ADVANCED BIONICS
POWERFUL CONNECTIONS

Target CI v1.6

GUÍA DE CIBERSEGURIDAD

Español

Actualizado: julio de 2026



A Sonova brand

ES

Contenido

1. INTRODUCCIÓN 3
   1.1 ABREVIATURAS Y DEFINICIONES: 3

2. OTROS RECURSOS 4
   2.1 ATENCIÓN AL CLIENTE 4
   2.2 PRO PORTAL DE AB 4
   2.3 GUÍA DE INSTALACIÓN AVANZADA 4
   2.4 CONFIGURACIÓN DEL FIREWALL DEL TARGET CI 4
   2.5 MDS2 5
   2.6 INSTRUCCIONES DE USO (IFU) 5
   2.7 HIMSA 5

3. RED Y DIAGRAMAS CONTEXTUALES 6
   3.1 MODELO DE IMPLEMENTACIÓN 1: INDEPENDIENTE 6
   3.2 MODELO DE IMPLEMENTACIÓN 2: NOAH DISTRIBUTED 7
   3.3 ARTEFACTOS DE IMPLEMENTACIÓN 8
   3.4 INTERCONEXIONES DEL SISTEMA 9

4. REQUISITOS DEL SISTEMA 11

5. CIBERSEGURIDAD EN EL CICLO DE VIDA DEL PRODUCTO 12
   5.1 DESPLIEGUE 12
   5.2 INSTALACIÓN 12
   5.3 CONFIGURACIÓN Y FUNCIONAMIENTO 13
   5.4 RETIRO Y DESMANTELAMIENTO 14

6. CONTROLES DE SEGURIDAD 16
   6.1 CONTROLES DE ACCESO 16
   6.2 REGISTRO DE AUDITORÍA Y CONTROLES DE RENDICIÓN DE CUENTAS 16
   6.3 ACCESO REMOTO 17

7. PROTECCIÓN DE LA INFORMACIÓN 18
   7.1 POLÍTICA DE PRIVACIDAD DE Advanced Bionics 18
   7.2 ESTÁNDARES FEDERALES DE PROCESAMIENTO DE LA INFORMACIÓN (FIPS) 18
   7.3 INFORMACIÓN DE IDENTIFICACIÓN PERSONAL/INFORMACIÓN DE SALUD PÚBLICA PROCESADA POR EL PRODUCTO 18
   7.4 SEGURIDAD EN TRÁNSITO 20
   7.5 SEGURIDAD EN REPOSO 21

ES

8. INTEGRIDAD DEL SOFTWARE 24
8.1 VERIFICACIÓN DE LOS MEDIOS DE INSTALACIÓN DESCARGADOS 24
8.2 VERIFICACIÓN MANUAL DEL SOFTWARE DE PROGRAMACIÓN ANTES DE LA INSTALACIÓN 24
8.3 VERIFICACIÓN AUTOMÁTICA DE LA INTEGRIDAD DEL SOFTWARE DE PROGRAMACIÓN INSTALADO 26
8.4 VERIFICACIÓN MANUAL DE LA INTEGRIDAD DEL SOFTWARE DE PROGRAMACIÓN INSTALADO 26

9. PARCHES Y ACTUALIZACIONES DE SOFTWARE 28

10. GESTIÓN DE DATOS 28
10.1 BASES DE DATOS 28
10.2 MIGRACIÓN DE DATOS 29
10.3 CONFIGURACIONES DE DISPOSITIVOS AUDITIVOS 29
10.4 ELIMINACIÓN DE DATOS 29

11. ENTORNO DE SEGURIDAD: RESPONSABILIDAD COMPARTIDA 30

12. FABRICACIÓN, DESARROLLO DE SOFTWARE Y GESTIÓN DE SEGURIDAD 32

13. COMPONENTES DE SOFTWARE Y LISTA DE MATERIALES 34

14. REFERENCIAS 56

1. INTRODUCCIÓN

Este documento proporciona información técnica de seguridad y privacidad acerca del sistema de software Target CI v1.6 de Advanced Bionics, en lo sucesivo, «software de adaptación». El software de adaptación 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 adaptación. 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 adaptación de AB
- Software de AB distinto de Target CI v1.6
- Sitios web de AB
- Aplicaciones móviles de AB
- Dispositivos auditivos de AB

1.1 ABREVIATURAS Y DEFINICIONES:

Acrónimo	Término
FSW	Software de adaptación
SaMD	Software como dispositivo médico
Noah	Un sistema de gestión de pacientes de terceros de HIMSA se utilizaba para almacenar y gestionar los datos demográficos y de ajuste de los pacientes.
TeamViewer	Una herramienta multiplataforma para acceso remoto y uso compartido de escritorio
SOUP (por sus siglas en inglés)	Software de procedencia desconocida
HCP	Audiólogo
SaMD	Software como dispositivo médico
AB	Advanced Bionics
Sonova	Advanced Bionics es una filial propiedad al 100 % de Sonova y funciona como una entidad integral dentro del Grupo Sonova.
IFU	Instrucciones de uso
PHI (por sus siglas en inglés)	Información sanitaria protegida

Acrónimo	Término
PII (por sus siglas en inglés)	Información de identificación personal
SBOM (por sus siglas en inglés)	Lista de materiales del software

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 adaptación, 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 adaptación y la documentación relacionada se pueden descargar desde https://www.abproportal.com o la plataforma 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 v1.6 está disponible previa solicitud. La guía proporciona información técnica sobre el instalador del software de adaptación, incluidas las opciones de línea de comandos para instalaciones silenciosas y automatizadas.

2.4 CONFIGURACIÓN DEL FIREWALL DEL TARGET CI

El documento de configuración del firewall está disponible bajo solicitud. Este documento proporciona orientación centrada en TI para garantizar que Target CI 1.6 funcione detrás de un firewall corporativo, detallando el acceso HTTP/HTTPS necesario y los nombres de host clave. Cubre la conectividad WebRTC a través de Twilio y Xirsys, describiendo los puertos TURN y de retransmisión entre pares, y señalando que muchas direcciones IP son dinámicas, por lo que se deben utilizar reglas basadas en el nombre de host siempre que sea posible.

2.5 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 información sobre seguridad y privacidad relacionada con el software de adaptación de AB. Este formulario está disponible bajo previa solicitud.

2.6 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 funcionamiento
- Eliminación y material peligroso
- Asistencia técnica

2.7 HIMSA

La Hearing Instrument Manufacturer's Software Association (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 adaptación 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/

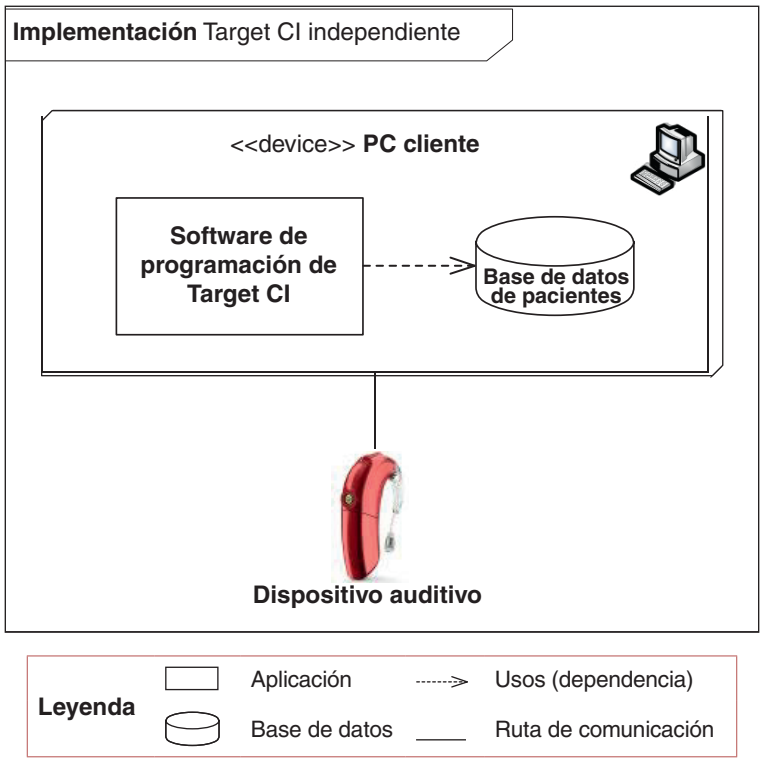
ES

3. RED Y DIAGRAMAS CONTEXTUALES

Hay dos modelos de implementación compatibles con el software de adaptación, 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.

