

Target CI v1.5

GUÍA DE CIBERSEGURIDAD

Español

Actualización: septiembre de 2025



A Sonova Brand

Contenido

1. INTRODUCCIÓN	4
1.1 ABREVIATURAS Y DEFINICIONES:	4
2. OTROS RECURSOS.....	4
2.1 ATENCIÓN AL CLIENTE	4
2.2 PRO PORTAL DE AB	4
2.3 GUÍA DE INSTALACIÓN AVANZADA.....	5
2.4 MDS2	5
2.5 INSTRUCCIONES DE USO (IFU)	5
2.6 HIMSA.....	5
3. RED Y DIAGRAMAS CONTEXTUALES	5
3.1 MODELO DE IMPLEMENTACIÓN 1: INDEPENDIENTE.....	6
3.2 MODELO DE IMPLEMENTACIÓN 2: NOAH DISTRIBUTED	6
3.3 ARTEFACTOS DE IMPLEMENTACIÓN	7
3.4 INTERCONEXIONES DEL SISTEMA.....	8
4. REQUISITOS DEL SISTEMA.....	10
5. INSTALACIÓN	11
5.1 REQUISITOS	11
5.2 TIPOS DE INSTALADORES.....	11
6. CONTROLES DE SEGURIDAD.....	11
6.1 AUTENTICACIÓN: IMPLEMENTACIÓN INDEPENDIENTE	11
6.2 AUTENTICACIÓN: IMPLEMENTACIÓN DE NOAH.....	12
6.3 AUTORIZACIÓN	12
6.4 AUDITORÍA: IMPLEMENTACIÓN INDEPENDIENTE.....	12
6.5 AUDITORÍA: IMPLEMENTACIÓN DE NOAH.....	12
6.6 ACCESO REMOTO	12
7. PROTECCIÓN DE LA INFORMACIÓN.....	13
7.1 POLÍTICA DE PRIVACIDAD DE ADVANCED BIONICS.....	13
7.2 ESTÁNDARES FEDERALES DE PROCESAMIENTO DE LA INFORMACIÓN (FIPS).....	13
7.3 SEGURIDAD EN TRÁNSITO.....	13
7.4 SEGURIDAD EN REPOSO	14
8. INTEGRIDAD DEL SOFTWARE.....	16
8.1 VERIFICACIÓN DE LOS MEDIOS DE INSTALACIÓN DESCARGADOS.....	16
8.2 VERIFICACIÓN MANUAL DEL SOFTWARE DE PROGRAMACIÓN ANTES DE LA INSTALACIÓN	16

8.3 VERIFICACIÓN AUTOMÁTICA DE LA INTEGRIDAD DEL SOFTWARE DE PROGRAMACIÓN INSTALADO	17
8.4 VERIFICACIÓN MANUAL DE LA INTEGRIDAD DEL SOFTWARE DE PROGRAMACIÓN INSTALADO	17
9. PARCHES Y ACTUALIZACIONES DE SOFTWARE.....	19
10.GESTIÓN DE DATOS	19
10.1 BASES DE DATOS	19
10.2 MIGRACIÓN DE DATOS	19
10.3 CONFIGURACIONES DE DISPOSITIVOS AUDITIVOS.....	19
10.4 ELIMINACIÓN DE DATOS	19
11.ENTORNO DE SEGURIDAD: RESPONSABILIDAD COMPARTIDA.....	19
12.PROCESO DE FABRICACIÓN Y DESARROLLO DE SOFTWARE	21
13.COMPONENTES DE SOFTWARE Y LISTA DE MATERIALES	21
14.REFERENCIAS.....	29

1. INTRODUCCIÓN

Este documento proporciona información técnica de seguridad y privacidad acerca del sistema de software Target CI v1.5 de Advanced Bionics, en lo sucesivo, «software de programación». El software de programación está diseñado para que lo utilice el audiólogo (HCP, por sus siglas en inglés) calificado para configurar (es decir, programar) dispositivos auditivos para pacientes que han recibido implantes cocleares de Advanced Bionics.

Este documento se centra específicamente en las consideraciones de ciberseguridad y privacidad que son relevantes para el uso del software de programación. Incluye una evaluación de los controles de seguridad y privacidad que actualmente están integrados en el software, así como aquellos que se prevé aplicar y configurar dentro del entorno de TI en el que se utilizará el producto para el propósito previsto.

Este documento no proporciona información técnica de seguridad y privacidad sobre:

- Versiones anteriores del software de programación de AB
- Software de AB distinto de Target CI v1.5
- Sitios web de AB
- Aplicaciones móviles de AB
- Dispositivos auditivos de AB

1.1 ABREVIATURAS Y DEFINICIONES:

Acrónimo	Término
FSW	Software de programación
HCP	Audiólogo
SaMD	Software como dispositivo médico
AB	Advanced Bionics
IFU	Instrucciones de uso

2. OTROS RECURSOS

2.1 ATENCIÓN AL CLIENTE

Si reside en Estados Unidos o Canadá, Advanced Bionics pone a su disposición un teléfono gratuito de asistencia técnica (877-271-6727) al que puede hablar para recibir asistencia profesional de lunes a viernes de las 5:00 a las 17:00 h, hora del Pacífico.

Si no reside en EE. UU. o Canadá, el servicio de asistencia técnica se proporcionará a nivel regional. Si tiene preguntas acerca del software de programación, del hardware asociado o cualquier problema de programación, póngase en contacto con su representante local de AB.

2.2 PRO PORTAL DE AB

El software de programación y la documentación relacionada se pueden descargar desde <https://www.abproportal.com> o el Web Client de Sonova. Es necesario iniciar sesión con una cuenta. Es posible que este recurso no esté disponible en todos los mercados; póngase en contacto con su representante de AB para obtener más información.

2.3 GUÍA DE INSTALACIÓN AVANZADA

La guía de instalación avanzada de Target CI v1.5 está disponible previa solicitud. La guía proporciona información técnica sobre el instalador del software de programación, incluidas las opciones de línea de comandos para instalaciones silenciosas y automatizadas.

2.4 MDS2

La Declaración de Divulgación del Fabricante sobre Seguridad de Dispositivos Médicos (MDS2, por sus siglas en inglés) es un formulario estándar de la industria que contiene respuestas de seguridad y privacidad sobre el software de programación de AB. El formulario está disponible previa solicitud.

2.5 INSTRUCCIONES DE USO (IFU)

Las instrucciones de uso se enviarán con el contenido multimedia de instalación del software. Para algunos mercados, las instrucciones de uso en formato electrónico están disponibles para su descarga en www.advancedbionics.com/ifu

Las siguientes secciones de las instrucciones de uso pueden ser relevantes para los profesionales de TI:

- Descripción del producto
- Características de rendimiento y requisitos mínimos del sistema
- Guía de seguridad informática
- Instrucciones de instalación
- Asistencia técnica

2.6 HIMSA

HIMSA es un proveedor de software externo que produce Noah System 4, un sistema de software diseñado para el sector del cuidado auditivo que proporciona a los audiólogos un sistema independiente del proveedor para llevar a cabo tareas relacionadas con el paciente.

El software de programación puede configurarse opcionalmente para utilizar Noah System 4 para el almacenamiento de datos en lugar de una base de datos local.

La página web de seguridad de HIMSA proporciona respuestas a preguntas comunes sobre seguridad informática acerca del Noah System 4.

<https://www.himsa.com/support/noah-enterprise-support/security-questionnaire-support/>

<https://www.himsa.com/support/noah-enterprise-support/security-considerations/>

Consulte la sección de Seguridad del Centro de aprendizaje de HIMSA para obtener información de seguridad adicional:

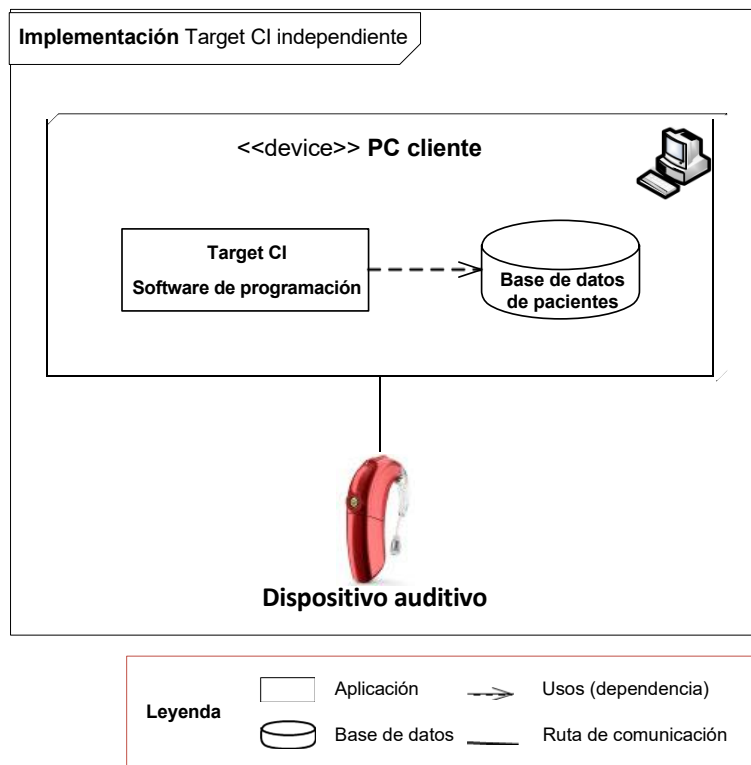
<https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/>

3. RED Y DIAGRAMAS CONTEXTUALES

Hay dos modelos de implementación compatibles con el software de programación, que es una aplicación cliente (SaMD) instalada en un PC con Microsoft Windows disponible en el mercado. El software no incluye ningún hardware ni sistema operativo.

