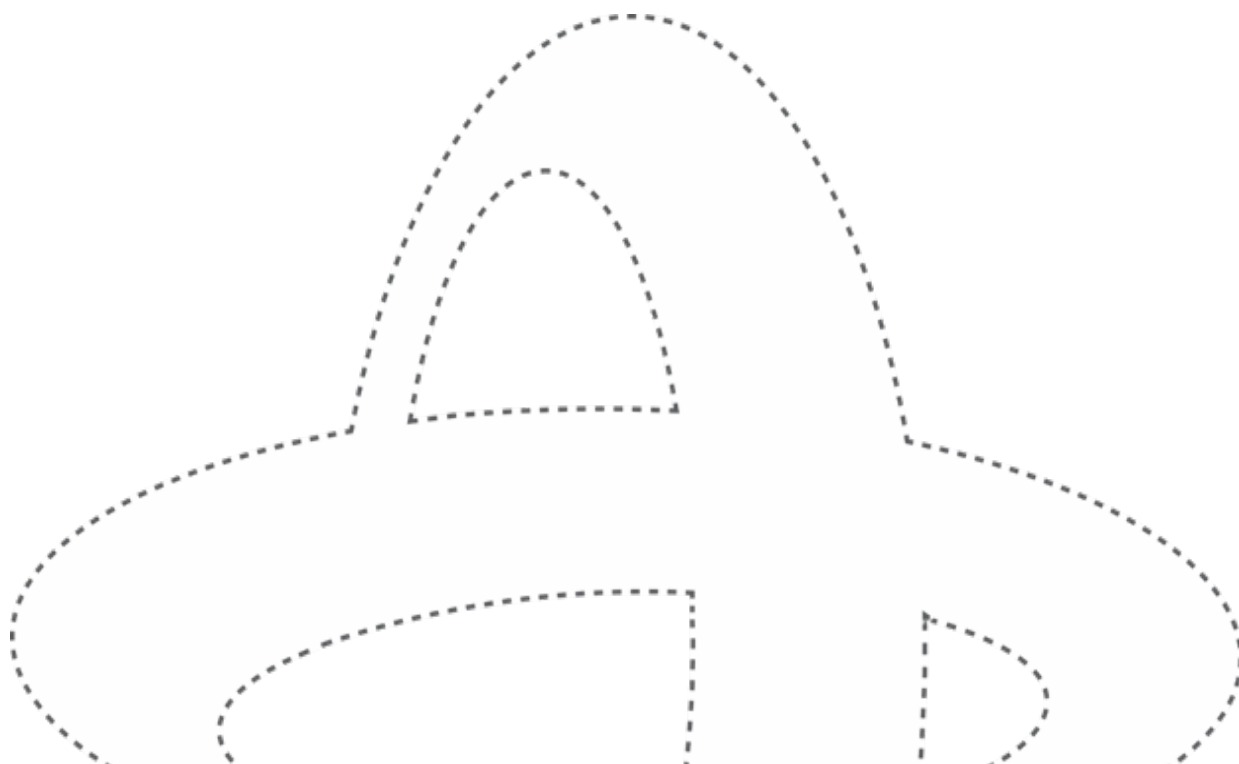




MANUAL DEL USUARIO

nCommand Lite v2.4

Versión manual: V.3



Índice

Capítulo 1	Introducción	4
Sección 1.1 -	Finalidad	4
Sección 1.2 -	Glosario	4
Sección 1.3 -	Descripción.....	5
1.3.1.	Uso previsto.....	5
1.3.2.	Indicaciones de uso.....	6
1.3.3.	Población prevista de pacientes.....	6
1.3.4.	Entorno de uso	6
1.3.5.	Contraindicaciones	6
1.3.6.	Capacidades de la plataforma.....	6
1.3.7.	Beneficios clínicos	7
1.3.8.	Usuarios previstos	7
1.3.9.	Entorno de funcionamiento	7
1.3.10.	Entorno de las instalaciones.....	8
1.3.11.	Requisitos mínimos	9
1.3.12.	Símbolos.....	10
1.3.13.	Vida útil.....	11
1.3.14.	Mejora/Actualización	11
Capítulo 2	Lista de advertencias y precauciones generales	12
Capítulo 3	Uso de la plataforma en cada ubicación	15
Sección 3.1 -	Acceso y uso de nCommand Lite.....	15
Sección 3.2 -	Acceso a la plataforma por primera vez	15
3.2.1.	Inicie sesión a través de nCommand Lite	16
3.2.2.	Iniciar sesión mediante IdP externo	17
Sección 3.3 -	Gestión de contraseñas.....	18
Sección 3.4 -	Acceso con perfil de técnico local	21
Sección 3.5 -	Acceso con perfil de técnico remoto.....	24
3.5.1.	Modo de acceso	25
3.5.2.	Barra de transmisión	28
3.5.3.	Multicámara	30
3.5.4.	Abrir otro dispositivo	32
3.5.5.	Verificación del sistema.....	34
Sección 3.6 -	Chat	36

Sección 3.7 -	Finalización de la sesión en la plataforma.....	39
Sección 3.8 -	Entrenamiento operativo	41
Sección 3.9 -	Directrices para la solución de problemas.....	42
Sección 3.10 -	Métodos de limpieza del hardware	47
Capítulo 4	Seguridad informática y privacidad	48
Sección 4.1 -	Riesgos de seguridad y privacidad.....	48
Sección 4.2 -	Protección de datos personales (cumplimiento con el RGPD/la HIPAA)	48
Sección 4.3 -	Gestión y autenticación del acceso	49
Sección 4.4 -	Control de acceso a la verificación del sistema.....	49
Sección 4.5 -	Segregación regional de datos y retención de registros	50
Sección 4.6 -	Seguridad e integridad de los datos	50
Sección 4.7 -	Respuesta ante incidentes de seguridad	50
Capítulo 5	Canales de servicio	52
Capítulo 6	Información legal y normativa.....	53
Capítulo 7	Historial de Revisiones	56
APÉNDICE I -	Lista de comprobación de inicio del servicio	57

**PRECAUCIÓN**

Las leyes federales limitan la venta de este dispositivo a médicos o por prescripción facultativa, según lo utilice un técnico médico autorizado en el estado donde ejerza.
(para los Estados Unidos de América)

**PRECAUCIÓN**

En Brasil, este software está autorizado por Anvisa para su uso exclusivo con dispositivos de resonancia magnética (RM). Queda prohibido cualquier otro uso.
(para uso en Brasil)

**PRECAUCIÓN**

Antes de usar, asegúrese de conocer los requisitos específicos de su país o región. El incumplimiento de las normativas puede conllevar riesgos para la salud.

**PRECAUCIÓN**

Asegúrese de que la versión de este manual de usuario coincida con la versión de la plataforma en uso. El uso de una versión no coincidente puede dar lugar a un funcionamiento incorrecto o a una interpretación incorrecta de las funciones.

Capítulo 1 Introducción

Sección 1.1 - Finalidad

Este manual tiene como objetivo proporcionar a los técnicos locales y remotos una comprensión completa de las funcionalidades específicas del Sistema nCommand Lite. Este documento, que sirve como manual de usuario, proporciona información concisa y práctica, guiando a los usuarios a través de las funcionalidades del sistema y la solución de problemas. Al seguir este manual, los usuarios podrán utilizar nCommand Lite de manera eficiente, lo que ayudará a maximizar la productividad y a reducir la dependencia del servicio técnico.

Sección 1.2 - Glosario

**PRECAUCIÓN**

Esta etiqueta se aplica a condiciones o acciones que puedan suponer un peligro. Ignorar estas instrucciones puede conllevar sufrir lesiones leves o daños materiales.

**¡ADVERTENCIA!**

Esta etiqueta identifica condiciones o acciones que conllevan un peligro específico. Ignorar estas instrucciones, puede causar lesiones personales graves o daños materiales importantes.

Términos de la plataforma	Términos correspondientes
Instalaciones de diagnóstico por radiografía	Instalaciones clínicas, unidad, unidades móviles, centro de salud, unidad de atención médica
Centro remoto	Estación de trabajo remota, Lugar remoto, Oficina remota, Ubicación remota, Centro de comando
Plataforma	Aplicación web nCommand Lite
Sistema	nCommand Lite con todos los subsistemas
Dispositivo	Escáner médico, Escáner, Equipo, Dispositivo médico, Dispositivo de imágenes, Equipo de imágenes
Técnico local	Usuario local, Técnico local, Profesional sanitario local (LHP), Usuario presencial

Sección 1.3 - Descripción

El Sistema nCommand Lite es un SaMD (Software as Medical Device o software proporcionado como dispositivo médico) dirigido al cliente, que proporciona acceso remoto a través de una aplicación web para ver/revisar imágenes, así como la capacidad de proporcionar de forma remota orientación a tiempo real al técnico autorizado (usuario local) en entornos cercanos al paciente que utilice los dispositivos de obtención de imágenes médicas en el contexto de la formación o evaluación de procedimientos, para escáneres de RM, TC y TEP/TC.

Los usuarios remotos son técnicos autorizados que pueden acceder a un dispositivo de radiografía médica desde un ordenador que cumpla las especificaciones mínimas requeridas localizado en cualquier lugar mediante una conexión de software segura que transmita vídeo y sea accesible mediante un teclado y un ratón. Esto permite a los usuarios remotos ayudar a los usuarios locales sin que la distancia sea una limitación. Este acceso debe ser concedido por el usuario local que utilice el sistema, y también puede ser revocado en cualquier momento por el usuario local, lo que le permite mantener un control completo de la sesión en todo momento. Además, cada sesión remota se controla a través de unas credenciales seguras gestionadas por el usuario local. Las conexiones a un producto sanitario están limitadas a una sesión remota cada vez con el fin de mantener un control estricto sobre quién interactúa remotamente con el sistema. Las imágenes revisadas remotamente no son para uso diagnóstico.