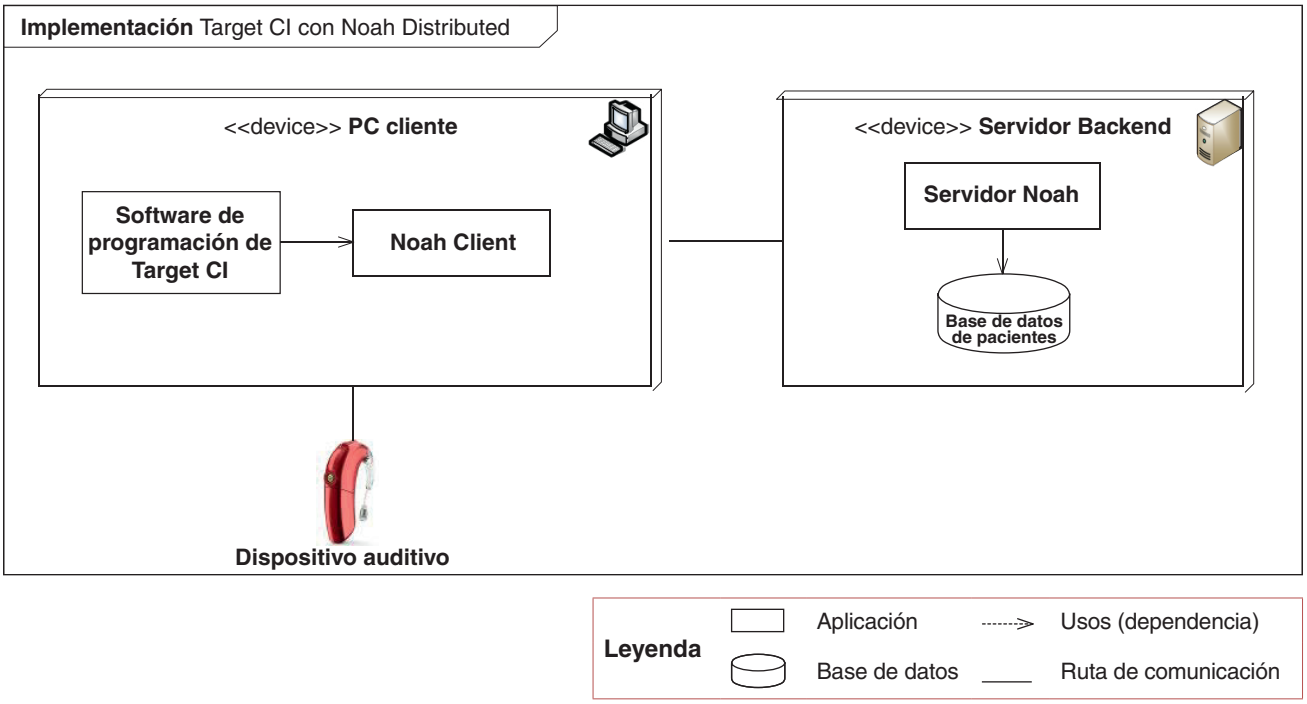
3.1 MODELO DE IMPLEMENTACIÓN 1: INDEPENDIENTE

En el modelo de implementación independiente, el software de adaptación 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 adaptación.



3.2 MODELO DE IMPLEMENTACIÓN 2: NOAH DISTRIBUTED

En el modelo de implementación de Noah Distributed, el software de adaptación se implementa en uno o más PC clientes que cuentan con Noah instalado. 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.



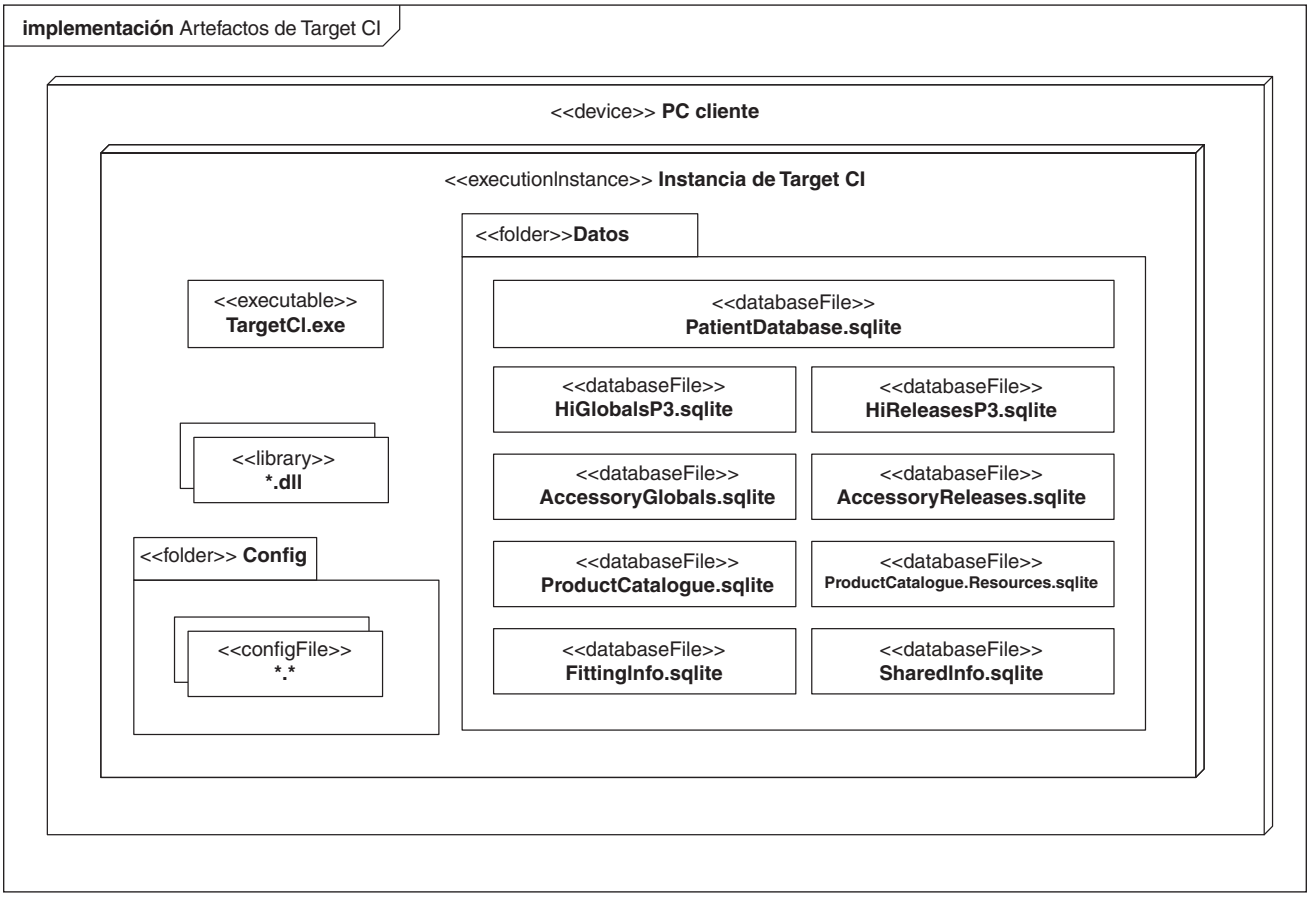
ES

3.3 ARTEFACTOS DE IMPLEMENTACIÓN

El software de adaptación 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.

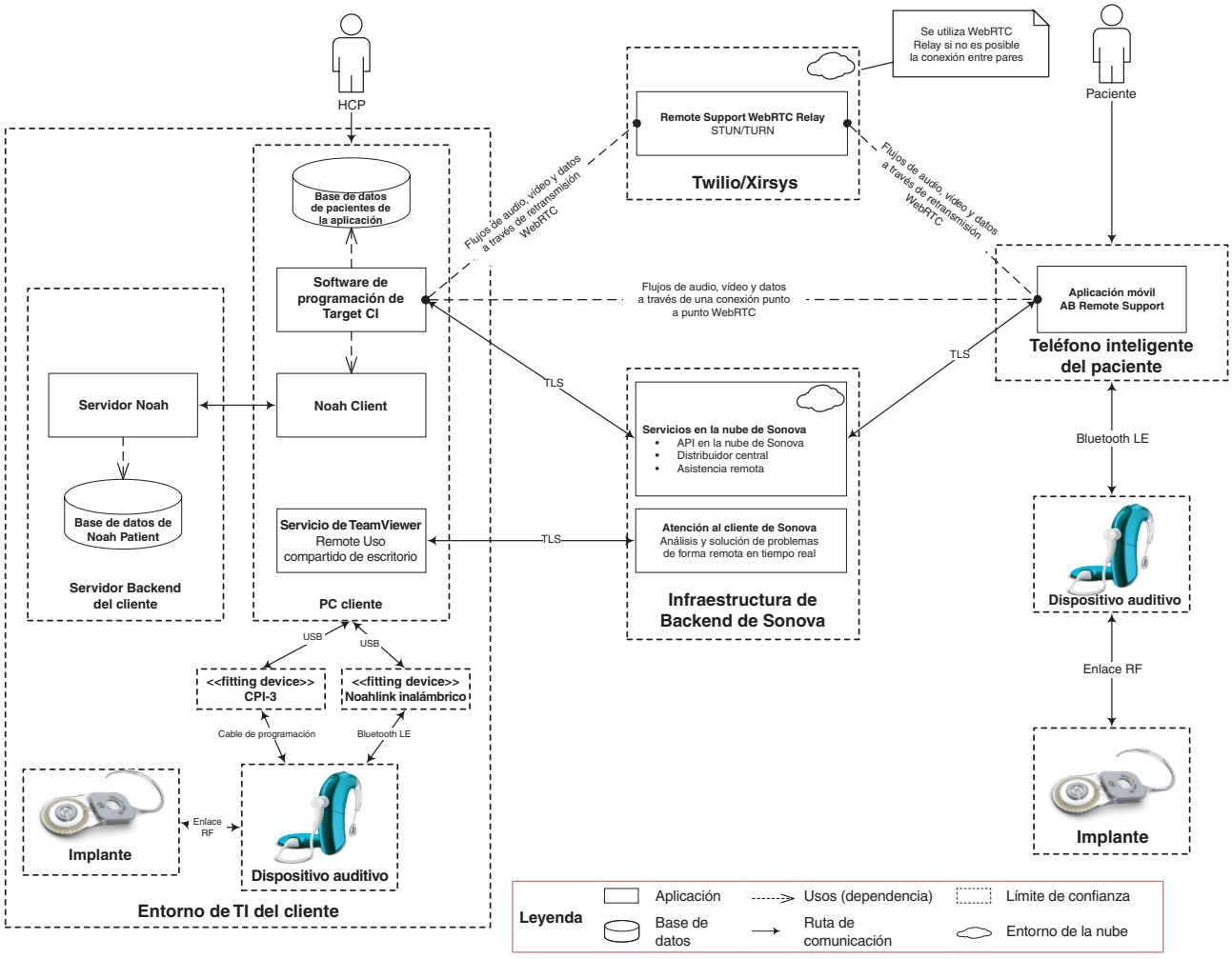
La base de datos transaccional, PatientDatabase.sqlite, almacena los datos demográficos y de ajuste del paciente y se instalará solo cuando el software de adaptación se implemente en modo independiente.