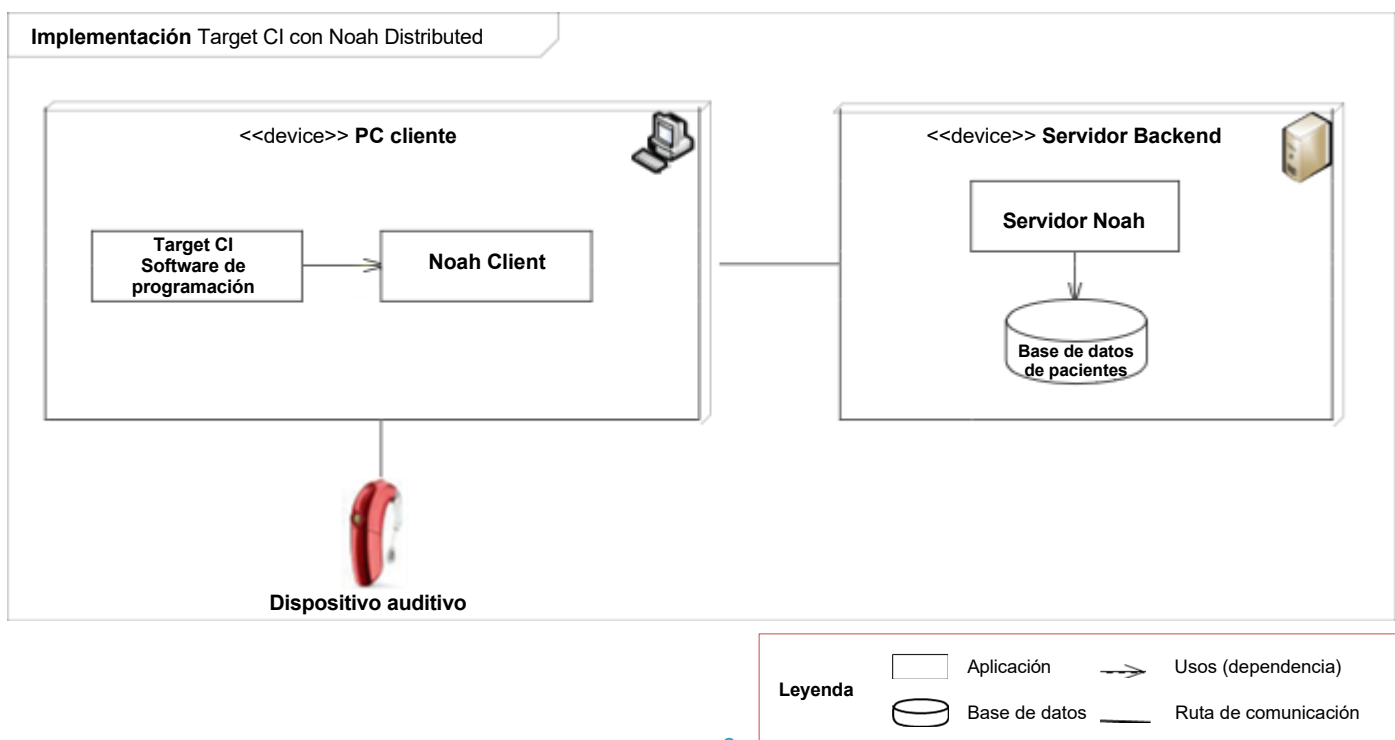
3.1 MODELO DE IMPLEMENTACIÓN 1: INDEPENDIENTE

En el modelo de implementación independiente, el software de programación se implementa en un PC cliente. La base de datos de pacientes se almacena en el mismo PC y se instala junto con el software de programación.



3.2 MODELO DE IMPLEMENTACIÓN 2: NOAH DISTRIBUTED

En el modelo de implementación de Noah Distributed, el software de programación se implementa en uno o más PC clientes. Noah, un sistema de gestión de pacientes de terceros, se implementa en un servidor interno accesible a los PC clientes. La base de datos de pacientes se almacena en el servidor Noah y uno o más PC clientes acceden a ella a través de la red.



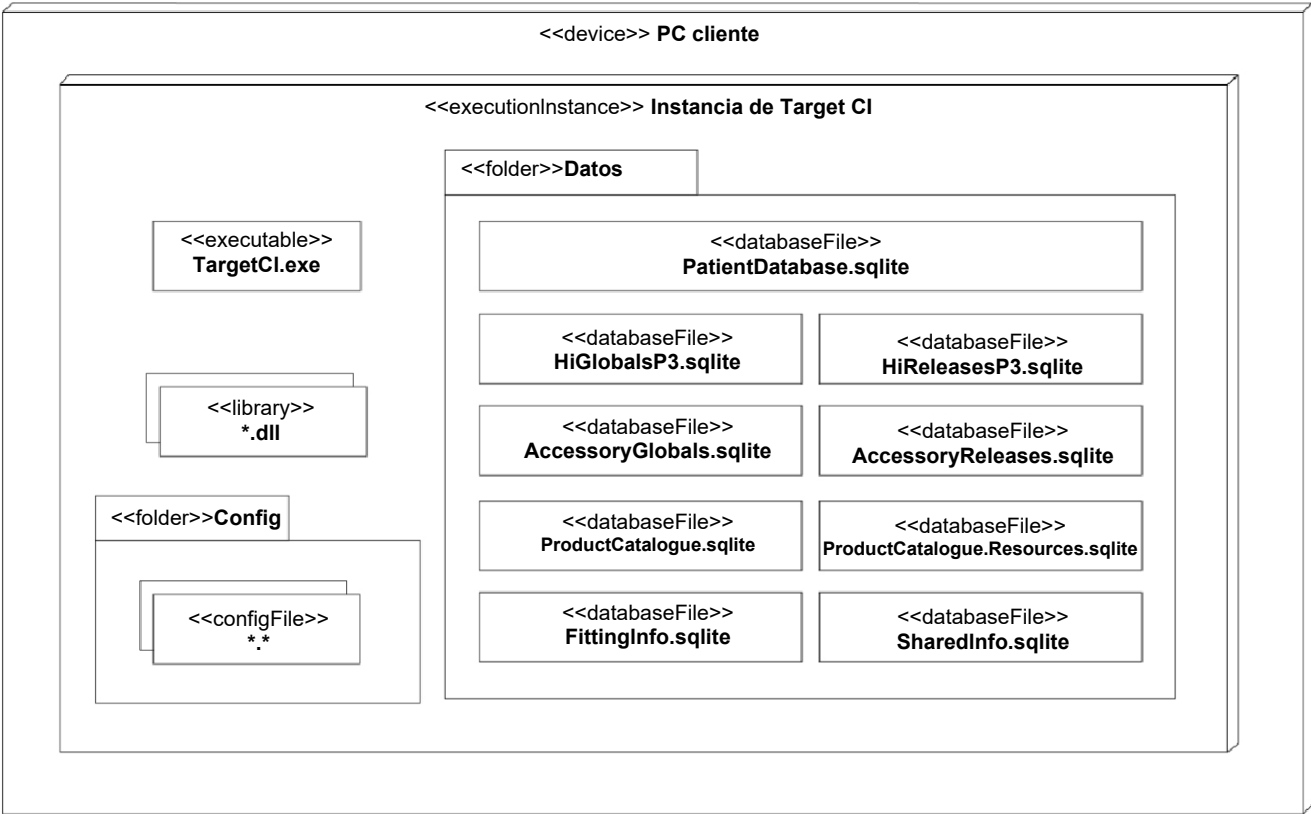
3.3 ARTEFACTOS DE IMPLEMENTACIÓN

El software de programación se instala con un archivo ejecutable y un conjunto de archivos asociados que incluyen DLL de componentes, archivos de configuración y archivos de base de datos SQLite. Los archivos de configuración se instalan en la carpeta «%ProgramData%\Advanced Bionics\Target CI\Target CI\Config» y los archivos de base de datos se instalan en la carpeta “%ProgramData%\Advanced Bionics\Target CI\Target CI\Data». La carpeta Data contiene un único archivo de base de datos transaccional y varios archivos de base de datos de información.

La base de datos transaccional, PatientDatabase.sqlite, almacena los datos demográficos y de ajuste del paciente y se instalará solo cuando el software de programación se implemente en modo independiente.