El sistema nCommand Lite consta de una solución de instalación basada en hardware y software informáticos que admite varias sesiones, lo que permite a los técnicos remotos acceder a varios dispositivos de obtención de imágenes médicas, según sea necesario. Los escáneres compatibles con el sistema nCommand Lite cumplen con un protocolo común, lo que permite la gestión de parámetros de escaneado y el escaneado remoto.

1.3.1. Uso previsto

El sistema nCommand Lite proporciona acceso remoto para ver/revisar imágenes, así como la capacidad de proporcionar de forma remota orientación a tiempo real al técnico autorizado que utilice el escáner. Esta orientación incluye formación, evaluación de procedimientos y gestión de parámetros de exploración.

1.3.2. Indicaciones de uso

El sistema nCommand Lite permite el acceso remoto para ver/revisar imágenes, así como la capacidad de proporcionar de forma remota orientación a tiempo real al técnico autorizado que utilice un escáner de RM, TC o TEP/TC compatible. Este acceso debe concederlo el técnico local autorizado que esté utilizando el sistema. El acceso remoto solo está disponible para sistemas que admitan la capacidad de conectividad remota. Las imágenes revisadas remotamente no son para uso diagnóstico.

1.3.3. Población prevista de pacientes

Para cualquier paciente al que se le haya prescrito someterse a estudios de imagen a través de un dispositivo médico de radiografía conectado.

1.3.4. Entorno de uso

Centros de diagnóstico por imagen que realicen exploraciones por resonancia magnética (RM), tomografía computarizada (TC) y tomografía por emisión de positrones – tomografía computarizada (TEP/TC) y centros de control remotos.

1.3.5. Contraindicaciones

La plataforma no debe ser utilizada por usuarios que no sean técnicos autorizados y que no hayan recibido formación en el uso de nCommand Lite.

1.3.6. Capacidades de la plataforma

- **Exploración remota:** muestra la pantalla del dispositivo médico de radiografía a tiempo real, lo que permite a un técnico autorizado remoto asistir a una examinación.
- **Chat:** permite la comunicación entre los técnicos autorizados remotos y locales a través de mensajes de texto y voz. Los técnicos locales y remotos también pueden realizar y recibir llamadas de voz y vídeo.
- **Multicámara:** facilita la observación remota de los pacientes y del centro médico durante el procedimiento. El técnico remoto puede acceder a la vista de las cámaras a través de las pestañas, que se dividen entre las pestañas de todas las cámaras y las individuales. Este mecanismo reproduce la supervisión visual que tendría un profesional sanitario si se situara cerca del paciente, introduciendo así un nivel de seguridad superior.
- **La exploración remota multisesión** permite al técnico remoto acceder a varios dispositivos médicos de radiografía según sea necesario.
- **Modo de acceso:** permite al técnico remoto elegir entre las vistas o controlar el dispositivo. En el modo Vista, los técnicos remotos solo pueden ver lo que se está transmitiendo. En el modo de Control, el técnico tiene control sobre el ratón y el teclado.
- **Gestionar el acceso de los técnicos remotos:** permite al técnico local controlar el acceso de los técnicos remotos y su modo de acceso (Vista o Control). Para permitir la conexión del técnico remoto, el técnico local debe conceder el acceso mediante la plataforma; este también puede ser revocado en cualquier momento por el técnico local, lo que le permite mantener un control completo de la sesión en todo momento.
- **Tamaño de transmisión:** el técnico remoto puede ver el tamaño de transmisión original y el tamaño de transmisión actual en píxeles. También se le notifica cuando el tamaño de transmisión actual es menor que el original.
- **Estado del ratón y del teclado:** el técnico remoto obtiene feedback sobre si el ratón y el teclado del dispositivo médico de radiografía funcionan correctamente.

- **Detalles de la sesión:** los técnicos locales y remotos pueden acceder a los detalles de la sesión.

1.3.7. Beneficios clínicos

nCommand Lite mejora la obtención de imágenes diagnósticas al permitir el funcionamiento remoto de los sistemas de **RM, TC y TEP-TC**, lo que garantiza una calidad de imagen uniforme y el cumplimiento de los protocolos. Permite a los técnicos experimentados supervisar y ayudar con las exploraciones a tiempo real, optimizando la eficiencia del flujo de trabajo y reduciendo los errores que podrían afectar a la precisión del diagnóstico. El sistema facilita la colaboración entre los técnicos, mejorando la coherencia de los exámenes y permitiendo una toma de decisiones más rápida en casos complejos. Al permitir a los profesionales remotos prestar asistencia a múltiples centros, **nCommand Lite** aumenta la **disponibilidad, la variedad y la calidad** de los exámenes de imágenes, lo que garantiza que más pacientes tengan acceso a diagnósticos avanzados, a la vez que optimiza los recursos sanitarios. Además, ayuda a mitigar la escasez de personal al reducir la dependencia de especialistas in situ, todo ello manteniendo el cumplimiento de estrictas normas reglamentarias y de seguridad de los datos.

1.3.8. Usuarios previstos

- **Técnico local**

El técnico local es el usuario del centro responsable de ayudar y guiar a los pacientes presenciales en el centro médico. Debe tener los conocimientos necesarios para realizar procedimientos de exploración con un dispositivo médico de radiografía determinado. Además, controla el modo de acceso del técnico remoto (Vista o Control) y el técnico local debe conceder el acceso remoto a través de la plataforma, pudiendo revocarlo en cualquier momento.

- **Técnico remoto**

Un profesional que realiza operaciones remotamente, con acceso y control del ordenador del producto. Al igual que el técnico local, el técnico remoto también debe tener los conocimientos necesarios para realizar procedimientos de exploración para un dispositivo de obtención de imágenes determinado.

- **Usuario de servicio técnico/TI**

Profesional responsable de configurar la plataforma (no incluido en este manual de usuario).

1.3.9. Entorno de funcionamiento

Las siguientes especificaciones se refieren a los requisitos ambientales del ordenador e-KVM.

- **Altitud máxima (sin presurización)**

- Funcionamiento: De 0 m (0 pies) a 3048 m (10 000 pies)
- Almacenamiento: De 0 m (0 pies) a 12 192 m (40 000 pies)

- **Temperatura**

- Funcionamiento: De 10°C (50°F) a 35°C (95°F)
- Almacenamiento: De -10°C (14°F) a 50°C (122°F)

- **Humedad relativa**
 - Funcionamiento: 20%-80% (sin condensación)
 - Almacenamiento: 10%-90% (sin condensación)

1.3.10. Entorno de las instalaciones

La plataforma nCommand Lite tiene dos tipos de localización de entorno diferentes:

- **Instalación de imágenes:** Centros que realizan exploraciones por resonancia magnética (RM), tomografía computarizada (TC) o tomografía por emisión de positrones – tomografía computarizada (TEP/TC).
- **Instalación remota:** Un lugar donde los técnicos remotos pueden acceder y administrar dispositivos de forma remota (escáneres de resonancia magnética, tomografía computarizada o tomografía por emisión de positrones / tomografía computarizada). Esta estación de trabajo se puede utilizar en varios entornos, como oficinas, centros de comando, ubicaciones remotas o incluso ubicaciones secundarias dentro del centro de atención médica. La estación de trabajo remota se puede ubicar en cualquier espacio que proporcione al usuario las condiciones adecuadas de concentración y conectividad mínima, y los requisitos de configuración del ordenador.

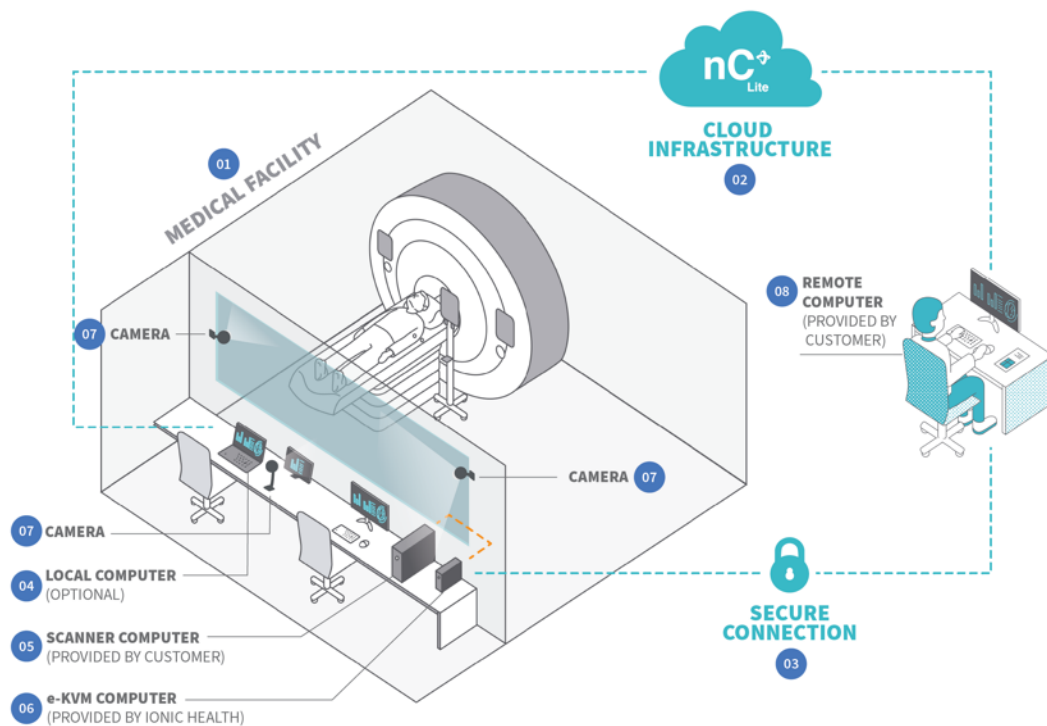


Figura 01: Descripción general del producto y sus conexiones a través de una conexión segura (p. ej., VPN).