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



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
Dispositivo auditivo	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)

Fuente/ Destino	Servicio	Protocolo	Puerto	Descripción
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 adaptación desde el almacenamiento Backend de Sonova • Transferir registros y datos de análisis • establecer una adaptación remota en tiempo real
Twilio/Xirsys, AB Remote Support y AB Remote Support + Mobile Apps	Asistencia remota	WebRTC	Se puede encontrar en el documento de configuración del firewall de Target CI	Utilizado por la función de soporte remoto para realizar señalización WebRTC y realizar sesiones de adaptación remoto 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 adaptación. Consulte la sección 6.3 ACCESO REMOTO para obtener más información.

4. REQUISITOS DEL SISTEMA

Sistema operativo	Windows 10,11, Pro/Enterprise
.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 4.16 o superior)
Conexión a Internet	Se requiere conexión a Internet para asistencia remota y registro de análisis; consulte la sección 3.4 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 2. Otros recursos: HIMSA para los puertos utilizados por el Noah System 4.

ES

5. CIBERSEGURIDAD EN EL CICLO DE VIDA DEL PRODUCTO

5.1 DESPLIEGUE

Métodos de despliegue aprobados:

1. Descárguelo desde el cliente web de Sonova (SFTP) en https://webclient.sonova.com o desde el portal AB Pro en https://www.abproportal.com
2. Instalar desde una memoria USB oficial de Advanced Bionics.

Antes de la instalación, verifique la firma digital del instalador y analice el archivo con un software antivirus actualizado. Consulte la Sección 8 para obtener instrucciones detalladas sobre la verificación de la integridad. Durante la implementación, aplique los controles de seguridad informática estándar para el sector sanitario, incluida la protección de los dispositivos finales y las restricciones de red.

Al usar una memoria USB:

- Utilice únicamente memorias USB oficiales proporcionadas por Advanced Bionics.
- Mantenga la memoria USB físicamente segura y no altere su contenido.
- Analice la unidad USB y el entorno de instalación con un antivirus actualizado y agregue aplicaciones a la lista blanca.
- Advanced Bionics no se responsabiliza de los datos no autorizados que se almacenen en las memorias USB que contengan el paquete de instalación.

5.2 INSTALACIÓN

Se requiere una cuenta de administrador para instalar el software de adaptación. 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 verificar 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 del software de adaptación que se va a instalar es la última disponible.
- El sistema operativo subyacente está actualizado.
- Se verifica la integridad y autenticidad de los datos del instalador del software de adaptación correspondiente. Consulte la sección 8, para obtener información sobre cómo validar la integridad del software antes de la instalación

Hay dos instaladores disponibles para instalar el software de adaptación:

- 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 adaptación. 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.

Para escenarios de instalación avanzados, siga las instrucciones de la Guía de instalación avanzada del software de adaptación (consulte la sección 2.3). Para escenarios de instalación estándar, consulte la Sección 2.5 de este documento, que incluye un enlace a las Instrucciones de uso del software de adaptación (IFU).

5.3 CONFIGURACIÓN Y FUNCIONAMIENTO

El software de adaptación admite un conjunto de controles y funciones de privacidad y seguridad. Algunas funciones de privacidad y seguridad del software de adaptación están habilitadas por defecto, otras son configurables en el momento de la instalación y dependen del modelo de implementación seleccionado, y otras son configurables durante el uso normal a través de la interfaz gráfica de usuario de la aplicación.

Consultar:

- Sección 6 para obtener una lista de los controles de seguridad que mejoran la protección del sistema de aplicación del software de adaptación correspondiente.
- Sección 7 para obtener una lista de los controles de seguridad que mejoran la protección de los datos procesados por la aplicación del software de adaptación correspondiente.

Se espera que los usuarios (por ejemplo, profesionales de la salud, administradores del sistema o personal de TI) habiliten y configuren controles adicionales de privacidad y seguridad (que no son compatibles con el software de adaptación a nivel de aplicación) a nivel del sistema operativo y/o de la infraestructura de TI. Consulte la Sección 11 de este documento para obtener una lista detallada de recomendaciones de mejores prácticas y controles de seguridad para el entorno de adaptación donde se utilizará el software de adaptación.

Firewall

El software de adaptación no incluye un firewall interno.

En caso de que se haya habilitado un firewall externo (por ejemplo, a nivel del sistema operativo), es posible que sea necesario actualizar su configuración para permitir el tráfico entrante y saliente requerido (por ejemplo, flujos de audio/vídeo/datos WebRTC durante una sesión de soporte remoto). Consulte el documento de configuración del firewall del software de adaptación, que contiene la lista de direcciones de red y puertos utilizados por dicho software.

Configuración del proxy

El software de adaptación se configura mediante un proxy local. Mediante la interfaz gráfica de usuario (GUI) del software de adaptación, es posible cambiar la configuración de dicho proxy:

- Sin proxy
- Detectar automáticamente la configuración del proxy
- Configuración manual del proxy. Si se selecciona esta opción, se podrán configurar los siguientes ajustes:
  - Dirección
  - Puerto
  - Habilitar/deshabilitar la autenticación por proxy (nombre de usuario, contraseña, dominio)

5.4 RETIRO Y DESMANTELAMIENTO

Consulte el documento de instrucciones de uso (IFU) del software de adaptación para obtener información detallada sobre cómo desinstalar el software.

El programa de desinstalación no elimina las categorías de datos que se enumeran en la siguiente tabla. A menos que se indique lo contrario en la columna «Notas» de la tabla, dichos datos deben ser eliminados manualmente de los sistemas por los administradores del sistema; por ejemplo, eliminando manualmente los archivos o borrando el disco del sistema utilizado para el almacenamiento de datos.

Categoría de datos	Ubicación por defecto	Notas
Datos de la aplicación	C:\ProgramData\ Advanced Bionics\ Target CI\Target CI	Incluye el siguiente tipo de datos: • Datos analíticos • Datos de configuración • Application logs • Archivos temporales

Categoría de datos	Ubicación por defecto	Notas
Datos personales	C:\ProgramData\ Advanced Bionics\Target CI\Target CI\Data	Base de datos de pacientes (relevante solo para el modelo de implementación independiente)
Herramienta de acceso remoto	C:\Program Files (x86)\Common Files\ Advanced Bionics\ TeamViewer	Se utiliza para realizar análisis en tiempo real y solucionar problemas que afectan al software de adaptación, incluidos los que surgen durante la instalación y la desinstalación. Consulte la sección 6.3 para obtener más información.

Al desinstalar el software de adaptación del ordenador/portátil que se va a dar de baja o desechar, asegúrese de borrar todos los datos confidenciales (por ejemplo, información de salud protegida, información de identificación personal).

Para las implementaciones de Noah, consulte las instrucciones detalladas para la eliminación de datos en:

https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/deleting-patient-records/

Los medios externos que contienen datos exportados desde el software de adaptación, incluidos los informes y registros, deben protegerse. Cuando ya no se utilicen, los datos deben borrarse de forma segura y/o el soporte debe borrarse o destruirse de manera segura.

Se 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).