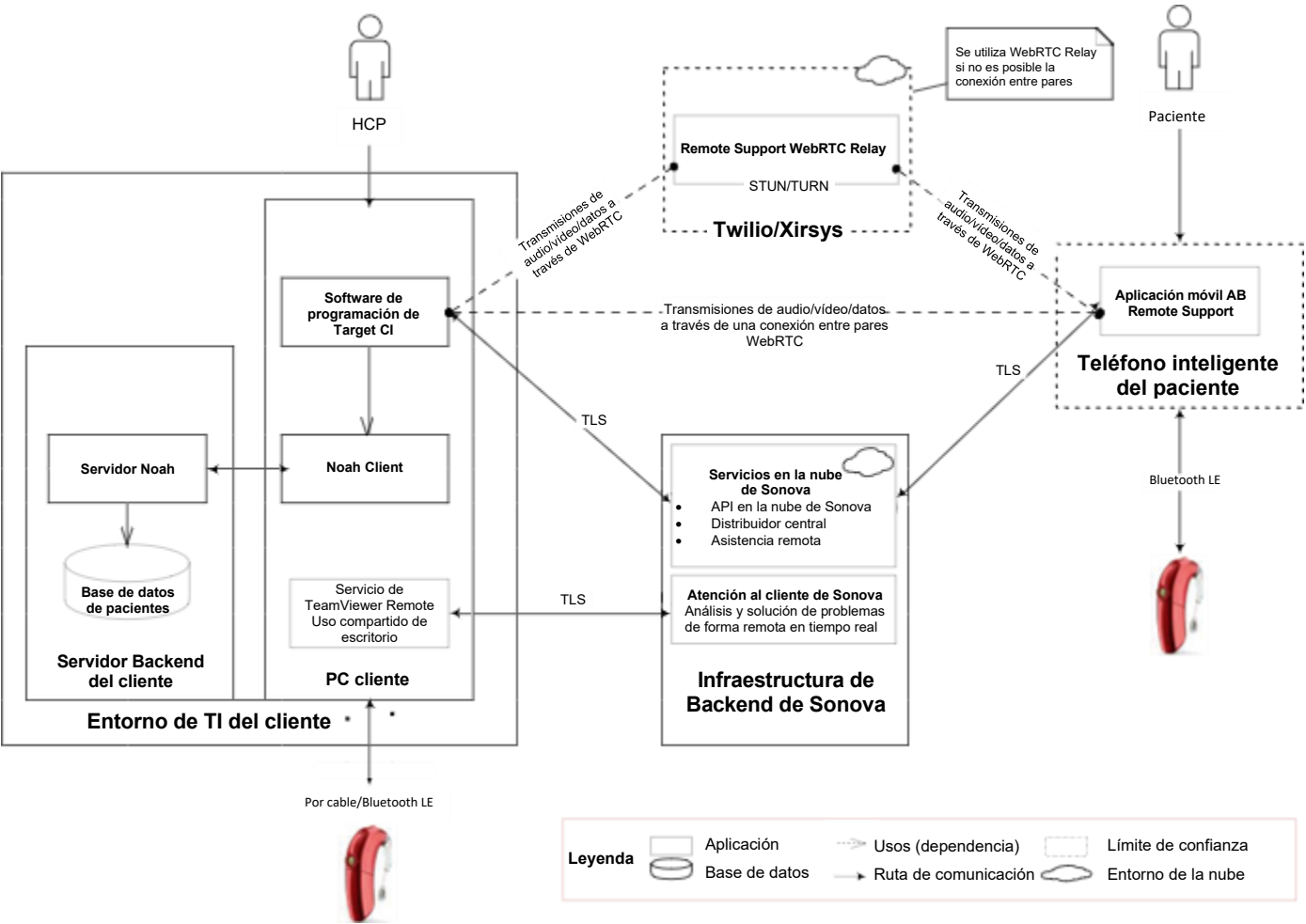
Cuando el software de programación se implementa como un módulo Noah, el sistema Noah proporciona los servicios de persistencia de datos de pacientes necesarios para el software de programación. Los archivos sqlite restantes son parte integral del software de programación y son necesarios para todos los modelos de implementación.

implementación Artefactos de Target CI



3.4 INTERCONEXIONES DEL SISTEMA

El diagrama y la tabla siguientes ilustran las interconexiones del sistema principal. Por lo regular, solo se utiliza una parte de las interconexiones disponibles.



Fuente/Destino	Servicio	Protocolo	Puerto	Descripción
Dispositivos auditivos	Comunicación con dispositivo auditivo	Conexión por cable/ Bluetooth® Low Energy	N/A	Se utiliza para comunicarse con dispositivos auditivos con fines de control, configuración y lectura de estado y datos
Noah	Módulo API de Noah 4	.NET Remoting	N/A	Interfaz principal del módulo utilizado para acceder al software Noah (solo en el modelo de implementación de Noah Distributed)
Servicios en la nube de Sonova	API en la nube de Sonova, distribuidor principal, asistencia remota	SOAP, REST	443	Los servicios de Sonova alojados en un centro de datos de Microsoft Azure se utilizan para: Obtener datos de configuración del cliente del software de programación desde el

Fuente/Destino	Servicio	Protocolo	Puerto	Descripción
				almacenamiento Backend de Sonova • Transferir registros y datos de análisis • Establecer sesiones de adaptación remotas en tiempo real
Twilio/Xirsys, aplicación móvil AB Remote Support	Asistencia remota	WebRTC	Lista de puertos disponibles previa solicitud	Los servicios de comunicación en la nube de Twilio están alojados en plataformas de nube de terceros, específicamente en Amazon Web Services (AWS) y Google Cloud Platform (GCP). Estos servicios son utilizados exclusivamente por la función de asistencia remota del software de programación, que permite la señalización WebRTC y la realización de sesiones de adaptación remotas en tiempo real.
Atención al cliente de AB	Uso compartido de escritorio	Protocolo patentado de TeamViewer	5938, 443, 80 Consulte los puertos de TeamViewer	Se utiliza para realizar análisis remotos en tiempo real y resolver problemas que afectan a las instalaciones del software de programación. Consulte la sección 6.6 SERVICIO REMOTO para obtener más información.

4. REQUISITOS DEL SISTEMA

Sistema operativo	Windows 10, Pro/Enterprise de 64 bits
.NET Framework	Versión 4.8
CPU	Intel® Core™ i5 o equivalente con rendimiento igual o mejor
RAM	4 GB o más
Espacio en el disco duro	3 GB o más
Requisitos mínimos de visualización	• Resolución de 1280 x 1024 (escala máxima del 125 %) • Color de 24 bits
Controladores del dispositivo	• Controlador Noahlink inalámbrico (se requiere la última versión disponible de HIMSA si se utiliza una interfaz de programación Noahlink inalámbrico conectada por USB de terceros). • Controlador CPI-3 (necesario si se utiliza una interfaz de programación CPI-3 conectada por USB).
Base de datos	SQLite o Noah System 4 (versión 4.14 o superior)
Conexión a Internet	Se requiere conexión a Internet para asistencia remota y registro de análisis; consulte la sección 4.4 Interconexiones del sistema. Se requiere intranet cuando se utiliza Noah System 4 en red.
Puertos de red	Consulte la sección 3.4 Interconexiones del sistema; consulte la sección 3. Otros recursos: HIMSA para los puertos utilizados por el Noah System 4.

5. INSTALACIÓN

5.1 REQUISITOS

Se requiere una cuenta de administrador para instalar el software de programación. Una vez instalado el software, se puede ejecutar sin permisos de administrador ni avanzados.

Consulte la sección 8, Integridad del software, para obtener información sobre cómo validar la integridad del software antes de la instalación.

Antes de la instalación, se recomienda a los administradores del sistema asegurarse de que:

- La versión del producto de software de programación que se va a instalar es la última disponible.
- El sistema operativo subyacente está actualizado.

5.2 TIPOS DE INSTALADORES

Hay dos instaladores disponibles para instalar el software de programación:

- Instalador estándar
- Instalador IT Professional

El instalador IT Professional es un único archivo MSI y excluye los componentes necesarios, pero por lo demás es equivalente al instalador estándar.

Los componentes necesarios incluyen Microsoft .NET Framework v4.8 y los paquetes redistribuibles de Microsoft Visual C++.

Ambos instaladores admiten escenarios de instalación avanzados, incluida la instalación silenciosa.

El instalador IT Professional solo debe utilizarse si su organización requiere que los componentes necesarios sean instalados y administrados por su organización y no por el instalador de software de programación. En todos los demás casos se debe utilizar el instalador estándar.

El instalador IT Professional se puede obtener a través del representante clínico de AB. El instalador IT Professional no se puede utilizar para reparar, reinstalar o desinstalar las instalaciones realizadas por el instalador estándar. El instalador estándar no se puede utilizar para reparar, reinstalar o desinstalar las instalaciones realizadas por el instalador IT Professional.

6. CONTROLES DE SEGURIDAD

El software de programación es una aplicación cliente que se instala en un PC con Microsoft Windows disponible en el mercado. El software de programación se puede instalar como aplicación independiente o como un módulo Noah.