01 – Centro médico; **02** – Infraestructura en la nube; **03** – Conexión segura; **04** – Ordenador local (accesorio opcional);
05 – Ordenador del escáner (suministrado por el cliente); **06** – e-KVM (suministrado por IONIC Health);
07 – Cámara; **08** - Ordenador remoto (proporcionado por el cliente)

**¡ADVERTENCIA!****Compatibilidad con escaneo remoto**

IONIC Health (IH) valida la funcionalidad de escaneo remoto en los dispositivos compatibles enumerados. IH realiza una evaluación completa de los requisitos de escaneo remoto de IH y prueba el sistema en el entorno de destino durante la instalación. Esto garantiza la compatibilidad y el rendimiento adecuado en ese momento para el escaneo remoto. Esta verificación no implica que se cumplan todos los requisitos de dispositivos OEM (de un fabricante de equipos originales) en esta configuración. Cualquier desviación de los requisitos de un dispositivo OEM es responsabilidad del usuario final.

Las modificaciones en el sistema o entorno después de la instalación deben informarse a IH para verificar la continuidad de la compatibilidad. IH no puede garantizar el rendimiento ni asumir la responsabilidad de configuraciones diferentes a las validadas durante la instalación.

1.3.11. Requisitos mínimos

- **Ordenador local**

Este ordenador es utilizado por el **técnico local** para autorizar y dar soporte al acceso remoto del dispositivo a través de nCommand Lite®. También permite la comunicación directa con el **técnico remoto** a través de la función de chat en la plataforma.

Las especificaciones técnicas mínimas requeridas son las siguientes:

- Procesador: AMD® A4-9120C o superior, o similar
- Memoria: 4 GB o superior
- Almacenamiento: SSD de 128 GB o superior
- Periféricos: micrófono y altavoz, o auriculares y cámara web.
- Monitor: 14" FHD (1920 x 1080) o superior
- Sistema operativo: SO Chrome, SO Windows o SO MAC
- Lugar de instalación: este ordenador debe estar cerca del ordenador del escáner
- Rutina de TI: crear un acceso directo a nCommand Lite en el escritorio de cada usuario
- Compatibilidad del navegador: Google Chrome o Microsoft Edge.

- **Estación de trabajo remota**

Esta estación es utilizada por el **técnico remoto** para acceder y controlar el dispositivo a través de nCommand Lite®. La estación de trabajo remota debe establecer una conexión segura con el ordenador e-KVM (proporcionado por IONIC HEALTH®).

El cliente es responsable de proporcionar el Equipo Remoto y decidirá sobre uno de dos escenarios siguientes: el primero es una operación 24x7 y el segundo es una operación en horario comercial.

A continuación encontrará las especificaciones adecuadas para cada escenario para elegir los modelos de ordenador:

Escenario 1 (funcionamiento 24x7): debe cumplir las siguientes especificaciones:

- Intel Xeon W-2223 (4 núcleos, 8 hilos, 8,25 MB de caché, 3,90 GHz Turbo) o superior.
- RAM: 16 GB o superior.
- Gráficos: NVIDIA RTX A2000 6 GB o superior, o similar.
- Almacenamiento: SSD de 128 GB o más.
- Sistema operativo: Windows 11 Pro 64B o superior.
- Requisitos mínimos del monitor: Tamaño 27", relación de aspecto 16:9, Resolución 4k.
- Auriculares: BLACKWIRE 3200 o similares.
- Compatibilidad del navegador: Google Chrome o Microsoft Edge.

Escenario 2 (funcionamiento en horario laboral): debe cumplir con las siguientes especificaciones:

- Intel® Core™ i7-12700k vPro® o superior.
- RAM: 16 GB o superior.
- Gráficos: NVIDIA T400 GB o superior, o similar.
- Almacenamiento: SSD de 128 GB o más.
- Sistema operativo: Windows 11 Pro 64B o superior.
- Requisitos mínimos del monitor: Tamaño 27", relación de aspecto 16:9, Resolución 4k.
- Auriculares: BLACKWIRE 3200 o similares.
- Compatibilidad del navegador: Google Chrome o Microsoft Edge.

**¡ADVERTENCIA!**

No cumplir con la configuración y los requisitos mínimos adecuados puede provocar una comunicación degradada o fallida entre los usuarios.

- **Configuraciones de red (requisitos mínimos)**

Para establecer la sesión entre el usuario remoto y el ordenador de e-KVM, debe asegurarse la comunicación de red entre ambos dispositivos. El sistema nCommand Lite utiliza peer-to-peer (P2P) para establecer la conexión entre el usuario local, el usuario remoto y el ordenador de e-KVM. Hay tres escenarios compatibles:

- **Escenario 1:** red corporativa que usa uno de los siguientes protocolos: LAN, LAN a LAN, MPLS o VPN;
- **Escenario 2:** red corporativa que utiliza WAN (red externa) de confianza y no utiliza ninguno de los siguientes protocolos: LAN, LAN a LAN, MPLS o VPN;
- **Escenario 3:** red pública del lado del equipo remoto (usuario remoto).

Las configuraciones para cada escenario se detallan en la documentación técnica.

1.3.12. Símbolos

Símbolo	Descripción	Referencia
	Fabricante	ISO 15223-1, ISO 7000-3082
	Fecha de fabricación	ISO 15223-1, ISO 7000-2497

	El símbolo indica que este producto es un producto sanitario	ISO 15223-1
	Identificador único del dispositivo	ISO 15223-1
	Referencia del modelo	ISO 15223-1, ISO 7000-2493
	Importador	ISO 15223-1, ISO 7000-3725
	Consulte el manual del usuario	ISO 15223-1, ISO 7000-1641
	Distribuidor	ISO 15223-1, ISO 7000-3724
	Precaución	ISO 15223-1, ISO 7000-0434A
	Advertencia	ISO 7010-W001
	Número de serie <i>(o versión de software)</i>	ISO 15223-1, ISO 7000-2498
	Representante autorizado en la Comunidad Europea	ISO 15223-1
	Representante autorizado en Suiza (CH-REP)	ISO 15223-1
	CE - Marcado de conformidad europeo; 2803 - Designación del organismo notificado	Reglamento de la UE 2017/745

1.3.13. Vida útil

La vida útil prevista del producto es de 5 años, teniendo en cuenta la vida útil de los componentes que componen el producto. Esta evaluación exhaustiva garantiza que la vida útil de cada componente crítico se alinee con la vida útil general, asegurando un rendimiento y una fiabilidad constantes durante toda la duración prevista del producto.

1.3.14. Mejora/Actualización

IONIC Health actualizará el sistema nCommand Lite como parte del mantenimiento planificado o de las versiones de actualización. Estas actualizaciones están diseñadas para garantizar el rendimiento y la fiabilidad continuos sin interrumpir la versión actualmente implementada en los sitios del cliente. Dependiendo de la naturaleza de la actualización, el producto puede actualizarse de forma remota o puede requerir una visita in situ por parte de un ingeniero de campo.

Capítulo 2 Lista de advertencias y precauciones generales



¡ADVERTENCIA!

Lea todas las advertencias siguientes antes de utilizar el Sistema nCommand Lite.



PRECAUCIÓN

El sistema nCommand Lite no puede someterse a reparación ni mantenimiento mientras se utiliza para controlar un equipo de resonancia magnética, tomografía computarizada o PET-CT en presencia de un paciente.

- Preste mucha atención a todos los avisos del sistema, ya que son cruciales para un funcionamiento seguro.
- Dé prioridad a la seguridad y la atención durante todas las operaciones.
- Las leyes federales limitan la venta de este dispositivo por parte de médicos o por prescripción facultativa, según costumbre de los técnicos médicos autorizados en el estado donde ejerzan.
- El Sistema nCommand Lite solo deben utilizarlo técnicos que hayan recibido formación sobre el uso de la plataforma.
- Utilice este sistema solo con navegadores web compatibles. Los navegadores compatibles son Google Chrome y Microsoft Edge.
- En caso de contingencia, un técnico cualificado y autorizado debe permanecer en el Centro de Diagnóstico por Imagen para realizar la operación de RM, TC o TEP/TC sin el nCommand Lite.
- El acceso simultáneo a varios dispositivos exige una gran concentración y comunicación con los equipos locales.
- Evite acceder al mismo tiempo a dispositivos con diseños idénticos o a exploraciones de la misma región anatómica.
- Puede ver varias pantallas, pero el control se limita a un solo dispositivo al mismo tiempo.
- Inicie siempre el chat mientras esté conectado a un dispositivo para mantener una comunicación clara.
- Los avisos de llamadas aparecen en la pantalla del dispositivo asociado; solo puede haber una llamada activa al mismo tiempo.
- Pruebe la comunicación de vídeo al acceder a la aplicación (antes del inicio de una sesión de trabajo) para comprobar si hay algún fallo en la conexión de salida de vídeo de los dispositivos de RM, TC o TEP/TC o cualquier dispositivo relacionado con la transmisión de vídeo.
- El dispositivo no debe enchufarse a la toma de corriente ni a la fuente de alimentación ininterrumpible y estabilizada a través de cables alargadores o regletas de enchufes.
- Si se producen fallos de vídeo, compruebe la conexión de vídeo entre el sistema del dispositivo y el ordenador e-KVM.
- Si la aplicación tiene un acceso remoto lento, actualice la página con el comando Ctrl+F5 en el navegador del ordenador del técnico remoto. Si el problema persiste, póngase en contacto con el servicio técnico.
- Siempre que se actualiza la página del navegador, también se interrumpe la conexión con el dispositivo, con lo que es necesario volver a realizar el proceso de aprobación.

