**Seguridad del API de Autenticación**

La seguridad del API que recibirá las peticiones del agente estará alineada con el mecanismo de autenticación ya definido en el agente, manteniendo un enfoque consistente en la generación y validación del token de seguridad. A continuación, se detallan los aspectos clave:

1. **Generación del Token**:
   * El token de autenticación será generado de acuerdo con el proceso que ya está establecido en el agente, utilizando los parámetros proporcionados: NIT, Usuario, Contraseña, Sistema e IP. Estos valores se convertirán en una solicitud XML que será procesada por el API para devolver un token válido.
2. **Validación de Credenciales**:
   * El API validará las credenciales entregadas (NIT, Usuario, Contraseña, Sistema e IP) utilizando el mismo mecanismo utilizado por el agente. Estas credenciales serán verificadas en conjunto con el código técnico fijo (cvetec), y en caso de ser válidas, se generará y devolverá un token.
3. **Sin validaciones adicionales de seguridad**:
   * No se realizarán validaciones adicionales de seguridad fuera de las requeridas y definidas por el proceso del agente. El enfoque de seguridad está limitado a la generación y validación del token según los parámetros mencionados anteriormente.
4. **No se incluirán mecanismos de autenticación o seguridad adicionales** como autenticación basada en certificados, OAuth, validación de IP en listas blancas, ni ningún otro esquema adicional, salvo lo que ya esté definido en el flujo estándar del agente.