Objetivo de la Prueba:

El objetivo principal de estas pruebas es evaluar el nivel de seguridad de la aplicación en dos aspectos críticos: el nivel de seguridad del sistema y el nivel de seguridad de la aplicación.

1. **Nivel de seguridad de la aplicación:**
    - Verificar que un actor solo pueda acceder a las funciones y datos autorizados para su usuario.
    - Asegurar que los usuarios estén restringidos a funciones específicas según la seguridad establecida.
    - Limitar el acceso a datos solo a aquellos que el usuario está autorizado a acceder.
2. **Nivel de Seguridad del Sistema:**
    - Verificar que solo los actores con acceso al sistema y a la aplicación están habilitados para acceder a ellas.
    - Garantizar que los usuarios autorizados puedan ejecutar funciones del sistema a través de los mecanismos apropiados.

que la seguridad de la aplicación se centra en proteger una aplicación de software específica y sus datos, la seguridad del sistema amplía su enfoque para abarcar la protección de toda la infraestructura del sistema, incluyendo hardware, software, redes y control de acceso físico. Ambos aspectos son esenciales para garantizar un entorno de TI seguro y confiable.

1. **Controles de Acceso Físico:**
    - **Explicación:** Evaluar la efectividad de las medidas de seguridad física para prevenir accesos no autorizados a los recursos del sistema. Esto incluye la restricción de acceso a servidores, salas de servidores y otros lugares físicos críticos.
    - **Ejemplo de Prueba:** Intentar acceder a áreas restringidas sin autorización física y evaluar la respuesta del sistema de seguridad.
2. **Acceso a Estructuras de Datos Específicas a través de Programas de Aplicación:**

- **Explicación:** Verificar que los usuarios solo puedan acceder y manipular datos para los cuales tienen autorización específica a través de las funciones de la aplicación.
- **Ejemplo de Prueba:** Intentar acceder a datos no autorizados mediante la manipulación de parámetros de la aplicación y verificar la resistencia a estos intentos.

3. **Seguridad en Sitios Remotos:**
    - **Explicación:** Evaluar la seguridad de las conexiones remotas al sistema, asegurándose de que estén protegidas contra amenazas como ataques de intermediarios y acceso no autorizado.
    - **Ejemplo de Prueba:** Simular un acceso remoto no autorizado y evaluar si el sistema detecta y responde adecuadamente.
4. **Existencia de Datos Confidenciales en Reportes y Pantallas:**
    - **Explicación:** Verificar que los informes y pantallas no muestren información confidencial a usuarios no autorizados.
    - **Ejemplo de Prueba:** Revisar informes y pantallas con diferentes niveles de acceso para confirmar que solo se muestra la información correspondiente al nivel autorizado.
5. **Controles Manuales, incluyendo Autorización y Aprobación, Formularios, Documentación Numerada, Transmisión de Datos, Balances y Conversión de Datos:**
    - **Explicación:** Evaluar la eficacia de los controles manuales implementados para garantizar la integridad y seguridad de los datos y procesos.
    - **Ejemplo de Prueba:** Realizar un seguimiento de la autorización y aprobación de transacciones, revisar formularios y documentos numerados, y verificar la transmisión segura de datos.
6. **Controles Automáticos, incluyendo Edición de Datos, Chequeo de Máquinas, Errores del Operador, Acceso a Datos Elementales y Archivos, Acceso a Funciones, Auditoría, entre Otros:**
    - **Explicación:** Evaluar la eficacia de los controles automáticos implementados para garantizar la integridad y seguridad de los datos y procesos.
    - **Ejemplo de Prueba:** Simular condiciones como edición de datos, errores del operador y accesos no autorizados, y verificar la respuesta del sistema.

Criterio de Completitud:

Este criterio establece las condiciones que deben cumplirse para considerar que las pruebas de seguridad y control de acceso han sido completadas de manera satisfactoria. Veamos en detalle cada componente del criterio:

1. **Para cada tipo de usuario conocido:**
    - **Significado:** Se refiere a todos los roles o perfiles de usuario identificados y definidos previamente en el sistema.
    - **Objetivo:** Asegurar que se han considerado todos los posibles roles de usuario que interactuarán con la aplicación.
2. **Las funciones y datos son apropiados:**
    - **Significado:** Cada tipo de usuario tiene acceso a las funciones y datos específicos que son apropiados para su rol o responsabilidades.
    - **Objetivo:** Garantizar que no haya funcionalidades o datos inapropiados asignados a ningún tipo de usuario, lo que podría comprometer la seguridad.
3. **Todas las transacciones funcionan como se esperaba:**

- **Cliente:** Debería poder realizar transacciones bancarias normales, como consultar el saldo y realizar transferencias, pero no debería tener acceso a funciones administrativas.
- **Cajero:** Debería tener acceso a funciones de cajero, como realizar depósitos y retiros, pero no debería tener permisos para cambiar la configuración del sistema.
- **Administrador:** Debería tener acceso completo a todas las funciones, incluyendo configuración y gestión de usuarios.