- No inicie sesión con un navegador diferente cuando ya haya iniciado sesión.
- La instalación de diagnóstico por imagen del cliente debe tener un enlace redundante a Internet con un proveedor diferente del principal, para poder realizar un cambio inmediato en caso de pérdida de comunicación entre el sistema y la plataforma.
- En caso de pérdida de comunicación o de lentitud del ratón, realice una «resincronización del ratón» en la página utilizada en el navegador.
- Asegúrese de que los ordenadores utilizados para el control del Sistema nCommand Lite, tanto en el centro de imagen como en el centro de mando, cumplan los requisitos mínimos; de lo contrario, podría producirse una pérdida del rendimiento de la aplicación.
- Debe aplicarse QoS (calidad de servicio) al enlace principal y al enlace redundante para la transmisión de la plataforma, y debe supervisarse el rendimiento del enlace.
- Antes del uso, compruebe los niveles de volumen de audio y micrófono, así como el permiso de audio y micrófono en el navegador web.
- Antes del uso, compruebe el funcionamiento del teclado y el ratón; si son lentos o no están sincronizados, active el botón de «resincronización del ratón». Compruebe si el ordenador e-KVM está conectado y encendido.
- Asegúrese de que la disposición del teclado en el centro remoto sea idéntica a la disposición del teclado en el centro de imágenes.
- Si es necesario cambiar el lugar donde se utiliza la plataforma, el cliente debe llamar al servicio técnico para realizar una nueva instalación. No vuelva a instalar sin ponerse en contacto con el servicio técnico.
- Antes de iniciar el proceso de acceso remoto del dispositivo de RM, TC o TEP/TC, es importante que los equipos técnicos comprueben todos los elementos necesarios para el correcto funcionamiento de la plataforma, para no obstaculizar la examinación. Estos elementos se enumeran en el documento «Lista de comprobación de inicio del servicio».
- La configuración del firewall del centro de imagenología debe comprobarse mensualmente con el equipo de TI, verificando que no haya problemas con la versión del firewall que puedan comprometer el uso del nCommand Lite.
- Cualquier anomalía observada en el uso de la aplicación debe notificarse inmediatamente al equipo de servicio técnico antes de iniciar el acceso o cancelarlo si ya se ha iniciado.
- La aplicación solamente deben utilizarla técnicos autorizados con formación en el uso de nCommand Lite.
- El acceso remoto a través de la plataforma no sustituye ni compite con ningún otro procedimiento operativo para operaciones de RM, TC o TEP/TC establecido por el fabricante del producto sanitario y los protocolos y procedimientos del centro de atención.
- Evite doblar o estirar los cables de hardware.
- Si se producen problemas con la comunicación por voz o chat, utilice la función de llamada telefónica para establecer la comunicación entre el técnico local en el centro de imágenes y el técnico remoto en el centro de mando. Siga las instrucciones descritas en el apartado «Directrices en caso de fallo» y, si es necesario, póngase en contacto con el servicio técnico para realizar la reparación.
- Si es necesario sustituir un ordenador o cualquier otro equipo que influya directamente en la instalación de nCommand Lite, active el servicio técnico, garantizando la conservación del funcionamiento del sistema.
- Solo una persona a la vez puede acceder de forma remota al dispositivo de RM, TC o TEP/TC.
- No toque ningún cable físico de vídeo mientras el ordenador del dispositivo y el Sistema nCommand Lite estén encendidos.

- Al acceder a un dispositivo adicional, se abrirá una nueva pestaña. Arrastre esta pestaña a un segundo monitor, ya que el sistema está diseñado para utilizarse con una pantalla independiente para cada dispositivo.

Cualquier incidente grave relacionado con el uso de este producto debe notificarse tanto al fabricante como a las autoridades sanitarias/autoridades competentes en el lugar de instalación del producto (*consulte más detalles en el capítulo Canales de servicio*).

Capítulo 3 Uso de la plataforma en cada ubicación

Sección 3.1 - Acceso y uso de nCommand Lite



¡ADVERTENCIA!

En caso de problemas, póngase en contacto con el servicio técnico para obtener ayuda.



¡ADVERTENCIA!

Compruebe la disposición del teclado y asegúrese de que sea idéntica en ambas ubicaciones (centro médico y centro remoto). Diferentes disposiciones del teclado pueden dificultar la experiencia del usuario.

Este capítulo le proporciona todo lo que necesita saber para acceder y comenzar a usar la plataforma nCommand Lite. Encontrará instrucciones sencillas y paso a paso para iniciar sesión, navegar por la interfaz y comprender las principales funciones. Ya sea trabajando en las instalaciones o de forma remota, esta guía le ayudará a comenzar de manera rápida y segura.

Cambio de idioma: el sistema está preconfigurado en inglés de forma predeterminada, pero puede cambiar fácilmente el idioma según sus preferencias. En la pantalla de inicio de sesión, haga clic en la esquina superior derecha donde se muestra «English (en-US)» (Inglés [inglés de los Estados Unidos de América]). Se abrirá una lista desplegable de idiomas disponibles entre los que podrá seleccionar el que prefiera.

Después de iniciar sesión, también puede cambiar el idioma haciendo clic en el idioma seleccionado actualmente en el lado derecho de la barra superior. Se abrirá una lista desplegable de idiomas disponibles para que pueda realizar su elección.

Tenga en cuenta que si cambia el idioma mientras está conectado a un dispositivo, la conexión actual terminará automáticamente y tendrá que volver a realizarla.

Al acceder a la plataforma, puede elegir su idioma preferido en la pantalla de inicio de sesión. Sin embargo, algunos mensajes que se muestran durante el proceso de inicio de sesión pueden aparecer en el idioma establecido en su navegador web, independientemente del idioma seleccionado en la plataforma. Para una experiencia coherente, recomendamos alinear la configuración de idioma de su navegador con el idioma de su plataforma preferida.

Sección 3.2 - Acceso a la plataforma por primera vez

El proceso de inicio de sesión en la plataforma se puede realizar de dos maneras: a través de nCommand Lite o a través de un proveedor de identidad externo (IdP externo). El usuario puede iniciar sesión utilizando uno de los métodos preconfigurados. Si el método configurado es el proveedor de identidades externo (IdP externo), el método nCommand Lite no funcionará y viceversa. Para iniciar sesión a través de un IdP externo, vaya directamente a **sub-item 3.2.2.**

3.2.1. Inicie sesión a través de nCommand Lite

Nota: esta sección no se aplica a los usuarios que inician sesión a través de un proveedor de identidad externo (IdP externo).

Encienda el ordenador y haga doble clic en el icono de acceso directo a nCommand Lite, que suele estar en el escritorio. También puede acceder a la URL directamente en el navegador.

Su primer acceso es un paso crucial para empezar a utilizar la plataforma de forma segura y eficiente. Esto es lo que debe saber:

1 - Correo electrónico de bienvenida: recibirá un correo electrónico con sus datos de acceso, incluyendo su correo electrónico personal asociado, una contraseña temporal y un enlace directo a la plataforma del cliente. Este correo electrónico es fundamental para iniciar su experiencia en nCommand Lite.

2 - Creación de contraseña: Tras acceder al enlace, deberá introducir su correo electrónico asociado y la contraseña recibida en el correo electrónico de bienvenida. Al hacer clic en «Sign in» (Iniciar sesión), se le redirigirá a una página para crear una nueva contraseña. Debe introducir la contraseña antigua, la nueva y la confirmación de la nueva. Debe ser robusta y segura, tener al menos 8 caracteres de longitud e incluir al menos 3 elementos de los siguientes: una letra minúscula, una letra mayúscula, un número y un símbolo. Al hacer clic en «Continue» (Continuar), se le redirigirá a una página para confirmar de nuevo su correo electrónico. Al hacer clic en «Continue» (Continuar), se le redirigirá a la pantalla de inicio, que se personaliza de acuerdo con su perfil del usuario específico.

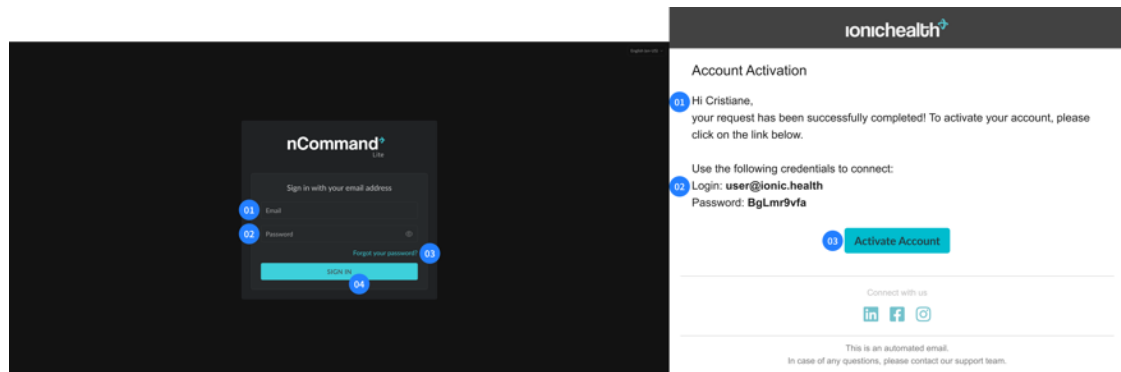


Figura 02: Primer acceso

Izquierda - Página de inicio de sesión: 01 – Dirección de correo electrónico; 02 – Password (Contraseña); 03 – “Forgot your password” (¿Ha olvidado su contraseña?); 04 – Sign In button (Botón de inicio de sesión)

Derecha - Correo electrónico de bienvenida: 01 – Texto de correo electrónico de activación de la cuenta; 02 – Credenciales de inicio de sesión; 03 – Botón Active Account (Cuenta activa)

Este procedimiento inicial está diseñado para garantizar la máxima seguridad de su cuenta desde el principio. A partir de su segundo acceso, el proceso se agilizará pero será igualmente seguro, ya que en cada inicio de sesión se enviará un código de autenticación de dos factores a su correo electrónico asociado, garantizando así la seguridad continua de su cuenta.