6. CONTROLES DE SEGURIDAD

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

6.1 CONTROLES DE ACCESO

El software de adaptación no restringe el acceso a sus funciones en función de los requisitos de inicio de sesión ni de los roles de los usuarios individuales. No se admiten controles de acceso basados en roles.

Acceso de usuario local

Cuando el software de adaptación se instala como una aplicación independiente, depende de los mecanismos de control de acceso del sistema operativo anfitrión. El personal de TI del cliente puede configurar el sistema operativo anfitrión para gestionar la autenticación de usuarios y asignar derechos o privilegios de acceso. Se recomienda encarecidamente a cada usuario que inicie sesión con una cuenta individual y única.

En la sección 11 de este documento y en la sección de Directrices para la seguridad informática de las Instrucciones de uso se describen controles compensatorios adicionales.

Cuando el software de adaptación se instala como un módulo de Noah, el control de acceso se gestiona a través de Noah System 4.

Para obtener más información sobre las funciones de control de acceso implementadas por Noah System 4, consulte la documentación disponible en www.HIMSA.com.

Acceso al servicio

Los técnicos de soporte técnico in situ pueden acceder al software de adaptación teniendo en cuenta los controles de acceso configurados por el personal informático del cliente para gestionar la autenticación.

Los ingenieros de soporte de AB pueden acceder al software de adaptación mediante la función de uso compartido de escritorio que admite dicho software. Consulte la sección 6.3 para obtener información detallada sobre los controles de seguridad habilitados para esta función.

6.2 REGISTRO DE AUDITORÍA Y CONTROLES DE RENDICIÓN DE CUENTAS

El software de adaptación no genera ningún registro de auditoría ni informe adicional aparte de los proporcionados por el sistema operativo subyacente.

Modelo de implementación independiente

Cuando el software de adaptación se instala como una aplicación independiente, depende de los mecanismos de auditoría proporcionados por el sistema operativo anfitrión. El software de adaptación no tiene ninguna función integrada de este tipo. El sistema operativo anfitrión puede ser configurado por el personal de TI del cliente para registrar determinados eventos, como el inicio o la ejecución del software de adaptación. Se recomienda que cada usuario inicie sesión en el sistema operativo anfitrión con una cuenta única para facilitar la auditoría.

Modelo de implementación Noah Distributed

Cuando el software de adaptación se instala como un módulo de Noah, el registro de auditoría es gestionado por Noah System (Registro de actividad de Noah). Para obtener más información sobre los controles de auditoría disponibles en Noah System 4, consulte la documentación proporcionada en www.himsa.com.

6.3 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 adaptación 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 de uso compartido de escritorio está protegido mediante protocolos y algoritmos criptográficos considerados seguros según los estándares actuales (intercambio de claves pública/privada RSA y cifrado de sesión AES de 256 bits).

La herramienta de acceso remoto puede eliminarse manualmente sin afectar a otras funcionalidades de Target FSW. El programa de instalación de Target FSW admite un parámetro de línea de comandos que permite realizar la instalación de Target FSW desde la línea de comandos sin incluir la herramienta de acceso remoto.

ES

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 adaptación 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 v1.6 cumple con los estándares de cifrado FIPS 140-2.

7.3 INFORMACIÓN DE IDENTIFICACIÓN PERSONAL/INFORMACIÓN DE SALUD PÚBLICA PROCESADA POR EL PRODUCTO

El software de adaptación procesa la información personal y de salud del paciente.

La información del paciente es introducida manualmente por el usuario del software de adaptación, o bien es recibida por la aplicación a través de uno o más de sus flujos de datos.

En los flujos de datos principales del software de adaptación se procesan los siguientes tipos de información:

	Servicios en la nube de Sonova (distribuidor central, soporte remoto)	Dispositivo auditivo	Aplicaciones móviles	Base de datos de pacientes (local/ Noah)	Acceso remoto
Nombre				X	X(2)
Dirección				X	X(2)
Fecha de nacimiento	X(1)		X	X	X(2)
Número de teléfono				X	X(2)
Dirección de correo electrónico				X	X(2)
Números de historial médico				X	X(2)
Identificadores de dispositivo y números de serie	X(1)	X	X	X	X(2)
Dirección IP	X(1)				
Audiogramas, RECD, REUG	X(1)	X	X	X	X(2)
Datos de adaptación		X	X	X	X(2)
Datos de uso de dispositivos auditivos	X(1)	X	X	X	
Datos de uso del software de adaptación	X(1)				

(1) Seudonimización previa a la carga en el Data Lake de Sonova.

(2) Durante una sesión de uso compartido de escritorio en tiempo real, los ingenieros de soporte al cliente de AB obtienen el control total del escritorio del HCP, incluido el acceso al sistema operativo y de archivos subyacente y a los datos almacenados en él. Consulte la sección 6.3 para obtener más información.

Para obtener información más detallada sobre la recopilación y el procesamiento de datos, póngase en contacto con su representante de soporte local.

7.4 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 [8], incluido:

- 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 1.2 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.

7.5 SEGURIDAD EN REPOSO

Datos de la aplicación

Los datos de la aplicación residen en la misma máquina, en el directorio predeterminado: C:\ProgramData\Advanced Bionics\Target CI\Target CI

El derecho de acceso se hereda de su carpeta principal y está limitado a los usuarios que hayan iniciado sesión en el sistema local (grupo de usuarios INTERACTIVE integrado1[1]) durante la instalación del software.

Los usuarios autorizados tienen acceso de lectura y escritura al directorio.

Para reducir el riesgo de acceso no autorizado a los datos de la aplicación a través de la red, asegúrese de que ninguna de las carpetas o archivos que contienen los datos se comparta en la red. Las ubicaciones predeterminadas de los datos de la aplicación se enumeran en el apartado 5.4.

Base de datos de pacientes: modelo de implementación independiente

Cuando el software de adaptación se instala como una aplicación independiente, la base de datos del paciente reside en la misma máquina y los registros de datos del paciente no se cifran en reposo. La aplicación no transmite información de identificación personal a través de la red.

Cualquier usuario que pueda iniciar sesión en la máquina con el software de adaptación instalado tendrá acceso completo a todos los datos de la aplicación, incluida la base de datos de pacientes. Consulte la sección Protección de los datos para obtener orientación sobre las medidas de protección de datos recomendadas.

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.

[1] https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-special-identities-groups#interactive

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 adaptación 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 (PII) almacenada en una base de datos Noah en red será accesible para otros usuarios en diferentes equipos que cuenten con permisos para acceder a dicha base de datos. La base de datos Noah también puede configurarse para el acceso sin red e instalarse en el mismo PC que el software de adaptación.

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 adaptación a través de Noah Client, el software de adaptación 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.

Para obtener más información sobre los estándares de cifrado utilizados por Noah System, consulte el siguiente enlace:

https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/patient-database-encryption/

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

El software de adaptación 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 2048 bits. El software de adaptación 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 adaptación puede transmitir o recibir información del cliente que no constituye información de identificación personal (PII) hacia o desde un dispositivo auditivo mediante un dispositivo cableado patentado (p. ej., CPI-3), las aplicaciones móviles AB Remote Support y AB Remote Support +, o un dispositivo Noahlink inalámbrico. El dispositivo Noahlink inalámbrico se conecta con el audífono mediante Bluetooth Low Energy (BLE), a través de un canal estándar BLE cifrado con AES de 128 bits.

8. INTEGRIDAD DEL SOFTWARE

8.1 VERIFICACIÓN DE LOS MEDIOS DE INSTALACIÓN DESCARGADOS

El medio de instalación del software de adaptación Target CI se puede descargar en algunas regiones desde la plataforma Pro Portal de Advanced Bionics o 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

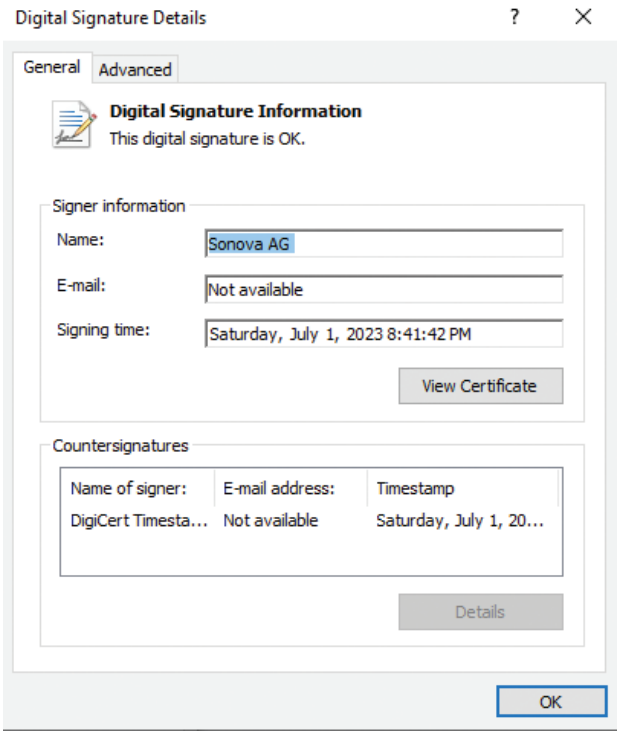
El hash SHA256 para el archivo zip de instalación de IT Professional es:
DDAD362CC3213EFEA702D9F4A61740B34EDF794FE997811B6B2C908CE754B25F