6.1 AUTENTICACIÓN: IMPLEMENTACIÓN INDEPENDIENTE

Cuando el software de programación se instala como una aplicación independiente, depende de los mecanismos de control de acceso proporcionados por el sistema operativo anfitrión. El personal de TI del cliente puede configurar el sistema operativo anfitrión para administrar la autenticación. El software de programación no tiene ninguna función integrada de este tipo. Advanced Bionics recomienda que cada usuario inicie sesión en el sistema operativo anfitrión con una cuenta única por usuario.

6.2 AUTENTICACIÓN: IMPLEMENTACIÓN DE NOAH

Cuando el software de programación se instala como un módulo Noah, el control de acceso lo proporciona Noah System 4. Consulte www.HIMSA.com para conocer los controles de auditoría utilizados por Noah System 4.

6.3 AUTORIZACIÓN

El software de programación no restringe el acceso a sus funciones con base en los roles de los usuarios individuales. El software admite una única función principal de adaptación de los dispositivos auditivos del paciente, y un único rol, el de profesional de la adaptación. Los controles de acceso basados en roles no son aplicables.

6.4 AUDITORÍA: IMPLEMENTACIÓN INDEPENDIENTE

Cuando el software de programación se instala como una aplicación independiente, depende de los mecanismos de auditoría proporcionados por el sistema operativo anfitrión. El software de programación no tiene ninguna función integrada de este tipo. El personal de TI del cliente puede configurar el sistema operativo anfitrión para registrar lanzamientos o ejecuciones del software de programación y de los inicios de sesión de los usuarios. Advanced Bionics recomienda que cada usuario inicie sesión en el sistema operativo anfitrión con una cuenta única por usuario para facilitar la auditoría.

6.5 AUDITORÍA: IMPLEMENTACIÓN DE NOAH

Cuando el software de programación se instala como un módulo Noah, el sistema Noah proporciona registros de auditoría. Consulte <https://www.himsa.com/> para conocer los controles de auditoría utilizados por Noah System 4.

6.6 ACCESO REMOTO

La función de uso compartido de escritorio permite el análisis remoto en tiempo real y la solución de problemas que afectan a las instalaciones de software de programación. Esta función se basa en la herramienta de terceros TeamViewer QuickSupport (implementada por defecto junto con el software de programación) y permite a los profesionales de atención al cliente de AB conectarse de forma remota al ordenador del audiólogo y obtener control total del escritorio, incluido el acceso al sistema operativo y al sistema de archivos subyacentes.

Para establecer una sesión de uso compartido de escritorio, se requiere la interacción del audiólogo. En primer lugar, el audiólogo deberá ejecutar la herramienta TeamViewer QuickSupport (por ejemplo, a través del software de programación de Target CI) y comunicar sus credenciales de identificación de TeamViewer al equipo de soporte de AB a través de un canal de comunicación fuera de banda (por ejemplo, una llamada telefónica).

El nombre del miembro del equipo de soporte de AB y su ID de TeamViewer se muestran por defecto en el monitor del ordenador del audiólogo durante cada sesión activa de uso compartido de escritorio.

Todo el tráfico de red del uso compartido de escritorio está protegido y cumple o supera los estándares de protocolos y algoritmos criptográficos (intercambio de claves públicas/privadas RSA y cifrado de sesión AES de 256 bits).

TeamViewer QuickSupport se puede eliminar manualmente sin que se vean afectadas otras funcionalidades de Target FSW. El programa de instalación de Target FSW admite un parámetro de instalación de línea de comandos para permitir una instalación de línea de comandos de Target FSW sin incluir la herramienta TeamViewer QuickSupport.

7. PROTECCIÓN DE LA INFORMACIÓN

7.1 POLÍTICA DE PRIVACIDAD DE ADVANCED BIONICS

La política de privacidad que describe cómo Advanced Bionics recopila, transfiere, almacena y utiliza datos personales se puede descargar en: AdvancedBionics.com/privacy.

Advanced Bionics no aloja, almacena, realiza copias de seguridad ni tiene acceso a ningún dato almacenado en el software de programación o en las bases de datos de Noah, a menos que los datos se envíen expresamente a Advanced Bionics.

7.2 ESTÁNDARES FEDERALES DE PROCESAMIENTO DE LA INFORMACIÓN (FIPS)

Target CI v1.5 cumple con los estándares de cifrado FIPS 140-2.

7.3 SEGURIDAD EN TRÁNSITO

La seguridad de las comunicaciones está garantizada y habilitada en todas las comunicaciones de red entrantes y salientes del software de programación. A excepción de la función de asistencia remota (que utiliza el protocolo WebRTC) y la comunicación Bluetooth con dispositivos auditivos y accesorios, todas las demás conexiones están protegidas por el protocolo Transport Layer Security (TLS), que proporciona confidencialidad, integridad y autenticidad.

TLS

La configuración de TLS cumple con las mejores prácticas y recomendaciones de seguridad actuales documentadas en BCP 195. Recomendaciones para el uso seguro de TLS y DTLS, incluyendo BCP 195:

- No se admiten versiones SSL y TLS anteriores a la 1.2.
- No se admiten conjuntos de cifrado que utilicen algoritmos criptográficos que ofrezcan menos de 128 bits de seguridad.
- Se admiten extensiones TLS recomendadas de BCP 195.
- No se admiten extensiones inseguras de BCP 195.

DTLS

El cifrado es una característica obligatoria de WebRTC y se aplica a todas las transmisiones multimedia enviadas a través de WebRTC. El protocolo de cifrado utilizado depende del tipo de canal; las transmisiones de datos se cifran utilizando DTLS y las transmisiones de contenido multimedia se cifran utilizando el Protocolo de transporte seguro en tiempo real (SRTP), que se utiliza porque es una opción más liviana que DTLS.

Consulte el siguiente enlace para obtener información más detallada sobre la configuración de seguridad de Remote Support WebRTC:

<https://developer.liveswitch.io/liveswitch-server/server/security.html>

BLE

La comunicación inalámbrica Bluetooth Low Energy con dispositivos auditivos y accesorios está cifrada y su integridad está protegida por defecto (excepto en los casos de uso de identificación y detección). Además de eso, la duración del modo de emparejamiento Bluetooth del dispositivo auditivo es limitada en el tiempo. Consulte la documentación del dispositivo auditivo disponible para obtener una descripción más detallada sobre la seguridad del canal de comunicación Bluetooth.

7.4 SEGURIDAD EN REPOSO

Base de datos de pacientes: modelo de implementación independiente

Si el software de programación se instala como una aplicación independiente, la base de datos de pacientes se almacena de forma local en: C:\ProgramData\Advanced Bionics\Target CI\Target CI\Data

Estos registros no están cifrados en reposo por defecto. La Información Médica Protegida (PHI, por sus siglas en inglés) y la Información de Identificación Personal (PII, por sus siglas en inglés) se almacenan en una base de datos interna del software de programación y no se transmiten a través de la red.

En algunas jurisdicciones, la normativa puede exigir el cifrado de todos los datos de los pacientes para evitar posibles responsabilidades en caso de pérdida o robo de datos. Habilite BitLocker o un cifrado de disco completo equivalente (en lo que respecta al sistema operativo o basado en hardware) para proteger los datos contra accesos o copias no autorizados mientras están en reposo.

BitLocker es una función integrada de Windows que cifra toda la unidad y requiere autenticación para acceder. Consulte siempre la guía oficial de Microsoft y la política de seguridad de TI de su organización antes de habilitar BitLocker.

Cómo habilitar BitLocker

Se requieren privilegios de administrador para gestionar BitLocker.

1. Busque «Gestionar BitLocker»

Abra el menú Inicio, escriba «Gestionar BitLocker» y seleccione esa opción en los resultados de la búsqueda.

2. Seleccione la unidad del sistema

Seleccione la unidad donde está instalado Windows para configurar los ajustes de cifrado.

3. Elija un método de desbloqueo

Seleccione una de las siguientes opciones:

- Solo TPM
- TPM + PIN
- TPM + memoria USB

Siga las recomendaciones de las mejores prácticas de Microsoft y la política de seguridad de TI de su organización al seleccionar el método de desbloqueo.

4. Realice una copia de seguridad de la clave de recuperación

Realice una copia de seguridad de la clave de recuperación con métodos seguros aprobados por la empresa. Las opciones recomendadas incluyen:

- Almacenamiento en Microsoft Entra ID (anteriormente Azure AD) o Active Directory para dispositivos unidos al dominio
- Guardado en una ubicación de red segura y con acceso controlado, con cifrado y registro de auditoría
- Uso de una solución de depósito de claves administrada aprobada por su organización

Evite guardar la clave en unidades locales, USB o imprimirla a menos que la política lo permita explícitamente. Las claves de recuperación deben protegerse con el mismo rigor que otras credenciales confidenciales y cambiarse inmediatamente si se exponen.

5. Inicie el cifrado

Elija:

- Unidad completa: recomendada para la mayoría de los escenarios empresariales. Cifra todos los sectores, incluido el espacio no utilizado, para evitar la remanencia de datos.