Después de iniciar sesión en nCommand Lite, el sistema le dirigirá automáticamente a la pantalla de inicio, que se personaliza de acuerdo con su perfil del usuario específico. Tanto si es un técnico local como si es un técnico remoto, la interfaz está diseñada para satisfacer las

necesidades y acceder a los datos relevantes para su función. Este diseño intuitivo garantiza que dispone de todas las herramientas y la información necesarias para una experiencia de usuario eficaz y eficiente desde el momento en que inicia sesión.

Nota: cuando el método de inicio de sesión está configurado como nCommand Lite, el inicio de sesión siempre debe realizarse a través de esta opción. Incluso si aparece un botón de IdP externo en la pantalla de inicio de sesión, no funcionará para estos usuarios. Cada cuenta de usuario se registra en la plataforma con un método de autenticación específico — ya sea con credenciales de nCommand Lite o mediante un servicio de IdP externo. Si un usuario intenta iniciar sesión utilizando un método diferente al asignado a su cuenta, el sistema mostrará un mensaje de error indicando que la cuenta no está autorizada para ese tipo de autenticación.

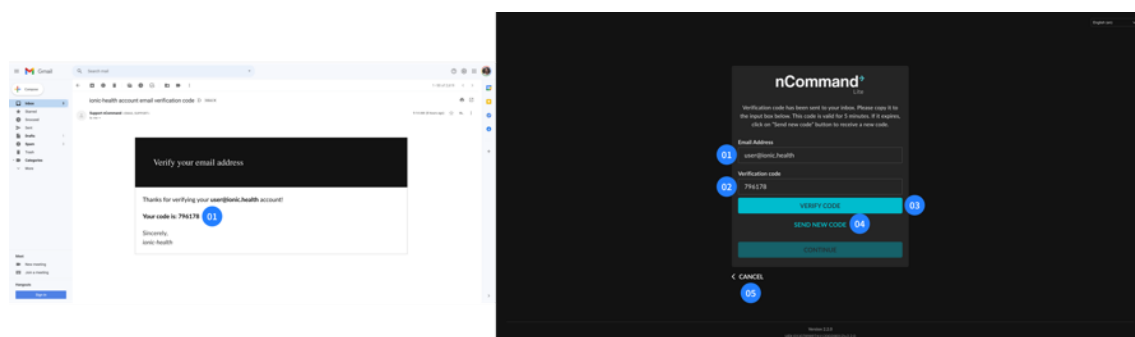


Figura 03: Autenticación de dos factores (2-FA)

Izquierda – Correo electrónico: 01 – Código de 2 -FA

Derecha - Página de autenticación de dos factores: 01 – Dirección de correo electrónico; 02 – Código de verificación;

03 – Botón de confirmación del código de verificación; 04 – Enviar nuevo código; 05 – Cancelar

3.2.2. Iniciar sesión mediante IdP externo

En algunos casos, los usuarios pueden iniciar sesión en la plataforma a través de un proveedor de identidad externo (IdP), lo que les permite utilizar el servicio de autenticación existente de su organización, un mecanismo también conocido como inicio de sesión único (SSO). Mediante este método, el usuario preregistrado no recibirá un correo electrónico de bienvenida. El servicio de TI local debe comprobar la compatibilidad, configurar el método e informar al usuario qué correo electrónico (IdP externo) debe utilizarse.

Cuando esta opción está disponible, el usuario siempre debe iniciar sesión con el IdP externo (por ejemplo, Amazon Cognito, Microsoft Entra ID, Microsoft AD B2C). El método de inicio de sesión a través de nCommand Lite no estará disponible para los usuarios de IdP externos.

Para iniciar sesión con el IdP externo, haga clic en el botón con el nombre del IdP y siga las instrucciones proporcionadas por el autenticador externo. Si su institución tiene más de un IdP externo integrado, asegúrese de confirmar con qué proveedor está registrado. Otros proveedores no funcionarán. Si tiene alguna pregunta o encuentra dificultades, póngase en contacto con su servicio informático local.

En los escenarios en los que los usuarios compartan la misma máquina y utilicen el inicio de sesión único (SSO), se recomienda que cada usuario seleccione la opción "no permanecer

conectado" durante el inicio de sesión del IdP externo (si está disponible) o que cierre la sesión del proveedor externo después de cerrar sesión en nCommand Lite.

Para esta opción de inicio de sesión, el proceso completo de inicio y cierre de sesión, incluidas las políticas de creación y vencimiento de contraseñas, la autenticación multifactor (MFA) y los bloqueos de cuentas, es administrado en su totalidad por el equipo de TI del cliente que configuró el IdP externo.

Al iniciar sesión a través de un IdP externo, las funciones "Olvidé mi contraseña" y "Cambiar contraseña" deben realizarse de acuerdo con el proceso del IdP externo.

Nota: la opción "Olvidé mi contraseña" seguirá apareciendo en la pantalla de inicio de sesión, pero no estará disponible para estos usuarios. Es posible que dirija a los siguientes pasos del proceso, pero no lo completará. Si necesita recuperar su contraseña, siga las instrucciones de su IdP externo.

Importante: incluso cuando se utiliza un IdP externo, el usuario debe estar preinscrito en la plataforma nCommand Lite para obtener acceso.

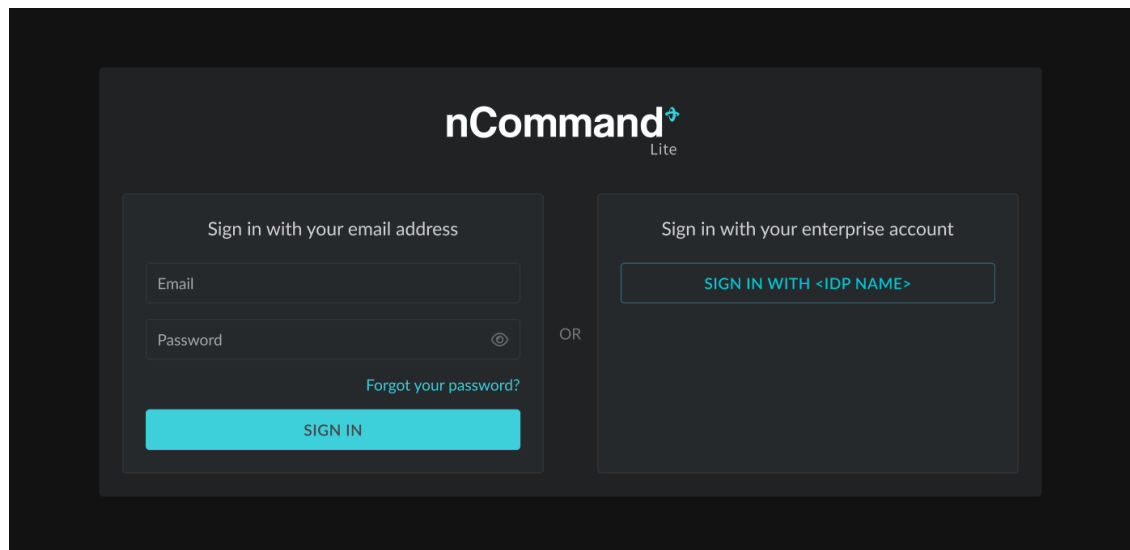


Figura 04: Ejemplo de pantalla de inicio de sesión a través de un IdP externo

Sección 3.3 - Gestión de contraseñas

Después de acceder a la plataforma por primera vez, los usuarios pueden cambiar su contraseña o, si la han olvidado, establecer una nueva contraseña.

Nota: al iniciar sesión a través de un IdP externo, las funciones **Olvidé mi contraseña** y **Cambiar contraseña** deben realizarse de acuerdo con el proceso del IdP externo.

- **Recuperar contraseña:** permite a los usuarios recuperar el acceso a la cuenta en caso de que olviden su contraseña. Simplemente haga clic en el enlace «Forgot your password?»

(¿Olvidó su contraseña?) en la página de inicio de sesión, introduzca la dirección de correo electrónico asociada y envíe la información. A continuación, el sistema enviará un correo electrónico con un código de verificación. Al rellenar el código y hacer clic en «Verify code» (Verificar código), se pedirá a los usuarios que confirmen el correo electrónico asociado. Al hacer clic en «Continue» (Continuar), los usuarios son dirigidos a una página donde pueden introducir una nueva contraseña y la confirmación de la nueva contraseña. Si la nueva contraseña cumple con los requisitos del sistema, los usuarios pueden registrarla correctamente e iniciar sesión posteriormente con las credenciales actualizadas.

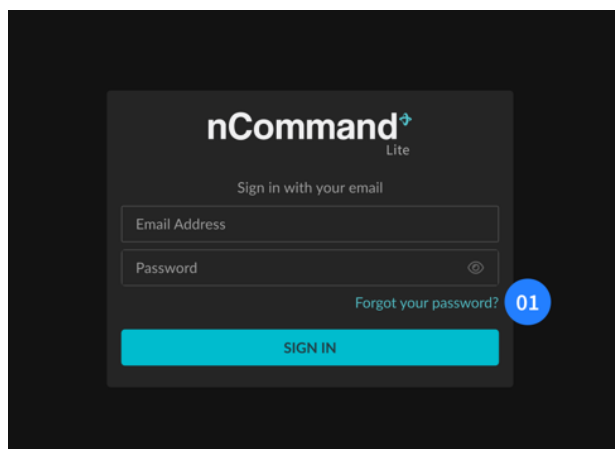


Figura 05: Enlace a la página de restablecimiento de contraseña
01 – ¿Olvidó su contraseña?