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 adaptación antes de la instalación:

1. Abra el Explorador de Windows y navegue hasta la carpeta raíz del medio de instalación del software de adaptación. 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:



6. Haga clic en el botón «Ver certificado» y en la pestaña «Detalles» y verifique que el valor del campo «Huella digital» coincida con este: db88d10f0a1bfb12be6c3c46c516e507e14f2593

7. Cierre los cuadros de diálogo emergentes y haga doble clic en SonovaVerify.exe.

8. Verifique que se muestre «NO ERRORS DETECTED» (NO SE DETECTARON ERRORES) como se muestra en la siguiente imagen

```
SonovaVerify 0.0.4.0 Copyright 2019-2025 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 . . .
```

El mensaje «NO ERRORS DETECTED» (NO SE DETECTARON ERRORES) corresponde a una verificación de integridad y autenticidad del contenido del medio de instalación del software de adaptación, realizada con éxito. Esto significa que SonovaVerify.exe ha autenticado y verificado la integridad de todos los archivos y carpetas. Esto verifica que el contenido del soporte de instalación del software de adaptación no haya sido manipulado, corrompido ni comprometido de ninguna otra manera.

SonovaVerify.exe mostrará advertencias o mensajes de error si faltan archivos o carpetas, o si se han añadido archivos o carpetas inesperados al medio de instalación. En caso de que se muestren mensajes de advertencia o error, la verificación de integridad y autenticidad del contenido del medio de instalación del software de adaptación ha fallado y se recomienda lo siguiente:

- no proceda con la instalación
- no abra ni ejecute ningún archivo contenido en la imagen de instalación del software de adaptación. Informe del problema al soporte de Advanced Bionics (consulte la Sección 2.1).

8.3 VERIFICACIÓN AUTOMÁTICA DE LA INTEGRIDAD DEL SOFTWARE DE PROGRAMACIÓN INSTALADO

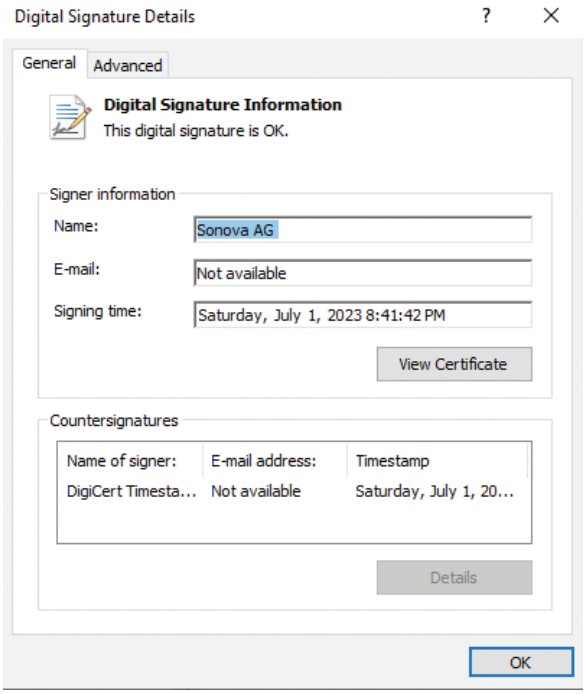
SonovaVerify está integrado con el software de programación y se ejecuta cada vez que se inicia la aplicación para verificar la integridad de los archivos de programa del software de programación. Los archivos de programa se firman de manera digital mediante prácticas estándar de la industria y certificados 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 adaptación 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:



6. Haga clic en el botón «Ver certificado» y en la pestaña «Detalles» y verifique que el valor del campo «Huella digital» coincida con este: db88d10f0a1bfb12be6c3c46c516e507e14f2593

7. Cierre los cuadros de diálogo emergentes y haga doble clic en SonovaVerify.exe.

8. Verifique que se muestre «NO ERRORS DETECTED» (NO SE DETECTARON ERRORES) como se muestra en la siguiente imagen:

```
SonovaVerify 0.0.4.0 Copyright 2019-2025 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 . . .
```

El mensaje «NO ERRORS DETECTED» (NO SE DETECTARON ERRORES) corresponde a una verificación de integridad y autenticidad del contenido del medio de instalación del software de adaptación, realizada con éxito. Esto significa que SonovaVerify.exe ha autenticado y verificado la integridad de todos los archivos y carpetas. Esto verifica que el contenido del soporte de instalación del software de adaptación no haya sido manipulado, corrompido ni comprometido de ninguna otra manera.

SonovaVerify.exe mostrará advertencias o mensajes de error si faltan archivos o carpetas, o si se han añadido archivos o carpetas inesperados al medio de instalación. En caso de que se muestren mensajes de advertencia o error, la verificación de integridad y autenticidad del contenido del medio de instalación del software de adaptación ha fallado y se recomienda lo siguiente:

- no proceda con la instalación
- no abra ni ejecute ningún archivo contenido en la imagen de instalación del software de adaptación. Informe del problema al soporte de Advanced Bionics (consulte la Sección 2.1).

9. PARCHES Y ACTUALIZACIONES DE SOFTWARE

Las actualizaciones automáticas no son compatibles. Consulte la sección 12 para obtener más información.

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 adaptación 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 adaptación. 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

Consulte la sección 5.4, Retirada y desmantelamiento, de este documento y la sección Eliminación y materiales peligrosos de las instrucciones de uso para obtener orientación sobre la eliminación de datos. Para implementaciones de Noah, encontrará instrucciones detalladas para eliminar registros de pacientes en:
https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/deleting-patient-records/

ES

11. ENTORNO DE SEGURIDAD: RESPONSABILIDAD COMPARTIDA

El software de adaptación 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 adaptación:

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
  - Habilitar el tiempo de espera de sesión inactiva
- Aplicar controles de auditoría a nivel de sistema operativo
- Asegúrese de que el sistema operativo esté actualizado
- Asegúrese de que la versión del software de adaptación instalada esté actualizada
- Utilice una protección antivirus y contra malware adecuada y actualizada
- Asegúrese de desactivar las funciones de AutoRun y AutoPlay
- Habilitar la lista blanca de aplicaciones

Protección de los datos

- Asegúrese de que ninguna de las carpetas o archivos que contienen datos de la aplicación se comparta en la red. Las ubicaciones predeterminadas de los datos de la aplicación se enumeran en la tabla de la sección 5.4. Para comprobar los recursos compartidos de red expuestos por un equipo, vaya a «Administración de equipos -> Carpetas compartidas -> Recursos compartidos» en la herramienta Administración de equipos de Microsoft o ejecute el comando de PowerShell Get-WmiObject -class Win32_Share.
- Durante la instalación, los permisos de la carpeta de datos de la aplicación se configuran de acuerdo con la Sección 6.1. Las carpetas de datos de la aplicación heredan los permisos de acceso de la carpeta principal. La gestión de permisos en la carpeta principal es responsabilidad del operador del software.

- Cifre los datos de los pacientes utilizando herramientas de terceros o controles a nivel del sistema operativo mediante el cifrado de unidades (por ejemplo, Microsoft BitLocker, que es gratuito) para proteger toda la información. 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 adaptación, 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.
- Garantice siempre la seguridad de los datos siguiendo estas prácticas:
  - Al transmitir datos a través de canales no seguros, anonimice o cifra los datos.
  - 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 aplicar los 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 está instalado el software de adaptación debe estar protegida físicamente de manera que no sea accesible para personal no autorizado ni pueda ser manipulada por este.
- Se debe controlar el acceso a las impresoras conectadas a la estación de trabajo
- El monitor de la estación de trabajo donde está instalado el software de adaptación debe colocarse de manera que limite la visibilidad del contenido de la pantalla exclusivamente al 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 adaptación.

- Únicamente el personal autorizado para mantener y operar el software de adaptación debe tener acceso a las cuentas de la máquina donde está instalado dicho software. Las cuentas de equipo y de dominio, así como los derechos de acceso asociados, deben revisarse periódicamente y desactivarse si ya no se necesita el acceso al equipo.
- Si nota alguna actividad sospechosa en sus cuentas de software de adaptación 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 adaptación para su aplicación en varios niveles, consulte:

- El informe técnico de EHIMA «Best Practices for Secure Fitting of Hearing Devices» (Mejores prácticas para la adaptación segura de dispositivos auditivos), EHIMAWhitePaper

12. FABRICACIÓN, DESARROLLO DE SOFTWARE Y GESTIÓN DE SEGURIDAD

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 adaptación 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 adaptación se ha lanzado al mercado.

Gestión de la configuración

AB desarrolla, documenta y mantiene internamente, bajo control de configuración, la configuración base de cada versión de software de adaptación que se publique.

