**Niveles De Protección Para La Prevención De Brechas De Seguridad**

* **Autenticación y autorización**: La aplicación debe contar con un sistema de autenticación seguro para garantizar que solo los usuarios autorizados puedan acceder a las funciones y datos adecuados. Además, la autorización debe ser adecuada para que los usuarios solo puedan acceder a las funciones y datos que tienen permiso para utilizar.
* **Seguridad de datos:** La aplicación debe contar con medidas de seguridad adecuadas para proteger los datos de los usuarios. Esto incluye:
  + Cifrado de extremo a extremo.
  + La gestión de contraseñas seguras.
  + Limitación del acceso a los datos solo a los usuarios autorizados.
* **Seguridad de red:** La aplicación debe contar con medidas de seguridad adecuadas para proteger las comunicaciones entre el servidor y los clientes. Esto incluye:
  + Implementación de protocolos seguros de transferencia de datos.
  + La protección contra ataques de denegación de servicio.
* **Monitoreo y registro de eventos:** La aplicación debe contar con una herramienta de monitoreo y registro de eventos para detectar cualquier actividad sospechosa. Esto puede incluir:
  + El seguimiento de inicios de sesión inusuales.
  + Intentos de acceso no autorizados.
  + Otras actividades sospechosas.
* **Pruebas de seguridad:** La aplicación debe ser sometida a pruebas de seguridad regulares para detectar cualquier vulnerabilidad. Esto incluye:
  + Pruebas de penetración.
  + Pruebas de vulnerabilidad.
  + Pruebas de seguridad de la aplicación en general.
* **Actualizaciones de seguridad:** La aplicación debe ser actualizada regularmente para corregir cualquier vulnerabilidad conocida y para mantener las medidas de seguridad adecuadas. Esto incluye:
  + La implementación de parches de seguridad.
  + La actualización de software y hardware relacionados.