Base de datos de pacientes: módulo de implementación de Noah Distributed

Cuando el software de programación se instala como un módulo Noah, la Información de Identificación Personal (PII) se almacena dentro de la base de datos de pacientes alojada por Noah. La base de datos de pacientes alojada por Noah puede residir en otra máquina. La Información de Identificación Personal y otros datos de los pacientes se mantienen mediante el software Noah, y el cifrado de los datos en reposo de los pacientes está garantizado por el sistema Noah. El software de programación puede transmitir o recibir información de identificación personal a través de una conexión de red por cable o inalámbrica cuando una base de datos Noah está configurada para el acceso a la red.

La Información de Identificación Personal almacenada en la base de datos Noah en red será visible para otros usuarios de dispositivos en diferentes PC que tengan permisos para acceder a la misma base de datos en red. La base de datos Noah también puede configurarse para el acceso sin red e instalarse en el mismo PC que el software de programación.

Noah impide que el software de programación acceda a la base de datos de registros de los pacientes. Cuando un usuario abre el registro de un paciente en el software de programación a través de Noah Client, el software de programación solo puede leer y escribir en el registro del paciente que está abierto y no puede acceder a otros registros de pacientes en la base de datos Noah.

Consulte la sección www.HIMSA.com para conocer los estándares de cifrado utilizados por Noah System 4.

Archivos de exportación de la autorización de devolución de mercancía (RMA, por sus siglas en inglés)

El software de programación permite exportar la información del paciente a un archivo. El archivo RMA se puede enviar a Advanced Bionics para resolver problemas de RMA o soporte relacionados.

El archivo RMA está cifrado de forma asimétrica con RSA mediante una clave de 512 bits. El software de programación no tiene ninguna función para descifrar un archivo RMA.

Archivos de exportación anónimos

El software de programación permite exportar la información del paciente a un archivo anónimo. La información de identificación personal del paciente, como la fecha de nacimiento y el nombre, se reemplaza con valores genéricos. El archivo no está cifrado y se puede importar a la misma instancia o a una instancia diferente del software de programación.

Archivos de exportación estándar

El software de programación permite exportar la información del paciente a un archivo de exportación estándar. El archivo utiliza un formato binario patentado y no está cifrado. El archivo se puede importar a la misma instancia del software de programación o a una diferente. Al utilizar esta función, los usuarios del software de programación deben asegurarse de que los archivos de exportación estándar se gestionen de acuerdo con sus políticas de TI locales para administrar Información de Identificación Personal (PII) no cifrada.

Dispositivo auditivo

El software de programación almacena la información del paciente en su dispositivo auditivo. La información de identificación personal, como el nombre y la fecha de nacimiento del paciente, no se almacena en el dispositivo auditivo. El resto de la información que no sea Información de Identificación Personal se almacena mediante cifrado PBKDF2 con una clave de 128 bits.

El software de programación puede transmitir o recibir información del paciente que no sea Información de Identificación Personal a/desde un dispositivo auditivo a través de un dispositivo por cable patentado (es decir, CPI-3), la aplicación móvil AB Remote Support o un dispositivo Noahlink inalámbrico. El dispositivo inalámbrico Noahlink se conecta con el dispositivo auditivo mediante Bluetooth Low Energy (BLE) a través de un canal cifrado AES BLE de 128 bits estándar.

8. INTEGRIDAD DEL SOFTWARE

8.1 VERIFICACIÓN DE LOS MEDIOS DE INSTALACIÓN DESCARGADOS

El medio de instalación del software de programación Target CI se puede descargar en algunas regiones desde el Pro Portal de Advanced Bionics o el Web Client de Sonova. Los medios de instalación descargados se pueden autenticar al utilizar cualquier herramienta de hash SHA-256 confiable.

El hash SHA256 para el archivo zip de instalación estándar es:

A42B8F41A5A4111D1CDF67394FFBBFBCDF2FB6215EC2696DB310B3AED6D4DD83

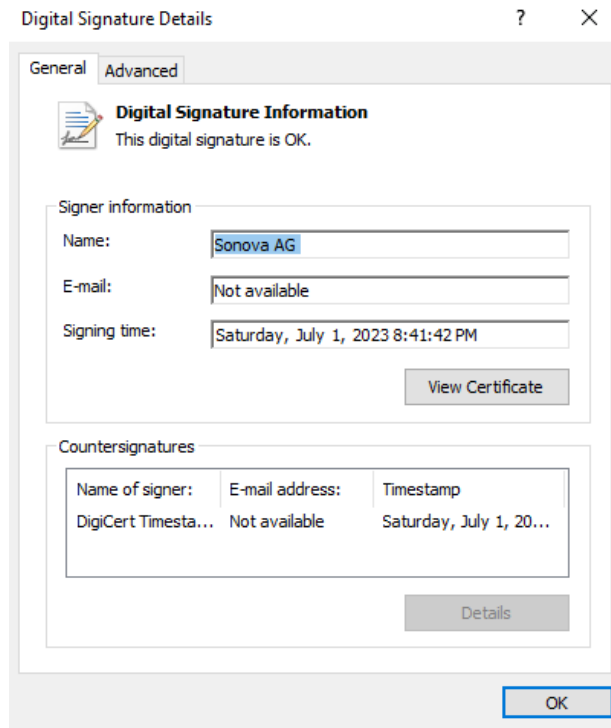
El hash SHA256 para el archivo zip de instalación de IT Professional es:

DDAD362CC3213EFEA702D9F4A61740B34EDF794FE997811B6B2C908CE754B25F

8.2 VERIFICACIÓN MANUAL DEL SOFTWARE DE PROGRAMACIÓN ANTES DE LA INSTALACIÓN

Los usuarios pueden realizar los siguientes pasos para verificar la integridad y autenticidad del software de programación antes de la instalación:

1. Abra el Explorador de Windows y navegue hasta la carpeta raíz del medio de instalación del software de programación. Si su medio de instalación es una unidad USB, insértela en un puerto USB y navegue hasta su raíz. Si su medio de instalación es un archivo zip, descomprímalo en una carpeta y navegue hasta esa carpeta.
2. Haga clic derecho en SonovaVerify.exe y seleccione Propiedades en el menú contextual.
3. Seleccione la pestaña Firmas digitales.
4. Haga doble clic en la firma SHA256 «Sonova AG».
5. Verifique que los elementos de la firma sean válidos. En particular, verifique que el mensaje «The digital signature is OK.» (La firma digital es correcta.) aparezca cerca de la parte superior y que el nombre del firmante y la hora de la firma coincidan con la siguiente imagen:



1. Cierre los cuadros de diálogo emergentes y haga doble clic en SonovaVerify.exe.
2. Verifique que se muestre «NO ERRORS DETECTED.» (NO SE DETECTARON ERRORES.) como se muestra en la siguiente imagen:

```
FILES PROCESSED: 79
IGNORED FILES: 1
.\sonovaverify.dat
NO ERRORS DETECTED.
Press any key to continue . . .
```

La imagen muestra que SonovaVerify ha autenticado y verificado las firmas digitales de todos los archivos en el medio de instalación, incluido el instalador. Esto verifica que el medio de instalación no se haya alterado, dañado o comprometido de alguna otra manera. SonovaVerify mostrará advertencias o mensajes de error si faltan archivos o carpetas, o si se han añadido archivos o carpetas inesperados al medio de instalación.

8.3 VERIFICACIÓN AUTOMÁTICA DE LA INTEGRIDAD DEL SOFTWARE DE PROGRAMACIÓN INSTALADO

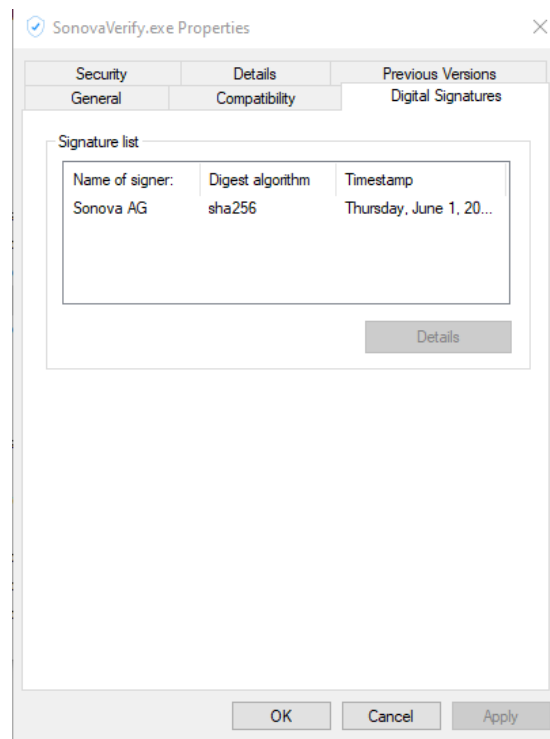
SonovaVerify está integrado con el software de programación y se ejecuta cada vez que se inicia la aplicación para verificar la integridad de los archivos de programa del software de programación. Los archivos de programa se firman de manera digital mediante prácticas estándar de la industria y certificados emitidos por una autoridad de certificación confiable. El software notifica al usuario mediante mensajes de advertencia si algún archivo de programa está en riesgo.