Todos los componentes de software de terceros utilizados por la aplicación de software de adaptación se identifican y documentan en la lista de materiales del software (SBOM). AB utiliza SBOM en la gestión de riesgos de ciberseguridad para evaluar y supervisar la exposición a amenazas de ciberseguridad y vulnerabilidades reveladas mediante el uso de herramientas de escaneo de vulnerabilidades actualizadas.

Actualizaciones de seguridad

AB realiza un seguimiento constante para detectar vulnerabilidades de seguridad que afecten al software de adaptación. Esto incluye vulnerabilidades en el software de adaptación y en los componentes de terceros utilizados por la aplicación de software de adaptación.

Las vulnerabilidades anunciadas se evalúan en función de la configuración y el uso del software adaptación.

Cuando sea necesario, las vulnerabilidades de seguridad pueden corregirse mediante una versión de software más amplia que implemente parches para componentes de software específicos dentro del conjunto de software.

Divulgación de vulnerabilidades

Estamos comprometidos con la divulgación de vulnerabilidades y con la mejora de la seguridad de nuestros productos y servicios.

Se recomienda informar sobre posibles vulnerabilidades o problemas de seguridad relacionados con nuestros productos o el software/infraestructura subyacente.

Lea nuestra política de divulgación de vulnerabilidades publicada en https://www.sonova.com/en/coordinated-vulnerability-disclosure-policy y siga las instrucciones para enviar un informe.

ES

13. COMPONENTES DE SOFTWARE Y LISTA DE MATERIALES

El software de adaptación 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 adaptación.

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
AForge.NET	AForge.NET es una biblioteca de matemáticas y multimedia que forma parte de IceLink y LiveSwitch, y que es necesaria para estos sistemas.	AForge.NET	2.2.5.0
Amplifon. Programmer	Componente del paquete de software de Amplifon	Amplifon	3.3.4.0
Amplifon. Programmer.Core	Componente del paquete de software de Amplifon	Amplifon	1.0.4.0
Mapeador automático	Automatiza el mapeo de objetos	Jimmy Bogard	10.1.1.0
BenchmarkDotNet	biblioteca para evaluación comparativa, que proporciona herramientas para medir y comparar el rendimiento del código	Comunidad BenchmarkDotNet	0.13.0.0
Castle.Core	Una biblioteca fundamental del Castle Project, que ofrece componentes como la generación dinámica de proxies y contenedores de inversión de control para aplicaciones .NET.	Castle Project	4.4.1
Chessie	Una biblioteca funcional de manejo de errores para F#	Open Source	0.6.0.0
Simulador de pérdida auditiva ciAD	Biblioteca de simuladores de pérdida auditiva para reproductor multimedia	ciAD (Jürg Haubold)	4.0.0.1
ClosedXML	Simplifica la lectura, manipulación y escritura de archivos de Excel sin necesidad de tener Excel instalado.	Comunidad ClosedXML	0.95.4.0

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
CommandLine Parser	Proporciona una API limpia y concisa para analizar los argumentos de la línea de comandos.	Comunidad CommandLineParser	2.4.3
Common.Logging	Una abstracción de registro portátil para aplicaciones .NET	Comunidad Common. Logging	3.4.1.0
CommonService Locator	Proporciona una interfaz común para la localización de servicios, lo que permite que las aplicaciones se desacoplen de contenedores IoC específicos.	Microsoft	2.0.5.0
Credential Management	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	2.0.78.45418
Destructurama. Attributed	Se utiliza en las bibliotecas Nephele.	Colaboradores de Serilog	3.1.0.0
Developer Express Suite	Un conjunto completo de controles y bibliotecas de interfaz de usuario para desarrolladores .NET, que ofrece herramientas para crear aplicaciones con multitud de funciones.	Developer Express Inc	20.2.10.0
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
ExcelNumberFormat	Proporciona funcionalidad para analizar y formatear formatos numéricos de Excel.	Open Source	1.1.0.0
FM.dll	Integrados a sus marcos de comunicación en tiempo real como LiveSwitch e IceLink.	FM (Frozen Mountain)	2.9.32

ES

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
FSharp.Core	La biblioteca principal para el lenguaje de programación F#	Microsoft	6.0.322.10402
FTDI Chip	Un paquete de controladores de Future Technology Devices International (FTDI) que facilita la comunicación entre dispositivos USB y aplicaciones de software.	FTDI	3.02.07
GNOtometrics. Aurical	GNOtometrics.Aurical reempaquetado para Sonova	Natus Medical Incorporated	2.0.1.9
SharedUtilities.dll	Proporciona funciones de utilidad comunes y recursos compartidos entre las aplicaciones de Natus.	Natus Medical Incorporated	1.0.0.0
Hardware.Info	Un componente que recopila y proporciona información detallada sobre la configuración de hardware de un sistema.	Open Source	11.1.0.1
Himsa.NLWSMAPI. dll	Una biblioteca asociada al software Noah de HIMSA.	HIMSA	2.0.3.0
natus.otometrics. hipro2	Bibliotecas de comunicación HiPro	Natus Medical Incorporated	2.0.0.4
Iced.dll	facilita las comunicaciones en tiempo real al permitir la transmisión inalámbrica de audio, vídeo y datos	FM (Frozen Mountain)	1.12.0.0
IceLink	Se utiliza para la integración de conferencias de audio/vídeo WebRTC.	FM (Frozen Mountain)	3.13.100.13250
icudt.dll	ofrece compatibilidad con Unicode y globalización para aplicaciones de software	FM (Frozen Mountain)	54.1.0.0
IdentityModel	Biblioteca cliente de OpenID Connect y OAuth 2.0 utilizada por el componente Kona.CommonServices. Authentication para la autenticación OAuth 2.	Dominick Baier, Brock Allen	6.2.0.0
IMCInterfaces	Biblioteca de interfaz de comunicación entre módulos Noah	HIMSA II K/S	4.4.0.2266

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
iText 7	Biblioteca PDF para crear, modificar e inspeccionar documentos PDF mediante programación.	Software iText	7.1.16.0
JetBrains. dotMemory	Una herramienta de análisis de memoria para detectar fugas de memoria y optimizar su uso en aplicaciones .NET.	JetBrains	111.0.0.0
JsonDiffPatch DotNet.dll	Proporciona funcionalidades para comparar y parchear objetos JSON.	Open Source	1.0.1.0
LibGit2Sharp	Se utiliza en bibliotecas procedentes de Sonova para comunicarse con Git	LibGit2Sharp contributors	0.26.1.93
LiveSwitch	Se utiliza para la integración de conferencias de audio/vídeo WebRTC.	FM (Frozen Mountain)	1.18.5.32382
log4net.dll	marco de registro para .NET	Apache	4.7.0.3189
Mapster	Se utiliza para mapear objetos en el código	chaowlert, eric_swann	7.2.0.0
Mapster.Core	Se utiliza para mapear objetos en el código	chaowlert, eric_swann	1.2.0.0
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 IAsyncEnumerable<T> e IAsyncDisposable y tipos auxiliares para .NET Standard 2.0.	Microsoft	6.0.21.52210
Microsoft. CodeAnalysis. Common	Se utiliza en las bibliotecas que provienen de Sonova. HardwareAbstraction.Palio. Trafo	Microsoft	3.900.21.12420
Microsoft. CodeAnalysis. CSharp	Se utiliza en las bibliotecas que provienen de Sonova. HardwareAbstraction.Palio. Trafo	Microsoft	3.900.21.12420
Microsoft.CSharp.dll	Proporciona compilación y generación de código usando C#.	Microsoft	4.700.19.56404
Microsoft. Diagnostics. FastSerialization.dl	Se utiliza para la serialización y deserialización eficiente de datos de diagnóstico.	Microsoft	1.0.0.0

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
Microsoft. Diagnostics. NETCore.Client.dll	Una biblioteca administrada que permite la interacción con el entorno de ejecución de .NET Core para diversas tareas de diagnóstico, como el rastreo y la solicitud de volcados de memoria.	Microsoft	0.2.4.27602
Microsoft. Diagnostics. Runtime.dll	Proporciona API para inspeccionar procesos en ejecución y volcados de memoria tras fallos, lo que permite a los desarrolladores crear herramientas de depuración y diagnóstico.	Microsoft	2.0.4.26801
Microsoft. Diagnostics.Tracing. TraceEvent.dll	Una biblioteca para analizar y procesar eventos de Event Tracing for Windows (ETW).	Microsoft	2.0.70
Microsoft DotNet.Platform Abstractions.dll	Proporciona API para acceder a información sobre la plataforma .NET.	Microsoft	3.100.620.31604
Microsoft Extensiones. Inyección de dependencias. Abstracciones	Define las abstracciones para la inyección de dependencias en aplicaciones .NET.	Microsoft	6.0.21.52210
Microsoft. Extensions.Logging	Facilita el registro estructurado en aplicaciones .NET.	Microsoft	6.0.21.52210
Microsoft. Extensions.Options	Admite la configuración de opciones en aplicaciones .NET	Microsoft	6.0.21.52210
Microsoft. Extensions. Primitives	Proporciona interfaces y clases para el seguimiento de cambios y tokens de cancelación, lo que facilita la gestión de datos mutables y la limpieza de recursos.	Microsoft	6.0.21.52210
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