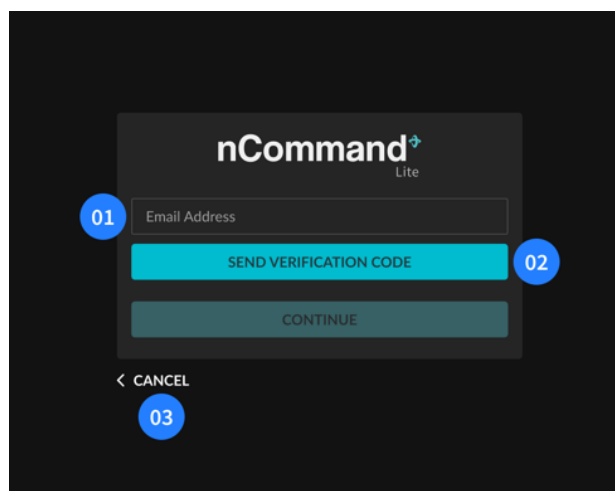


Figura 06: Página de restablecimiento de contraseña
01 – Dirección de correo electrónico; 02 – Enviar código de verificación; 03 – Cancelar

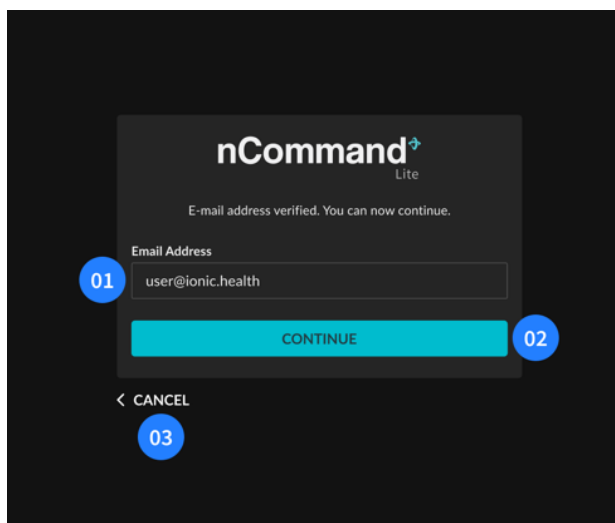


Figura 07: Confirmación de correo electrónico
01 – Dirección de correo electrónico; **02** – Botón Continuar; **03** – Cancelar

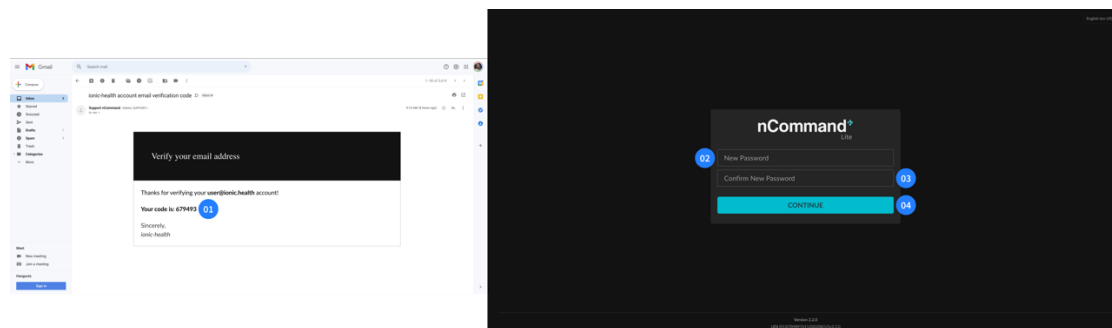
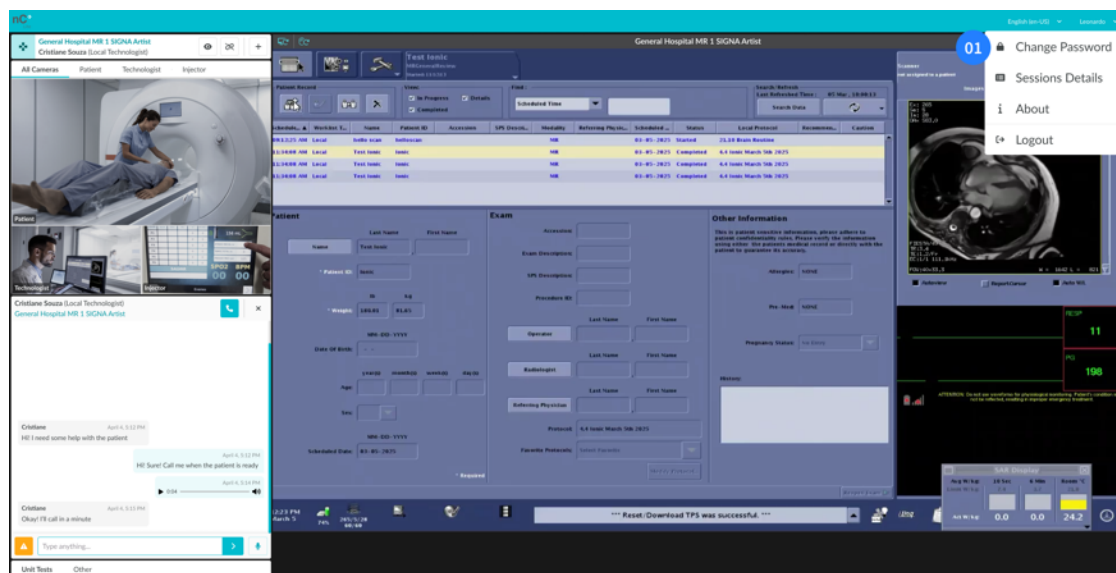
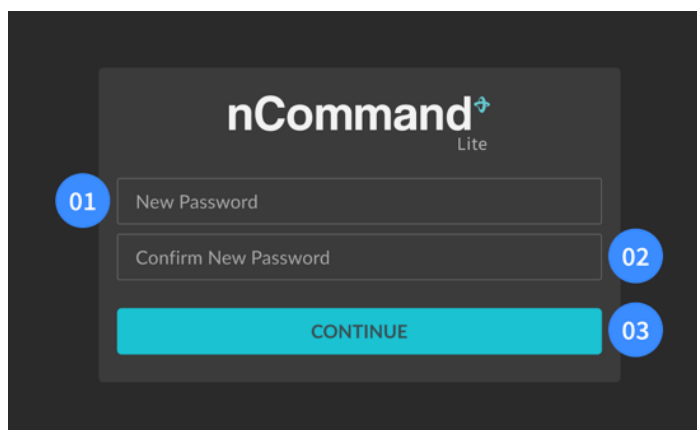


Figura 08: Correo electrónico con código para registrar nueva contraseña (izquierda) - 01 – Código de autenticación de 2 factores
Página de cambio de contraseña (derecha) - 02 – New Password (Nueva contraseña); 03 – Confirm New Password (Confirmar nueva contraseña); 04 – Botón Continue (Continuar)

- Cambiar contraseña:** permite a los usuarios actualizar su contraseña cumpliendo criterios específicos, incluidos al menos 3 elementos de los siguientes: una letra minúscula, una letra mayúscula, un número y un símbolo, y tener al menos 8 caracteres de longitud. El sistema comprueba si la nueva contraseña cumple estos criterios y avisa al usuario con un mensaje si no lo hace. Además, los usuarios deben confirmar la nueva contraseña para evitar errores de entrada. El usuario puede cambiar la contraseña después del proceso de inicio de sesión haciendo clic en el icono de la esquina superior derecha y elegir el menú «Change Password» (Cambiar contraseña). Se le desconectará de la plataforma y se le redirigirá a una página para confirmar el correo electrónico asociado. A continuación, el sistema enviará un correo electrónico con un código de verificación. Al rellenar el código y hacer clic en «Verify code» (Verificar código), se dirige a los usuarios a una pantalla en la que pueden introducir una nueva contraseña.



**Figura 09: Elemento del menú desplegable de cambio de contraseña
01 –Change Password (Cambiar contraseña)**



**Figura 10: Página de cambio de contraseña
01 – New Password (Nueva contraseña); 02 – Confirm New Password (Confirmar nueva contraseña); 03 – Botón Continue (Continuar)**

Sección 3.4 - Acceso con perfil de técnico local



¡ADVERTENCIA!

Antes de utilizar la plataforma, póngase en contacto con el técnico remoto por teléfono.



¡ADVERTENCIA!

Con el fin de evitar el sobrecalentamiento, no coloque ningún objeto delante del refrigerador de aire del ordenador e-KVM y, con el fin de evitar cualquier daño, no coloque ningún objeto encima de este.

**¡ADVERTENCIA!**

Durante las sesiones remotas, el técnico local es responsable de gestionar y aplicar las reglas de seguridad locales para cada tipo de examen y sus requisitos específicos. Permanezca siempre presente en la sala de control o en la sala de examen para garantizar la seguridad tanto del paciente como de los profesionales implicados.

**¡ADVERTENCIA!**

Los movimientos de la mesa durante la sesión solo deben ser realizados por el tecnólogo local cuando el sistema lo solicite. Antes de salir del quirófano, el técnico local debe revocar siempre el acceso del técnico remoto.

**¡ADVERTENCIA!**

Solo el técnico local tiene permitido mover la mesa para colocar al paciente dentro del dispositivo y dejarle salir de forma segura. Antes de salir del quirófano, el técnico local debe revocar siempre el acceso del usuario remoto.

Después de iniciar sesión en la plataforma, seleccione el dispositivo deseado en el cuadro Device Selection (Selección del dispositivo). Usted será responsable de este dispositivo, de forma que podrá revisar la solicitud del técnico remoto de acceso al dispositivo. Cuando un técnico remoto desee acceder al dispositivo, aparecerá una ventana emergente que le permitirá revisar toda la información presentada antes de otorgar o denegar el acceso. Manténgase alerta ante una solicitud entrante de un técnico remoto. Es de máxima importancia comprobar cuidadosamente cada detalle. En los casos en los que no se reconozca la información proporcionada, no conceda acceso.