8.4 VERIFICACIÓN MANUAL DE LA INTEGRIDAD DEL SOFTWARE DE PROGRAMACIÓN INSTALADO

Los usuarios pueden realizar los siguientes pasos para verificar la integridad y autenticidad del software de programación instalado en cualquier momento sin necesidad de iniciarlo:

1. Abra el Explorador de Windows y navegue hasta la carpeta ejecutable del software de programación, generalmente ubicada en: C:\Program Files (x86)\Advanced Bionics\Target CI\
2. Haga clic derecho en SonovaVerify.exe y seleccione Propiedades en el menú contextual.

3. Seleccione la pestaña Firmas digitales.
4. Haga doble clic en la firma SHA256 «Sonova AG».
5. Verifique que los elementos de la firma sean válidos, en particular que aparezca el mensaje «The digital signature is OK.» (La firma digital es correcta.) cerca de la parte superior y que el nombre del firmante y la hora de la firma coincidan con la siguiente imagen:



1. Cierre los cuadros de diálogo emergentes y haga doble clic en SonovaVerify.exe.
2. Verifique que se muestre «NO ERRORS DETECTED.» (NO SE DETECTARON ERRORES.) como se muestra en la siguiente imagen:

```

SonovaVerify 0.0.4.0 Copyright 2019-2023 Sonova

Verifying: C:\Program Files (x86)\Advanced Bionics\Target CI\SonovaVerify.DAT
Target: C:\Program Files (x86)\Advanced Bionics\Target CI
Product: Target CI 1.5.11.0

FILES PROCESSED: 779

IGNORED FILES: 3
    .\config\App.xml
    .\data\
    .\sonovaverify.dat

NO ERRORS DETECTED.
Press any key to continue . . .

```

La imagen muestra que SonovaVerify ha autenticado y verificado las firmas digitales de todos los archivos de programa instalados. Esto verifica que el software de programación no se haya alterado, dañado o comprometido de alguna otra manera. SonovaVerify mostrará advertencias o mensajes de error si faltan archivos o carpetas, o si se han añadido archivos o carpetas inesperados a la carpeta de archivos de programa.

9. PARCHES Y ACTUALIZACIONES DE SOFTWARE

No se admiten actualizaciones automáticas.

10. GESTIÓN DE DATOS

10.1 BASES DE DATOS

El software de programación utiliza una base de datos transaccional para almacenar datos del paciente y un conjunto de bases de datos de información que proporcionan las configuraciones de metadatos requeridas por la aplicación.

Consulte la Sección 3. Diagramas de red y contexto: artefactos de implementación para obtener una lista detallada de todas las bases de datos implementadas por el software de programación.

Cuando el software de programación se instala como una aplicación independiente, la base de datos de pacientes funciona de manera interna en el software de programación. La base de datos de pacientes, almacenada en el archivo PatientDatabase.sqlite, reside en la misma máquina que el software de programación y proporciona el almacenamiento de los datos del paciente. Para realizar una copia de seguridad de los datos de la aplicación cuando Target CI se implementa como una aplicación independiente, cree una copia de seguridad de toda la carpeta ubicada en %ProgramData%\Advanced Bionics\Target CI\Target CI\Data. Proteja las copias de seguridad de datos no solo contra la pérdida de datos, sino también contra el robo. Cuando el software de programación se instala como un módulo Noah, los datos del paciente se almacenan en la base de datos proporcionada por el sistema Noah. La base de datos Noah puede configurarse para el acceso a la red. La base de datos Noah también puede configurarse para el acceso sin red e instalarse en el mismo PC que el software de programación. Configure el cifrado de la base de datos Noah para proteger los datos (consulte la documentación de HIMSA).

Para el modo de implementación de Noah Distributed, consulte el siguiente enlace para obtener instrucciones acerca de la copia de seguridad y la restauración de la base de datos de pacientes de Noah:

<https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/backing-up-and-restoring-the-data-in-your-noah-database/>

10.2 MIGRACIÓN DE DATOS

El software de programación permite a los usuarios migrar registros de pacientes desde el software de programación anterior de AB, SoundWave 3.2. Los registros de pacientes deben ser accesibles desde la carpeta de instalación de SoundWave 3.2 en el mismo ordenador en que está instalado Target CI para poder migrarlos.

10.3 CONFIGURACIONES DE DISPOSITIVOS AUDITIVOS

El software de programación permite exportar e importar configuraciones y ajustes del dispositivo.

10.4 ELIMINACIÓN DE DATOS

Las instrucciones para la eliminación de datos se pueden encontrar en las Instrucciones de uso o en el siguiente sitio para implementaciones de Noah: <https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/deleting-patient-records/>

11. ENTORNO DE SEGURIDAD: RESPONSABILIDAD COMPARTIDA

El software de programación ha sido diseñado para un uso previsto en el que la gestión de riesgos de ciberseguridad se considera una responsabilidad compartida entre las partes interesadas en todo el sector del cuidado auditivo, que incluye, entre otros, usuarios de dispositivos auditivos, padres o tutores legales de niños que son usuarios de dispositivos auditivos, audiólogos, administradores de TI, instalaciones y proveedores de cuidado auditivo, proveedores de dispositivos auditivos y equipos de programación.

A continuación se muestra una lista de recomendaciones de las mejores prácticas comunes y controles de seguridad para el entorno de adaptación en el que se utilizará el software de programación:

Nivel de sistema operativo

- Aplicar controles de acceso a nivel de sistema operativo, por ejemplo:
 - Eliminar las cuentas de invitados
 - Activar el inicio de sesión de usuario de Windows
 - Mantener una lista de operadores autorizados para controlar el acceso al sistema
 - Establecer usuarios y roles personalizados
 - Aplicar requisitos de contraseñas seguras y mantener las credenciales en secreto
- Aplicar controles de auditoría a nivel de sistema operativo
- Mantener el sistema operativo actualizado
- Mantener actualizada la versión instalada del software de programación
- Habilitar la protección antivirus y contra malware actualizada
- Habilitar la lista blanca de aplicaciones

Protección de los datos

- Cifre los datos de los pacientes con herramientas o controles de terceros a nivel del sistema operativo, por ejemplo, al utilizar el cifrado de unidad (como el cifrado gratuito Microsoft BitLocker) para proteger todos los datos. Para las implementaciones de Noah, considere utilizar el cifrado de bases de datos de Noah.
- Los medios externos que contienen datos exportados desde el software de programación, incluidos los informes y registros, deben protegerse. Cuando ya no se utilicen, los datos y/o los medios deberán eliminarse de forma segura.
- Utilice medios de almacenamiento USB con funcionalidad de seguridad incorporada, como unidades USB cifradas con teclado integrado.
- Asegúrese de mantener siempre los datos seguros:
 - Al transferir datos a través de canales poco seguros, envíe datos anónimos o cifrelos.
 - Proteja las copias de seguridad de datos no solo contra la pérdida de datos, sino también contra el robo.
 - Elimine del soporte de datos todos los datos que ya no se utilizan o que deberían ser desechados.
- Los usuarios deben utilizar procedimientos y herramientas aprobados para la eliminación segura de datos almacenados en medios extraíbles, de acuerdo con las normas y pautas aplicables para el manejo de información del paciente, la Información de Identificación Personal (PII) o la Información Médica Protegida (PHI).

Infraestructura de TI

Use el software de programación en un entorno de red seguro y protegido contra intrusiones no autorizadas. Existen muchas técnicas efectivas para aislar y proteger los sistemas de información médica, incluida la implementación de protección de firewall, zonas desmilitarizadas (DMZ), redes de área local virtuales (VLAN) y enclaves de red. Mantenga una conexión de red activa para recibir actualizaciones del sistema operativo.

Nivel físico

- La estación de trabajo donde se instala el software de programación debe estar protegida físicamente de manera que no sea accesible para usuarios no deseados.
- Asegúrese de que el personal no autorizado no manipule el sistema.
- Se debe controlar el acceso a las impresoras conectadas a la estación de trabajo.
- El monitor de la estación de trabajo en la que se instala el software de programación debe colocarse de manera que se limite la visibilidad del contenido de la pantalla solo para el usuario.

Nivel organizativo

- Solo personal profesionalmente capacitado y totalmente calificado está autorizado a operar el sistema. Antes de autorizar a cualquier persona a manejar el sistema, se debe verificar que la persona haya leído y comprendido completamente las instrucciones de funcionamiento proporcionadas con el software de programación.
- Si nota alguna actividad sospechosa en sus cuentas de software de programación o cualquier operación inesperada, comuníquese con Advanced Bionics. Consulte la sección 2.1 para obtener más información.

Para obtener más información sobre la responsabilidad compartida y una lista más detallada de recomendaciones de las mejores prácticas y controles de seguridad para el entorno de adaptación en el que se utilizará el software de programación para su aplicación en varios niveles, consulte:

- El informe técnico de EHIMA «Mejores prácticas para la adaptación segura de dispositivos auditivos», [EHIMAWhitePaper](#)

12. PROCESO DE FABRICACIÓN Y DESARROLLO DE SOFTWARE

La ciberseguridad se considera durante todo el proceso de desarrollo de software. El software de programación está desarrollado de acuerdo con las normas IEC 62304 e IEC 82304.

El software de programación se analiza en busca de virus y malware como parte del proceso de fabricación.