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
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 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	6.8.0.11012
Microsoft.IdentityModel.Logging	Dependencia de Microsoft.IdentityModel.Tokens	Microsoft	6.8.0.11012
Microsoft.IdentityModel.Tokens	Dependencia del SOUP Microsoft.IdentityModel.JsonWebTokens	Microsoft	6.8.0.11012
Microsoft.ML.OnnxRuntime	Un motor de inferencia para ejecutar modelos de aprendizaje automático en el formato ONNX (Open Neural Network Exchange).	Microsoft	1.12.1
Microsoft.ML.OnnxRuntime.Managed	El contenedor .NET administrado para ONNX Runtime	Microsoft	1.12.1
Microsoft.Office.Interop.Excel.dll	Esta DLL, que forma parte de los ensamblados de Office Interop, permite que las aplicaciones .NET interactúen con Microsoft Excel.	Microsoft	14.0.4733.1000
Microsoft.VisualStudio.TextTemplates.10.0	Proporciona funcionalidades de plantillas de texto dentro de Visual Studio, lo que permite a los desarrolladores generar código y otros artefactos basados en texto utilizando plantillas T4.	Microsoft	10.0.40219.1
Microsoft.Win32.Registry.dll	Proporciona acceso al registro de Windows	Microsoft	5.0.20.51904
Microsoft.Win32.SystemEvents.dll	Admite el manejo de eventos del sistema en aplicaciones .NET	Microsoft	8.0.23.53103
Microsoft.Win32.TaskScheduler.dll	Se utiliza para la herramienta de copia de seguridad FSW (copias de seguridad automatizadas).	David Hall	2.5.11.0

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
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.	xamlexperiencesteam, Microsoft	1.0.1.0
Microsoft DIA SDK	Proporciona API para trabajar con información de depuración en archivos PDB	Microsoft	2.0.0.0
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	11.0.51106.1
Microsoft Visual C++ 2017 Redistributable (x86)	Microsoft Visual C++ 2017 Redistributable	Microsoft	14.16.27024.1
Mono.Cecil	Se utiliza para inspeccionar, modificar y crear ensamblados .NET	Microsoft	0.11.3.0
Moq.dll	Biblioteca .NET de código abierto para crear objetos simulados durante las pruebas unitarias	Comunidad Moq (Código abierto)	4.16.1.0
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	1.9.0.0
.NET Framework	Marco de tiempo de ejecución .NET	Microsoft	4.8.3928.0
Newtonsoft.Json	Se utiliza para la serialización y deserialización de JSON.	James Newton-King	13.0.3.27908
Newtonsoft.Json.Schema.dll	Una biblioteca de validación de esquemas para datos JSON	James Newton-King	3.0.14.25421

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
Nibelung	Bibliotecas de adaptación Noahlink inalámbrico	HIMSA	1.3.16.1
Nibelungo2.CPD	Bibliotecas de adaptación Noahlink inalámbrico	HIMSA	2.0.3.0
Nlog	Esta es una dependencia de HIMSA Nibelung.CPD (Noahlink inalámbrico)	Kim Christensen	5.0.4.1331
NoahLink	Controlador del dispositivo de adaptación NoahLink	HIMSA	1.55.6.166
Controlador de Noahlink inalámbrico	Controlador del dispositivo de adaptación Noahlink inalámbrico	HIMSA	1.1.0.0
Actualizador de Noahlink inalámbrico	Actualizador de firmware de Noahlink inalámbrico	HIMSA	3.1.0.82
ModuleAPI.dll (Noah System)	Un componente del sistema Noah System, que proporciona API para integrar y gestionar datos audiológicos	HIMSA	4.13.0.5404
NiXPS SDK	Proporciona funcionalidades para el manejo de documentos XPS (XML Paper Specification)	NiXPS NV	2.6.0.0
NPOI	Una biblioteca de código abierto que facilita la lectura y escritura de documentos de Microsoft Office en aplicaciones .NET	NPOI communi	2.4.1.0
NuGet Package Manager	Una herramienta para gestionar bibliotecas y paquetes .NET.	Microsoft	6.3.0.131
Nunit	Un marco de pruebas unitarias para aplicaciones .NET	NUnit Project	3.12.0.0
ONNX Runtime	Motor para modelos de intercambio de redes neuronales abiertas (ONNX)	Microsoft	1.12.20220803.2.7048164

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
Open XML SDK	Proporciona herramientas para trabajar con documentos Office Open XML.	Microsoft	2.7.2
OSExtensions.dll	Biblioteca que ofrece extensiones para funcionalidades del sistema operativo.	Microsoft	1.0.0.0
Otometrics. REMaccess	Capa de abstracción de Otometrics sobre la biblioteca de interfaz de comunicación entre módulos Noah	GN Otometrics	1.0.0.10
Paket.Core.dll	Un gestor de dependencias de código abierto para proyectos .NET y Mono	Comunidad Paket (Código abierto)	7.1.5.0
Patagames.Pdf	La biblioteca PDF de C# para crear y editar documentos PDF en aplicaciones .Net.	patagames.com	8.57.30.48
Patagames.Pdf. Wpf	La biblioteca PDF de C# para crear y editar documentos PDF en aplicaciones .Net.	Patagames.com	4.19.18.48
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	7.2.3.0
Portable. BouncyCastle	Esta es una dependencia de HIMSA Nibelung.CPD (Noahlink inalámbrico)	The Legion of the Bouncy Castle Inc	1.8.15362.1

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
Portable. BouncyCastle. Crypto	Esta es una dependencia de HIMSA Nibelung.CPD (Noahlink inalámbrico)	The Legion of the Bouncy Castle Inc	1.9.0.1
protobuf-net.dll	Marco de serialización utilizado para blob RC.	Open Source	2.3.2.0
Google.Protobuf	La biblioteca oficial de Protocol Buffers de Google para .NET, que facilita la serialización y deserialización de datos estructurados.	Google Inc	3.19.3.0
Perfolizer.dll	Una biblioteca de código abierto para el análisis del rendimiento.	Open Source	0.2.1.0
Rhino.Mocks.dll	Un marco de trabajo dinámico para objetos simulados en .NET	Cominudad Rhino Mocks	3.6.0.0
Security. Cryptography. NetCore.dll	Proporciona funcionalidades criptográficas para aplicaciones .NET Core	HardDev	1.0.1.0
Serilog	El componente de registro que se utiliza para toda la aplicación Chinook.	Colaboradores de Serilog	3.0.1.0
Serilog. Enrichers.Thread	Eventos de Enrich Serilog con propiedades del hilo actual	Colaboradores de Serilog	3.1.0.0
Serilog. Extensions. Logging	Integra Serilog con las abstracciones de registro de Microsoft	Colaboradores de Serilog	3.1.0.0
Serilog. Expressions	Filtrado de eventos mediante expresiones para Serilog.	Colaboradores de Serilog	2.0.0.0
Serilog.Sinks. Console	Un sink Serilog que escribe eventos de registro en la consola o terminal.	Colaboradores de Serilog	4.0.0.0

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
Serilog.Sinks. Debug	Un sink Serilog que escribe eventos de registro en la ventana de salida de depuración.	Colaboradores de Serilog	2.0.0.0
Serilog.Sinks.File	Escribe eventos de Serilog en archivos de texto en formato simple o JSON.	Colaboradores de Serilog	4.1.0.0
Serilog.Sinks. NUnit.dll	Se integra con NUnit, dirigiendo los eventos de registro a la salida de prueba de NUnit, lo que ayuda en el diagnóstico de las pruebas.	Colaboradores de Serilog	1.0.3.0
Serilog.Sinks. Trace	El sink de seguimiento de diagnóstico para Serilog.	Colaboradores de Serilog	2.1.0.0
Serilog.Settings. AppSettings	Compatibilidad con configuración XML (System.Configuration <appSettings>) para Serilog.	Colaboradores de Serilog	2.2.2.0
Security. Cryptography. NetCore.dll	Extensiones de las API de seguridad incluidas con el marco .NET	Microsoft	1.0.1.0
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

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
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	1.3.3.11
SharpDX	Utilizado por LiveSwitch: SharpDX.Direct3D11, SharpDX.Direct2D1, SharpDX.Mathematics	Alexandre Mutel	4.0.1
SocketIOClient	Proporciona un cliente para Socket.IO, lo que permite la comunicación bidireccional en tiempo real basada en eventos en aplicaciones .NET.	HeroWong	2.2.4.0
Superpower	Una biblioteca de combinador de analizadores para C#	Datalust, colaboradores de Superpower y Sprache	2.3.0.0

