**Actividad 1: Sistema de Detección de Ciberataques**

**1. Ejemplos de Acciones Posibles del Atacante**

Un atacante podría intentar realizar diversas acciones maliciosas sobre la plataforma web, como:

- **Inyección SQL**: Intentar manipular consultas a la base de datos para acceder a información sensible.
- **Ataques de fuerza bruta**: Probar múltiples combinaciones de contraseñas para acceder a cuentas de usuarios.
- **Cross-Site Scripting (XSS)**: Inyectar scripts maliciosos en la plataforma para ejecutar acciones en el navegador de otros usuarios.
- **Denegación de Servicio (DoS/DDoS)**: Enviar un gran volumen de tráfico para saturar el servidor y hacerlo inaccesible.
- **Robo de sesiones (Session Hijacking)**: Interceptar o robar cookies de sesión para suplantar la identidad de un usuario.
- **Escaneo de vulnerabilidades**: Usar herramientas automáticas para identificar posibles debilidades en la plataforma.

**2. Funciones del Sistema de Detección y Técnicas de Defensa**

El sistema de detección de ciberataques debe monitorear y analizar la actividad en la plataforma para identificar intentos de ataque y responder de manera efectiva. Algunas funciones incluyen:

- **Monitoreo de tráfico en tiempo real**: Analizar el flujo de datos y detectar patrones sospechosos.
- **Registro y análisis de logs**: Identificar comportamientos anómalos basándose en registros de actividad.
- **Implementación de firewalls y WAF (Web Application Firewall)**: Filtrar y bloquear tráfico malicioso.
- **Uso de inteligencia artificial y machine learning**: Detectar patrones de ataques previamente desconocidos.
- **Autenticación multifactor (MFA)**: Reducir la efectividad de ataques de fuerza bruta.
- **Bloqueo de direcciones IP sospechosas**: Restringir el acceso a posibles atacantes.
- **Sandboxing**: Ejecutar archivos o scripts en entornos aislados antes de permitir su ejecución en el sistema real.

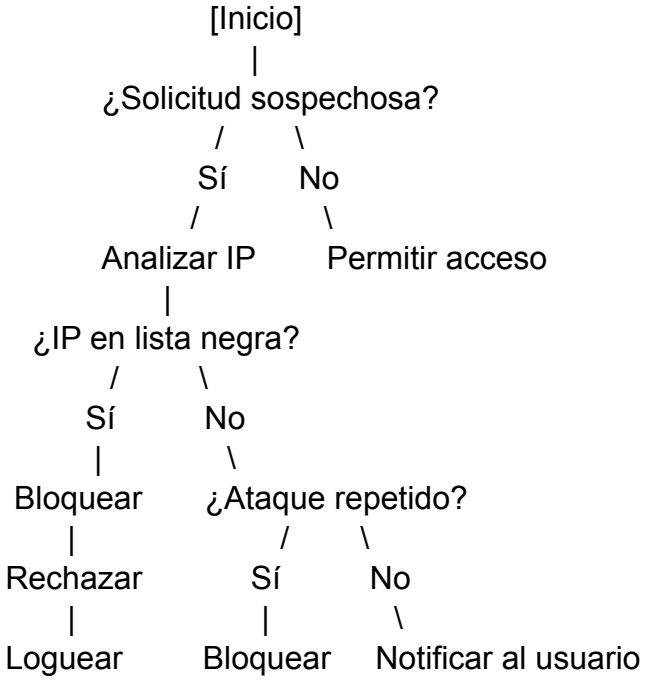
**3. Aplicación de la Poda Alfa-Beta**

La poda alfa-beta es una optimización del algoritmo minimax que se usa en la toma de decisiones, reduciendo la cantidad de nodos evaluados en un árbol de búsqueda. En el contexto del sistema de detección de ciberataques, esta técnica podría aplicarse en escenarios como:

- **Análisis de tráfico sospechoso**: Evaluar múltiples factores (origen, comportamiento, tipo de solicitud) y descartar ramas que no sean relevantes.
- **Priorización de amenazas**: Determinar si una acción es potencialmente dañina y dejar de analizar rutas que no presenten riesgos.
- **Filtrado de eventos en registros de seguridad**: Si una secuencia de eventos indica claramente un ataque, se pueden ignorar otras rutas menos críticas.

La poda alfa-beta ayuda a reducir la cantidad de decisiones analizadas, optimizando la detección y respuesta a ciberataques.

**4. Árbol de Decisión Simplificado**
Aquí se muestra un árbol de decisión básico para responder a intentos de ataques:




Este árbol de decisión ayuda a tomar medidas según el tipo de amenaza detectada, optimizando la seguridad sin afectar la experiencia de usuario legítimo.