Las vulnerabilidades en los componentes de terceros enumerados en la Base de Datos Nacional de Vulnerabilidades (NVD, por sus siglas en inglés) del NIST se evalúan y mitigan durante el proceso de desarrollo y se monitorizan una vez que el software de programación se ha lanzado al mercado.

13. COMPONENTES DE SOFTWARE Y LISTA DE MATERIALES

El software de programación incorpora determinados componentes de software disponibles en el mercado.

La siguiente tabla enumera todos los SOUP (Software de procedencia desconocida) distribuidos con el software de programación.

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
Simulador de pérdida auditiva ciAD	Biblioteca de simuladores de pérdida auditiva para reproductor multimedia	ciAD (Jurg Haubold)	1.0.0.1
CredentialManagement	El paquete de administración de credenciales es un contenedor para la API de administración de credenciales de Windows	iLya Lozovyy	1.0.2
CSharpAnalytics	Se utiliza para Google Analytics.	Attack Pattern	1.6.1
Dapper	ORM	Sam Saffron, Marc Gravell y Nick Craver	2.0.78
Deconstructurama.Attributed	Se utiliza en las bibliotecas Nephele.	Colaboradores de Serilog	3.0
DirectShow 2005	Permite el acceso a la funcionalidad DirectShow de Microsoft desde aplicaciones .NET.	Microsoft	2.0
DSL4	DSL 4 Fitting formula library.	National Centre for Audiology, Canadá	4.2
DSL5	DSL 5 Fitting formula library.	National Centre for Audiology, Canadá	5.0.34
GNOtometrics.Aurical	GNOtometrics.Aurical reempaquetado para Sonova	GNOtometrics	2.0.1.9
IceLink	Se utiliza para la integración de conferencias de audio/vídeo WebRTC.	FM (Frozen Mountain)	3.8.0.22151
IdentityModel	Biblioteca cliente OpenID Connect y OAuth 2.0 utilizada por el componente Kona.CommonServices.Authentication para la autenticación OAuth 2.	Dominick Baier, Brock Allen	5.0.1
IMCInterfaces	Biblioteca de interfaz de comunicación entre módulos Noah	HIMSA II K/S	4.4.0.2266
LibGit2Sharp	Se utiliza en bibliotecas procedentes de Sonova para comunicarse con Git	Colaboradores de LibGit2Sharp	0.26.1
Mapster	Se utiliza para mapear objetos en el código	chaowlert, eric_swann	7.2.0.0
MathNet.Numerics	Se utiliza para ajustar algoritmos (ruta de señal, comparador de objetivos, etc.)	Christoph Ruegg, Marcus Cuda, Jurgen Van Gael y colaboradores	4.11.0
Microsoft.Bcl.AsyncInterfaces	Proporciona las interfaces IEnumerable<T> e IAsyncDisposable y tipos auxiliares para .NET Standard 2.0.	Microsoft	5.0.0
Microsoft.CodeAnalysis.Common	Se utiliza en las bibliotecas que provienen de Sonova.HardwareAbstraction. Palio.Trafo	Microsoft	3.9
Microsoft.CodeAnalysis.CSharp	Se utiliza en las bibliotecas que provienen de Sonova.HardwareAbstraction. Palio.Trafo	Microsoft	3.9

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
Microsoft.Identity.Client	La biblioteca MSAL para .NET forma parte de la plataforma de identidad de Microsoft para desarrolladores (anteriormente Azure AD) v2.0. Permite adquirir tokens de seguridad para llamar a API protegidas. Utiliza el estándar de la industria OAuth2 y OpenID Connect.	Microsoft	4.38.0.0
Microsoft.Identity.Client.Extensions.Msal	Caché de tokens multiplataforma segura para aplicaciones cliente públicas de MSAL.	Microsoft	2.19.3.0
Microsoft.IdentityModel.JsonWebTokens	Incluye tipos que brindan soporte para crear, serializar y validar tokens web JSON. Es utilizado por componentes que se comunican con servicios Backend que usan tokens web JSON para la autenticación.	Microsoft	6.8.0
Microsoft.IdentityModel.Logging	Dependencia de Microsoft.IdentityModel.Tokens	Microsoft	6.8.0
Microsoft.IdentityModel.Tokens	Dependencia de SOUP Microsoft.IdentityModel.JsonWebTokens	Microsoft	6.8.0
Microsoft.Win32.TaskScheduler.dll	Se utiliza para la herramienta de copia de seguridad FSW (copias de seguridad automatizadas).	David Hall	2.5.11.0
Microsoft.Xaml.Behaviors.Wpf	XAML Behaviors es un medio fácil de usar para añadir interactividad común y reutilizable a sus aplicaciones WPF con un código mínimo.	xamlexperienceteam, Microsoft	1.0.1
MS VC++ 2008 Redistributable	Microsoft Visual C++ 2008 Redistributable	Microsoft	9.0.30729.6161
Microsoft Visual C++ 2010 x86 Redistributable	Microsoft Visual C++ 2010 Redistributable	Microsoft	10.0.40219.325
Microsoft Visual C++ 2012 Redistributable	Microsoft Visual C++ 2012 Redistributable	Microsoft	11.0.61030.0
Microsoft Visual C++ 2017 Redistributable (x86)	Microsoft Visual C++ 2017 Redistributable	Microsoft	14.16.27024.1
Bibliotecas en tiempo de ejecución de MS-Visual C++ 7.1	Bibliotecas en tiempo de ejecución de Microsoft Visual C++	Microsoft	7.10.6030.0
NAL-NL1	NAL-NL1 Fitting formula library.	Australian Hearing	1.1.0.0
NAL-NL2	NAL-NL2 Fitting formula library.	Australian Hearing	2.0.11
NAudio.dll	Se utiliza para ajustar el volumen y reproducir archivos de sonido.	Open Source	1.9
.NET Framework	Marco de tiempo de ejecución .NET	Microsoft	4.8.3928.0

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
Newtonsoft.Json	Se utiliza para la serialización y deserialización de JSON.	James Newton-King	12.0.3
Nibelung	Bibliotecas de adaptación Noahlink inalámbrico	GN ReSound	1.3.16.1
Nlog	Esta es una dependencia de HIMSA Nibelung.CPD (Noahlink inalámbrico)	Kim Christensen	4.4.0
NoahLink	Controlador del dispositivo de adaptación NoahLink	HIMSA	1.55.6.166
Noahlink inalámbrico	Controlador del dispositivo de adaptación Noahlink inalámbrico	HIMSA	2.0.0.68
Otometrics.HiPro2	Bibliotecas de comunicación HiPro	GNOtometrics	2.0.0.4
Otometrics.REMaccess	Capa de abstracción de Otometrics sobre la biblioteca de interfaz de comunicación entre módulos Noah	GN Otometrics	1.0.0.10
Pdfium.Net.SDK	La biblioteca PDF de C# para crear y editar documentos PDF en aplicaciones .Net.	Patagames.com	4.54.2704.0
Polly	Biblioteca que permite a los desarrolladores expresar resiliencia y políticas de manejo de fallos transitorios como Retry, Circuit Breaker, Bulkhead Isolation y Fallback de manera fluida y segura para subprocesos.	App vNext	7.2.1
Polly.Extensions.Http	Una biblioteca que contiene métodos prácticos para configurar políticas Polly con el fin de gestionar fallos transitorios típicos de llamadas a través de HttpClient.	App vNext	3.0
Polly.Contrib.WaitAndRetry	Una biblioteca para Polly que contiene métodos auxiliares para diversas estrategias de espera y reintento.	Grant Dickinson, App vNext	1.1.1
Portable.BouncyCastle	Esta es una dependencia de HIMSA Nibelung.CPD (Noahlink inalámbrico)	BouncyCastle.Crypto	1.8.10.0
protobuf-net.dll	Marco de serialización utilizado para blob RC.	Open Source	2.0.0.668
Serilog	El componente de registro que se utiliza para toda la aplicación Chinook.	Colaboradores de Serilog	2.10.0
Serilog.Enrichers.Thread	Eventos de Enrich Serilog con propiedades del hilo actual	Colaboradores de Serilog	3.1
Serilog.Expressions	Filtrado de eventos mediante expresiones para Serilog.	Colaboradores de Serilog	2.0
Serilog.Sinks.Console	Un sink Serilog que escribe eventos de registro en la consola o terminal.	Colaboradores de Serilog	4.0.0.0
Serilog.Sinks.Debug	Un sink Serilog que escribe eventos de registro en la ventana de salida de depuración.	Colaboradores de Serilog	2.0
Serilog.Sinks.File	Escribe eventos de Serilog en archivos de texto en formato simple o JSON.	Colaboradores de Serilog	4.1