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
SQLite.Interop	Biblioteca de interoperabilidad nativa SQLite 3.36.0. SQLite es la base de datos integrada que se utiliza para almacenar información sobre el paciente (en modo independiente), nuestro catálogo de productos y sus recursos, así como los metadatos de adaptación, accesorios y sistemas auditivos. SQLite es de dominio público.	Equipo de desarrollo de SQLite	1.0.115
System.Buffers	Proporciona agrupación de recursos de cualquier tipo para aplicaciones de rendimiento crítico que asignan y liberan objetos con frecuencia.	microsoft, dotnetframework	4.6.28619.01
System. Collections. Immutable	Se utiliza en las bibliotecas que provienen de Sonova. HardwareAbstraction. Palio.Trafo	Microsoft	7.0.22.51805
Sistema.Modelo de Componente . Anotaciones	Proporciona atributos que se utilizan para definir metadatos para los objetos utilizados como fuentes de datos.	microsoft, dotnetframework	4.6.26515.06
Sistema. Configuración. Administrador de Configuración	Proporciona tipos que admiten el uso de archivos de configuración.	Microsoft	5.0.20.51904
System. CodeDom.dll	Proporciona clases para generar y compilar código fuente en archivos ejecutables o ensamblados	Microsoft	8.0.23.53103

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
System.Data.SQLite	Se utiliza en las bibliotecas que provienen de Sonova.HardwareAbstraction.Palio.Trafo	Equipo de desarrollo de SQLite	1.0.115.0
Sistema.Diagnóstico DiagnosticSource	Una biblioteca de registro que permite a los desarrolladores rastrear y monitorear datos de diagnóstico.	Microsoft	6.0.21.52210
Sistema.DiagnósticoContador de Rendimiento	Proporciona API para interactuar con los contadores de rendimiento de Windows	Microsoft	7.0.22.51805
System.Drawing.Common	Proporciona acceso a la funcionalidad de gráficos GDI+.	Microsoft	8.0.324.11603
System.Formats.Asn1.dll	Admite la codificación y decodificación de datos en Abstract Syntax Notation One (ASN.1).	Microsoft	6.0.21.52210
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	6.8.0.11012
System.IO.Abstractions	Un conjunto de abstracciones que ayuda a que las interacciones del sistema de archivos sean comprobables.	Tatham Oddie & friends	12.0.10.46693

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
System.IO.Hashing.dll	Proporciona funcionalidades de hash dentro de .NET, incluidos algoritmos para calcular sumas de verificación y hashes criptográficos.	Microsoft	6.0.222.6406
System.IO.Packaging.dll	Permite la lectura y escritura de archivos de paquete	Microsoft	6.0.21.52210
System.IO.Ports.dll	Proporciona clases para la comunicación por puerto serie, lo que permite que las aplicaciones .NET interactúen con el hardware conectado a través de puertos serie.	Microsoft	8.0.23.53103
System.Net.Http.WinHttpHandler.dll	Un controlador HTTP especializado para Windows	Microsoft	6.0.422.16404
System.Numerics.Vectors	Proporciona tipos numéricos acelerados por hardware, adecuados para aplicaciones gráficas y de procesamiento de alto rendimiento.	microsoft, dotnetframework	4.6.26515.06
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.	microsoft, dotnetframework	4.6.31308.01

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
System.Reactive.dll		Open Source	5.0.0.1
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	4.700.20.21406
System.Reflection.Metadata	Estos paquetes proporcionan 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	5.0.20.51904
System.Reflection.TypeExtensions	Proporciona métodos de extensión para la API de reflexión	Microsoft	4.700.19.56404
System.Runtime.CompilerServices.Unsafe	Proporciona System.Runtime.CompilerServices. Clase Unsafe, que proporciona funcionalidad genérica de bajo nivel para manipular punteros.	microsoft, dotnetframework	6.0.21.52210

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
System.Security.AccessControl	Proporciona clases base que permiten administrar listas de control de acceso y auditoría en objetos que se pueden proteger.	Microsoft	6.0.21.52210
System.Security.Permissions	Proporciona tipos compatibles con la seguridad de acceso al código (CAS).	Microsoft	5.0.20.51904
System.Security.Principal.Windows	Proporciona clases para recuperar el usuario actual de Windows y para interactuar con usuarios y grupos de Windows.	Microsoft	5.0.20.51904
System.Security.Cryptography.Cng.dll	Proporciona funcionalidad criptográfica mediante las API de Cryptography Next Generation (CNG).	Microsoft	5.0.20.51904
System.Security.Cryptography.Pkcs.dll	Ofrece cursos para el manejo de estándares de criptografía de clave pública (PKCS), incluidos datos firmados y encapsulados.	Microsoft	6.0.1923.31806
System.Security.Cryptography.ProtectedData.dll	Proporciona métodos para proteger y desproteger datos, utilizando la API de protección de datos de Windows (DPAPI) para un almacenamiento seguro de datos.	Microsoft	6.0.21.52210
System.Security.Cryptography.Xml.dll	Permite el cifrado XML y las firmas digitales, lo que brinda soporte para el manejo seguro de datos XML en aplicaciones .NET.	Microsoft	6.0.822.36306

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
System. ServiceModel. Http.dll	Proporciona funcionalidad de comunicación basada en HTTP para los servicios de Windows Communication Foundation (WCF)	Microsoft	4.700.19.56502
System. ServiceModel. Primitives.dll	Contiene clases fundamentales para los servicios WCF, incluidas clases base e interfaces para contratos de servicio y canales.	Microsoft	4.700.19.56502
System.Text. Encoding. CodePages	Proporciona soporte para codificaciones con base en páginas de códigos, incluidas Windows-1252, Shift-JIS y GB2312.	Microsoft	5.0.20.51904
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	microsoft, dotnetframework	6.0.21.52210

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
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	6.0.222.6406
System. Threading.Tasks. Extensions	Proporciona tipos adicionales que simplifican el trabajo de escritura de código simultáneo y asíncrono.	microsoft, dotnetframework	4.6.28619.01
System. Threading. Channels	Proporciona un conjunto de estructuras de datos de sincronización para el intercambio de datos entre productores y consumidores, lo que permite una programación paralela de alto rendimiento.	Microsoft	6.0.21.52210

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
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.	microsoft, dotnetframework	4.6.26515.06
TestStack.BDDfy. dll	Un marco de desarrollo basado en el comportamiento (BDD) para .NET	Comunidad de TestStack	4.3.2.0
Thrift	Se utiliza para la definición del protocolo Remotelink	Apache	0.13.0.0
Unity.Container	El Unity Container (Unity) es un contenedor de inyección de dependencias extensible y con todas las funciones.	Unity Container Project	5.8.13.0
Unity. Configuration	El Unity Container (Unity) es un contenedor de inyección de dependencias extensible y con todas las funciones.	Unity Container Project	5.2.5.0
Unity. Abstractions	El Unity Container (Unity) es un contenedor de inyección de dependencias extensible y con todas las funciones.	Unity Container Project	3.3.1.0
Unity. Interception. Configuration	El Unity Container (Unity) es un contenedor de inyección de dependencias extensible y con todas las funciones.	Unity Container Project	5.1.7.0

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
Unity. Interception	El Unity Container (Unity) es un contenedor de inyección de dependencias extensible y con todas las funciones.	Unity Container Project	5.5.5.0
Unity Registration ByConvention	El Unity Container (Unity) es un contenedor de inyección de dependencias extensible y con todas las funciones.	Unity Container Project	2.1.9.0
Unity. ServiceLocation	El Unity Container (Unity) es un contenedor de inyección de dependencias extensible y con todas las funciones.	Unity Container Project	2.1.2.0
Controlador del adaptador WAP BT	Controlador del adaptador WAP BT (adaptador compatible)	iAnywhere Solutions	3.0.0.6095
WebSync	Se utiliza para la integración del canal de datos de adaptación	FM (Frozen Mountain)	4.9.32.0
WPFHexaEditor. dll	Un control de editor hexadecimal para aplicaciones WPF	FM (Frozen Mountain)	2.1.6
WpfScreen Helper.dll	Una biblioteca de utilidades para aplicaciones WPF que proporciona información sobre la pantalla y el monitor.	FM (Frozen Mountain)	2.1.0.0
Kit de herramientas WPF extendido Xceed	Una colección de controles y utilidades de WPF que mejoran las aplicaciones WPF con componentes de interfaz de usuario adicionales.	Xceed	3.5.0.0
xmlunit-core.dll	Una biblioteca para probar y comparar la salida XML.	Comunidad XMLUnit	2.9.0.205

ARTÍCULO SOUP	DESCRIPCIÓN DE LA FUNCIONALIDAD	FABRICANTE	VERSIÓN
Renderizado de XPS a PDF (NiXPS)	Convertir archivos XPS a PDF mediante programación; utilizado en la generación de informes de aplicaciones de adaptación.	NiXPS	2.6.7.0

ES

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

CE 0123

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

info.us@advancedbionics.com

EU REP Advanced Bionics
Logistic Services GmbH
Rheinmetallstraße 18A
99610 Sömmerda, Germany

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.

029-S398-06

ADVANCED BIONICS
POWERFUL CONNECTIONS

029-S398-06 Rev A 2026-07-13
©2026 Advanced Bionics LLC y sus filiales.
Todos los derechos reservados.