El técnico remoto puede acceder al dispositivo utilizando uno de los dos modos de acceso: **Control o Vista:**

- **Modo Control** - permite al técnico remoto controlar el ratón y el teclado, así como ver la transmisión del dispositivo. Sin embargo, el técnico local no pierde el control del ratón y el teclado locales y puede tomar el control en cualquier momento.
- **Modo Vista** - permite al técnico remoto solo ver la pantalla del dispositivo y utilizar el chat para comunicarse

Después de seleccionar el dispositivo, el usuario tiene acceso a la función de chat, lo que permite la comunicación mediante texto, mensajes de audio, voz y videollamadas con los demás usuarios.

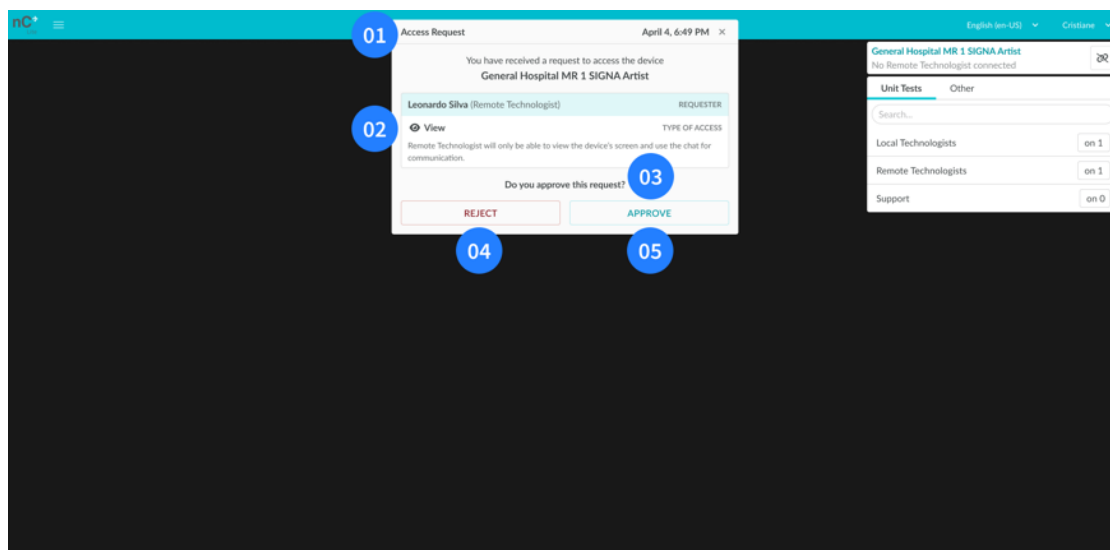


Figura 11: Pantalla principal del técnico local con notificación de solicitud de acceso

01 – Título (Access Request [Solicitud de acceso]); **02** – Nombre del solicitante, función y descripción del tipo de acceso; **03** – Indicador: «Do you approve this request?» (¿Aprueba esta solicitud?); **04** – Botón Reject (Rechazar); **05** – Botón Approve (Aprobar)

Después de la aprobación, el técnico local puede revocar el acceso del técnico remoto en cualquier momento simplemente haciendo clic en el botón REVOKE (REVOCAR).

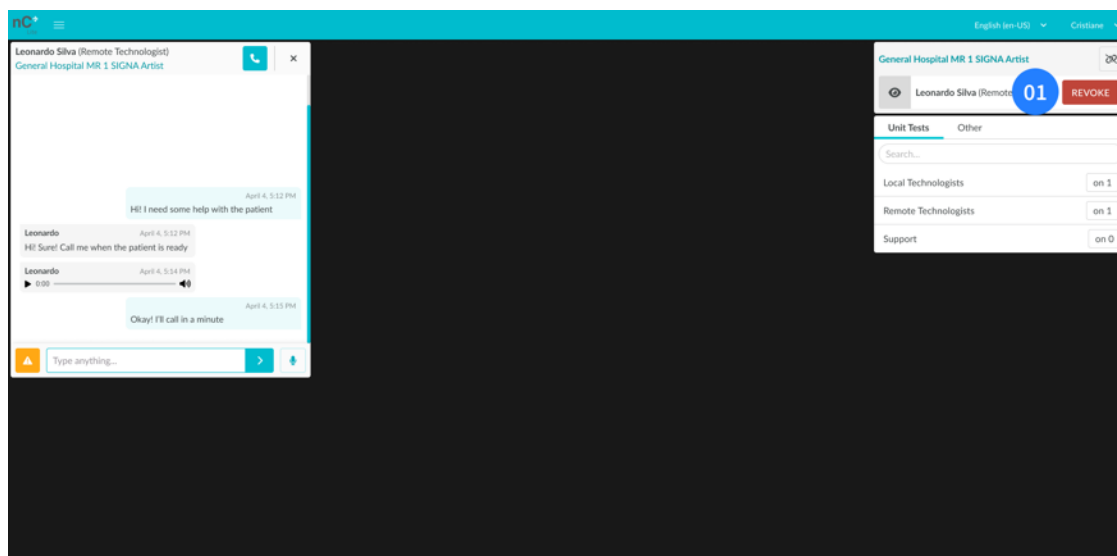


Figura 12: Pantalla principal del técnico local al conectarse a un dispositivo

01 – Botón Revoke (Revocar)

Durante la sesión remota, el técnico remoto puede solicitar un cambio del modo de acceso. Aparecerá una ventana emergente de solicitud en la pantalla. Puede aprobarla o rechazarla. Tenga en cuenta las prerrogativas que cada modo de acceso permite al técnico remoto.

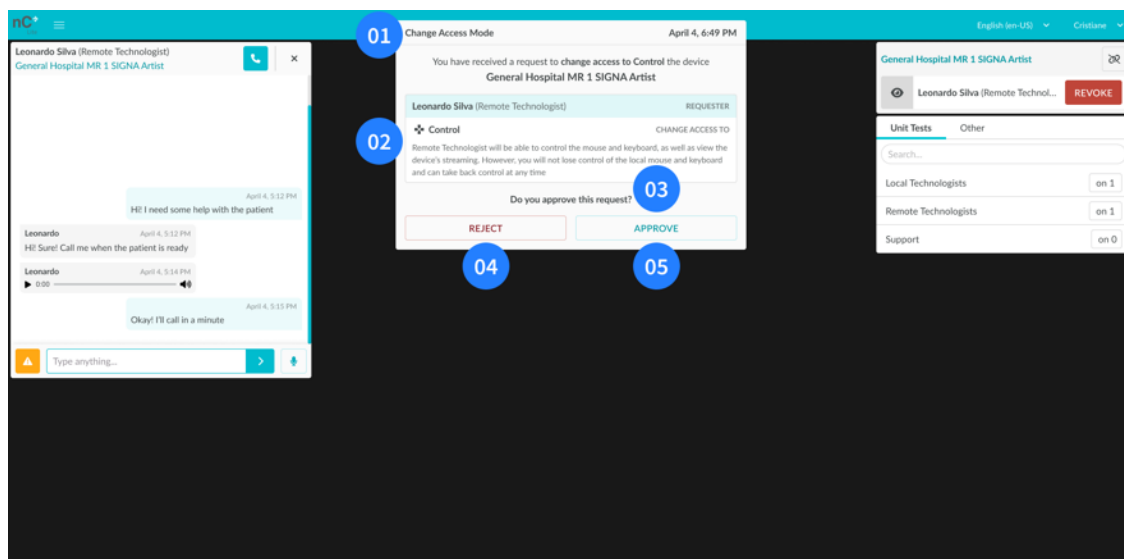


Figura 13: Pantalla principal del técnico local con solicitud para cambiar el modo de acceso

01 – Título (Change Access Mode [Cambiar el modo de acceso]); **02** – Nombre del solicitante, función y descripción del tipo de acceso; **03** – Indicador: «Do you approve this request?» (¿Aprueba esta solicitud?); **04** – Botón Reject (Rechazar); **05** – Botón Approve (Aprobar)



¡ADVERTENCIA!

En caso de que se perdiese la conexión con el ordenador local, el técnico remoto seguirá teniendo acceso al *dispositivo*. Póngase en contacto **inmediatamente** con el técnico remoto y pídale que **desconecte** O que inicie sesión en otro ordenador y que **revoque el acceso** del técnico remoto O **pulse el botón de encendido** para apagar el ordenador e-KVM.



¡ADVERTENCIA!

En caso de mantenimiento del escáner:

antes de que el ingeniero de campo inicie cualquier procedimiento (ya sea en el dispositivo o en la sala de control), informe al técnico remoto y revoque el acceso haciendo clic en el botón «REVOKE ACCESS» (REVOCAR ACCESO). A continuación, cierre la sesión en la plataforma nCommand Lite.

Si no hay ningún técnico remoto conectado, cierre la sesión en la plataforma nCommand Lite antes de iniciar el mantenimiento.

Sección 3.5 - Acceso con perfil de técnico remoto



¡ADVERTENCIA!

Nombre del usuario del ordenador del dispositivo y contraseña raíz: ambos deben ser gestionados por el responsable local que recibirá el equipo de instalación.



¡ADVERTENCIA!

Los movimientos de la mesa durante la sesión solo deben ser realizados por el tecnólogo local cuando el sistema lo solicite. Antes de salir del quirófano, el técnico local debe revocar siempre el acceso del técnico remoto.

**¡ADVERTENCIA!**

Solo el técnico local tiene permitido mover la mesa para colocar al paciente dentro del dispositivo y dejarle salir de forma segura. Antes de salir del quirófano, el técnico local debe revocar siempre el acceso del usuario remoto.

**¡ADVERTENCIA!**

Tenga siempre en cuenta la sala a través de la cámara de vídeo y asegúrese de comunicarse con el técnico local antes de realizar cualquier actividad.

**¡ADVERTENCIA!**

Si se pierde la conexión con el ordenador local, póngase en contacto de inmediato con el técnico local y desconecte.