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
Serilog.Sinks.Trace	El sink de seguimiento de diagnóstico para Serilog.	Colaboradores de Serilog	2.1
Serilog.Settings.AppSettings	Configuración XML (System.Configuration <appSettings>) soporte para Serilog.	Colaboradores de Serilog	2.2.2
Security.Cryptography	Extensiones de las API de seguridad incluidas con el marco .NET	Microsoft	1.7.2
SharpBITS API	SharpBITS.NET es un contenedor .NET de BITS API y una pequeña aplicación de interfaz de usuario de Windows para facilitar el acceso a las cargas y descargas de BITS.	perpetualKid	2.1.0.0
SharpZipLib	#ziplib (SharpZipLib, anteriormente NzipLib) es una biblioteca Zip, Gzip, Tar y Bzip2 escrita completamente en C# para la plataforma .NET. Esta biblioteca proporciona funcionalidad de compresión (comprimir, descomprimir, compresión de flujo, etc.). La usamos en la aplicación de actualización de firmware.	Open Source	1.1.0.145
Superpower	Una biblioteca de combinador de analizadores para C#	Datalust, colaboradores de Superpower y Sprache	2.3
SQLite.Interop	SQLite es una biblioteca de software que proporciona un sistema de gestión de bases de datos relacionales. El «lite» de SQLite significa peso ligero en términos de configuración, administración de base de datos y recursos requeridos. SQLite tiene las siguientes características notables: independiente, sin servidor, sin configuración y transaccional. Es una base de datos (SQLite 3.32.1) para almacenar información sobre el paciente (en modo independiente), los recursos de nuestro catálogo de productos y los metadatos para adaptación, accesorios y HIs.	Equipo de desarrollo de SQLite	1.0.113
System Buffers	Proporciona agrupación de recursos de cualquier tipo para aplicaciones de rendimiento crítico que asignan y liberan objetos con frecuencia.	23rogramma, dotnetframework	4.5.1
System.Collections.Immutable	Se utiliza en las bibliotecas que provienen de Sonova.HardwareAbstraction. Palio.Trafo	Microsoft	5.0
System.ComponentModel.Annotations	Proporciona atributos que se utilizan para definir metadatos para los objetos utilizados como fuentes de datos.	23rogramma, dotnetframework	4.7
System.Configuration.Configuration Manager	Proporciona tipos que admiten el uso de archivos de configuración.	Microsoft	5.0
System.Data.SQLite.Core	Se utiliza en las bibliotecas que provienen de Sonova.HardwareAbstraction. Palio.Trafo	Equipo de desarrollo de SQLite	1.0.113.7

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
System.Drawing.Common	Proporciona acceso a la funcionalidad de gráficos GDI+.	Microsoft	5.0.1
System.IdentityModel.Tokens.Jwt	Incluye tipos que proporcionan soporte para crear, serializar y validar tokens web JSON. Es utilizado por componentes que se comunican con servicios Backend que usan tokens web JSON para la autenticación.	Microsoft	6.8.0
System.IO.Abstractions	Un conjunto de abstracciones que ayuda a que las interacciones del sistema de archivos sean comprobables.	Tatham Oddie & friends	12.0.10
System.Numerics.Vectors	Proporciona tipos numéricos acelerados por hardware, adecuados para aplicaciones gráficas y de procesamiento de alto rendimiento.	24rogramma, dotn etfra me work	4.5
System.Memory	Proporciona tipos para la representación y agrupación eficiente de segmentos de memoria administrados, de pila y nativos, y secuencias de dichos segmentos, junto con funciones básicas para analizar y dar formato al texto codificado en UTF-8 almacenado en esos segmentos de memoria.	24rogramma, dotn etfra me work	4.5.4
System.Reactive.Core	Extensiones reactivas (Rx) para .NET	.NET Foundation	3.1.1
System.Reactive.Interfaces	Extensiones reactivas (Rx) para .NET	.NET Foundation	3.1.1
System.Reactive.Linq	Extensiones reactivas (Rx) para .NET	.NET Foundation	3.1.1
System.Reactive.PlatformServices	Extensiones reactivas (Rx) para .NET	.NET Foundation	3.1.1
System.Reactive.Windows.Threading	Extensiones reactivas (Rx) para .NET	.NET Foundation	3.1.1
System.Reflection.DispatchProxy	Proporciona una clase para crear de forma dinámica tipos de proxy que implementen una interfaz específica y deriven de un tipo DispatchProxy específico. Las invocaciones de métodos en la instancia de proxy generada se envían a ese tipo base DispatchProxy.	Microsoft	4.7.1
System.Reflection.Metadata	Este paquete proporciona un lector y escritor de metadatos .NET (ECMA-335) de bajo nivel. Está orientado al rendimiento y es la opción ideal para crear bibliotecas de nivel superior que pretendan proporcionar su propio modelo de objetos, como los compiladores.	Microsoft	5.0

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
System.Runtime.CompilerServices.Unsafe	Proporciona el System.Runtime. Clase CompilerServices.Unsafe, que proporciona una funcionalidad genérica de bajo nivel para manipular punteros.	24rogramma, dotnetframework	5.0
System.Security.AccessControl	Proporciona clases base que permiten administrar listas de control de acceso y auditoría en objetos que se pueden proteger.	Microsoft	5.0
System.Security.Permissions	Proporciona tipos compatibles con la seguridad de acceso al código (CAS).	Microsoft	5.0
System.Security.Principal.Windows	Proporciona clases para recuperar el usuario actual de Windows y para interactuar con usuarios y grupos de Windows.	Microsoft	5.0
System.Text.Encoding.CodePages	Proporciona soporte para codificaciones con base en páginas de códigos, incluidas Windows-1252, Shift-JIS y GB2312.	Microsoft	5.0
System.Text.Encodings.Web	Proporciona tipos para codificar y ocultar cadenas de caracteres para su uso en JavaScript, lenguaje de marcado de hipertexto (HTML) y localizadores de recursos uniformes (URL). Es una dependencia de SOUP IdentityModel	24rogramma, dotn etfra me work	5.0
System.Text.Json	Proporciona tipos de alto rendimiento y baja asignación que serializan objetos en JavaScript Object Notation (JSON) y deserializan texto JSON en objetos, con soporte UTF-8 incorporado. También proporciona tipos para leer y escribir texto JSON codificado como UTF-8, y para crear un modelo de objetos del documento (DOM) en memoria, que es de solo lectura, para el acceso aleatorio a los elementos JSON dentro de una vista estructurada de los datos.	Microsoft	5.0.1
System.Threading.Tasks.Extensions	Proporciona tipos adicionales que simplifican el trabajo de escritura de código simultáneo y asíncrono.	25rogramma, dotnetfra mework	4.5.4
System.ValueTuple	Proporciona las estructuras System.ValueTuple, que implementan los tipos subyacentes para tuplas en C# y Visual Basic. Añade soporte para tuplas de valor, ya que solo se incluyen en versiones posteriores de .NET Framework.	25rogramma, dotnetfra mework	4.5.0
Thrift	Se utiliza para la definición del protocolo Remotelink	Apache	0.13.0.0
Unity	El Unity Container (Unity) es un contenedor de inyección de dependencias extensible y con todas las funciones.	Proyecto de Unity Container	5.8.13
Controlador del adaptador WAP BT	Controlador del adaptador WAP BT (adaptador compatible)	iAnywhere Solutions	3.0.0.6095

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
WebSync	Se utiliza para la integración del canal de datos de adaptación	FM (Frozen Mountain)	4.9.32.0
Renderizado de XPS a PDF (NiXPS)	Convertir archivos 25rogrammatically XPS a PDF; se utiliza en informes de aplicaciones de adaptación.	NiXPS	2.6.7.0

14. REFERENCIAS

Título	Sitio web
Instrucciones de uso (formato electrónico)	https://ifu.advancedbionics.com/
Política de privacidad global de Advanced Bionics	https://advancedbionics.com/privacy
HIMSA	https://www.himsa.com/
Noah System 4	https://www.himsa.com/products/all-about-noah-system-4/
Copias de seguridad y restauración de datos en su base de datos Noah	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/backing-up-and-restoring-the-data-in-your-noah-database/
Se ha alcanzado la capacidad máxima de la base de datos del sistema Noah.	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/noah-system-database-capacity-has-been-reached/
TeamViewer: lista de puertos utilizados	https://community.teamviewer.com/English/kb/articles/4139-ports-used-by-teamviewer
BCP 195	https://www.rfc-editor.org/info/bcp195
Documentación de seguridad del servidor LiveSwitch	https://developer.liveswitch.io/liveswitch-server/server/security.html
Mejores prácticas para la adaptación segura de dispositivos auditivos (informe técnico de EHIMA)	https://www.ehima.com/wp-content/uploads/2021/09/EHIMA_Cybersecurity-FSW-Security-Whitepaper_v1-Sep2021_.pdf

 Advanced Bionics LLC
28515 Westinghouse Place
Valencia, CA 91355, United States
T: +1.661.362.1400

info.us@advancedbionics.com

 Advanced Bionics GmbH
Feodor-Lynen-Strasse 35
D-30625 Hannover

info.switzerland@advancedbionics.com

Para obtener información sobre otras ubicaciones de AB,
visite *advancedbionics.com/contact*

AB: A Sonova brand

Consulte con su representante local de AB la aprobación
reglamentaria y la disponibilidad en su región.

La marca y los logotipos de Bluetooth® son marcas
comerciales registradas propiedad de Bluetooth SIG, Inc.,
y cualquier uso de dichas marcas por parte de Sonova
AG se realiza bajo licencia.