**Desarrollo de un Protocolo de Seguridad en el Desarrollo**

Seguridad en el código:

Para garantizar el desarrollo seguro de la aplicación, se deberá de seguir un protocolo de seguridad estricto. Para desarrollar un código seguro, se evitará el uso de código obsoleto de terceros o funciones inseguras que tengan vulnerabilidades de seguridad. Además, se implementarán validaciones de entrada y sanitación de datos.

Se puede implementar un sistema de privilegios con distintos permisos autorizados mediante passwords o incluso autenticación a dos pasos para restringir el acceso a recursos o ficheros sensibles. La gestión de secretos como contraseñas o configuraciones se hará mediante GitHub Secrets, así evitando exponer esta información en el código fuente.

Seguridad en el Pipeline:

Las vulnerabilidades de seguridad en el código se deben de detectar antes de su despliegue en el entorno de pruebas. Hay varias herramientas disponibles para evaluar estas vulnerabilidades durante la compilación del código. Además, se pueden hacer pruebas de penetración periódicas en entornos de prueba para identificar brechas de seguridad antes de la puesta en producción.

Seguridad en el equipo de desarrollo:

Se deben hacer capacitaciones frecuentes con el equipo sobre amenazas y practicas correctas de seguridad. Se debe fomentar este protocolo de seguridad en cada paso del desarrollo, y revisar el mismo para adaptarse a las necesidades cambiantes del proyecto. También seria adecuado establecer planes de respuesta a diferentes tipos de brechas de seguridad para evitar el caos frente a este tipo de situaciones, y practicar simulacros de eventos de este tipo.

Con estas medidas, la aplicación se podrá desarrollar de una manera segura y así evitar contratiempos o filtraciones antes de el lanzamiento del producto.