazas: Mantener una base de datos actualizada con información sobre nuevas amenazas y vulnerabilidades es fundamental para que tu software siga siendo efectivo.
    - Mantenimiento de versiones: Continuar lanzando versiones actualizadas del software para corregir errores, mejorar funcionalidades y adaptar el producto a nuevas necesidades del mercado.
- **Marketing y ventas**
    - Estrategias de marketing digital: El marketing será clave para llegar a tu audiencia. Esto incluye SEO, publicidad en Google (SEM), marketing en redes sociales y la creación de contenido relacionado con ciberseguridad para educar a tus clientes y aumentar la visibilidad del producto.
    - Gestión de canales de venta: Administrar y optimizar tus canales de distribución (como la página web, plataformas de software y correo electrónico) para garantizar que las ventas sean eficientes y las conversiones sean altas.
- **Soporte al cliente y servicio postventa**
    - Atención a clientes: Aunque el software es autónomo, ofrecer soporte a través de canales como correo electrónico o chat será importante para resolver problemas técnicos y mantener la satisfacción del cliente.
    - Capacitación y formación: Proporcionar capacitación en línea sobre cómo utilizar el software, qué medidas tomar en caso de un ataque, y cómo configurar adecuadamente las protecciones, especialmente a nivel empresarial.
- **Gestión de infraestructura tecnológica**
    - Monitoreo y mantenimiento de servidores: Asegurar que los servidores estén operativos y actualizados para garantizar la correcta distribución del software y el almacenamiento de datos.
    - Escalabilidad del sistema: A medida que el número de clientes crezca, será necesario asegurar que la infraestructura técnica pueda escalar adecuadamente para manejar la carga adicional sin afectar el rendimiento.
- **Desarrollo de relaciones con proveedores y plataformas**

- Acuerdos con proveedores de tecnología: Mantener relaciones con proveedores de servicios en la nube, plataformas de distribución de software y otros recursos tecnológicos para asegurar que el producto sea de alta calidad y esté accesible en todo momento.