**¡ADVERTENCIA!****En caso de mantenimiento del escáner:**

Tras recibir una notificación del inicio del mantenimiento del dispositivo, asegúrese de que el técnico local haya revocado el acceso y cierre la sesión desde la plataforma nCommand Lite. Si no se ha revocado el acceso, cierre la sesión en la plataforma nCommand Lite y póngase en contacto inmediatamente con el técnico local para notificárselo.

**¡ADVERTENCIA!**

Para controlar el ratón y el teclado de forma remota, el modo de acceso seleccionado debe ser Control; en el modo Vista, el técnico remoto solo puede visualizar cámaras locales y de transmisión.

**¡ADVERTENCIA!**

Si la respuesta a su solicitud tarda más de lo previsto, póngase en contacto con el técnico local por chat o por teléfono.

El lugar de trabajo del técnico remoto incluye equipos como un ordenador, monitores (normalmente tres), un ratón, un teclado y auriculares.

En el flujo clínico, los *técnicos locales* tienen contacto directo con el paciente. Son responsables de la interacción con el paciente, del posicionamiento y de garantizar la seguridad y el cumplimiento de los protocolos durante los procedimientos de resonancia magnética, tomografía computarizada o PET/TC, de acuerdo con los estándares institucionales y reglamentarios.

3.5.1. Modo de acceso

Después de iniciar sesión en la plataforma, seleccione el dispositivo al que desea conectarse en el cuadro Device Selection (Selección del dispositivo). Se abrirá una ventana emergente para elegir el modo de acceso entre **Control** y **Vista**:

- **Modo Control** – en este modo, el control del ratón y el teclado está habilitado además de la vista de la pantalla. Los profesionales locales mantienen el acceso completo al ratón y al teclado locales y pueden retomar el control en cualquier momento.
- **Modo Vista** – solo es posible ver la pantalla del dispositivo y utilizar el chat para comunicarse.

Al seleccionar el modo de acceso, se mostrará un cuadro con el texto «Waiting for approval» (Esperando aprobación), que indica que es necesaria la aprobación del técnico local conectado para continuar. Este técnico local tiene plena autoridad para aprobar o rechazar el acceso y

revocarlo en cualquier momento si se considera necesario. Esta medida es esencial para garantizar un control estricto y mantener la seguridad al utilizar el dispositivo.

Después de seleccionar el dispositivo, el usuario tiene acceso a la función de chat, lo que permite la comunicación a través de texto, mensajes de audio, voz y videollamada con los otros usuarios. No es necesario que el usuario esté aprobado para acceder al chat.

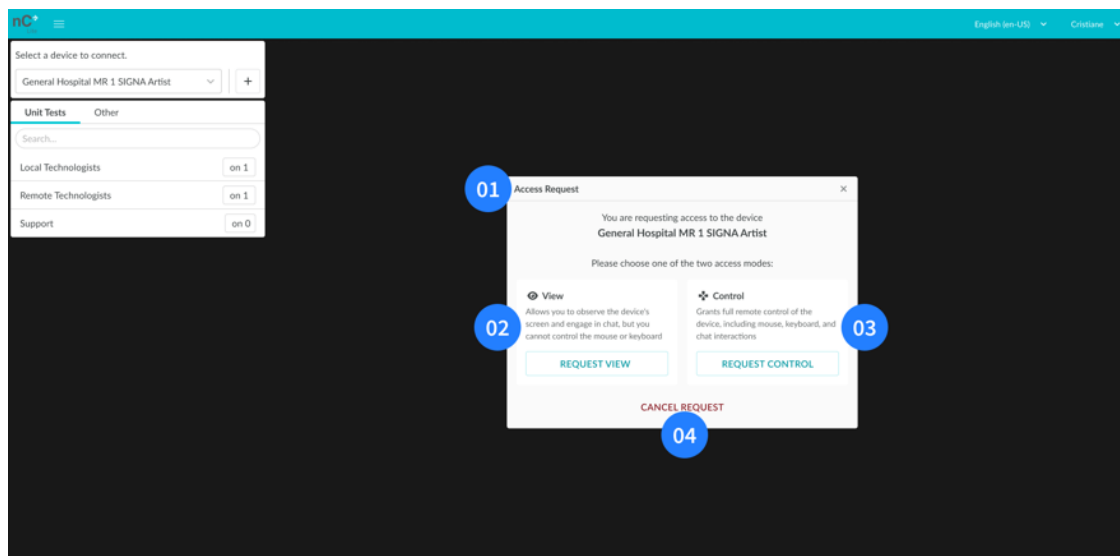


Figura 14: Diálogo de solicitud de acceso para técnicos remotos

01 – Título (Access Request [Solicitud de acceso]); **02** - Descripción del modo View (Vista) y botón Request View (Solicitar vista); **03** – Descripción del modo Control y botón Request Control (Solicitar control); **04** – Cancel Request (Cancelar solicitud)

Una vez que el técnico local haya autorizado el acceso al dispositivo, la interfaz del técnico remoto se actualizará para mostrar la transmisión en directo del dispositivo y sus cámaras asociadas. Si el modo de acceso elegido es Control, se habilitará la capacidad de funcionamiento remoto del dispositivo.

Este proceso garantiza una interacción eficaz y segura, permitiendo el uso remoto seguro del dispositivo sin comprometer su integridad ni la seguridad del paciente.

Para solicitar un cambio en el modo de acceso durante una sesión remota, haga clic en el icono correspondiente. El técnico local puede aceptar o rechazar la solicitud:

- **Aceptar** – el streaming se recargará, pero el contenido del chat no se perderá. Si está en una llamada de voz y vídeo, esta finalizará y uno de los usuarios deberá reiniciarla.
- **Decline** - aparecerá una ventana emergente notificándole el rechazo del técnico local y el acceso actual permanecerá activo

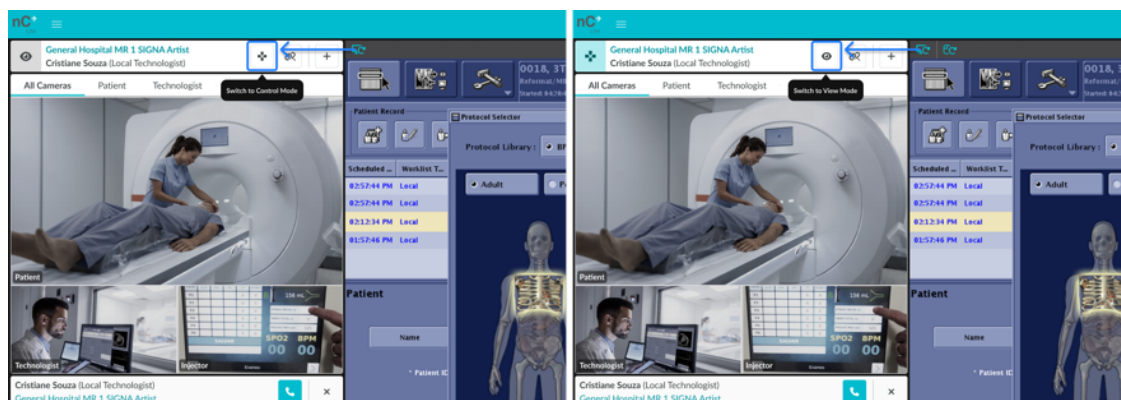


Figura 15: Cambiar modo de acceso

Izquierda - Icono de cambio al modo Control e información sobre herramientas

Derecha - Icono de cambio al modo Vista e información sobre herramientas

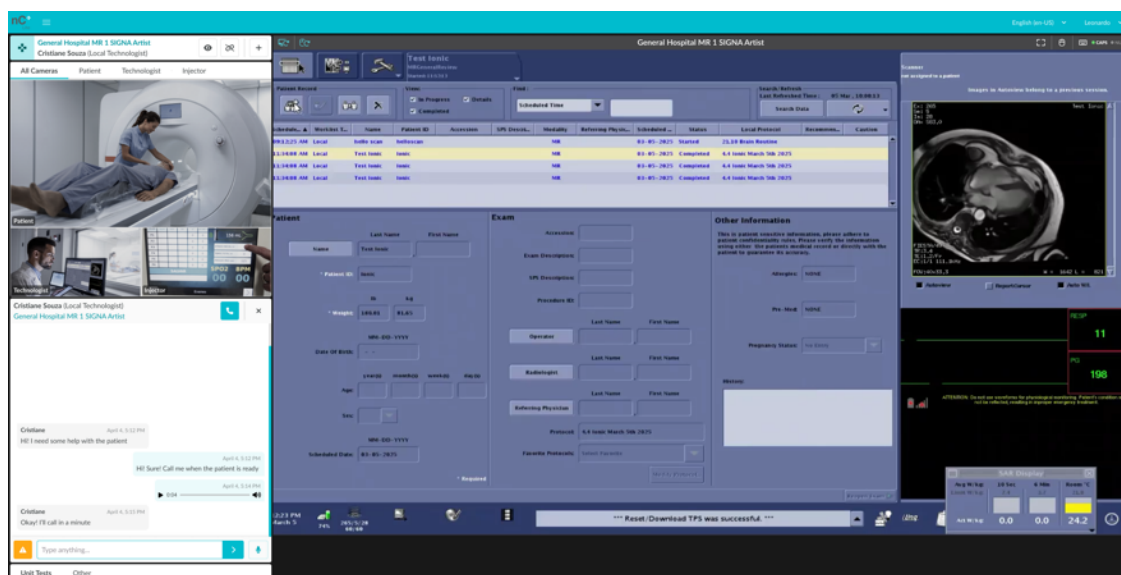


Figura 16: Pantalla principal del técnico remoto al conectarse a un dispositivo

Cuando el técnico remoto solicita acceso y no hay ningún técnico local conectado al dispositivo, la plataforma muestra una advertencia emergente. En cuanto el técnico local se conecta, la plataforma informa al técnico remoto de que puede solicitar acceso de nuevo.

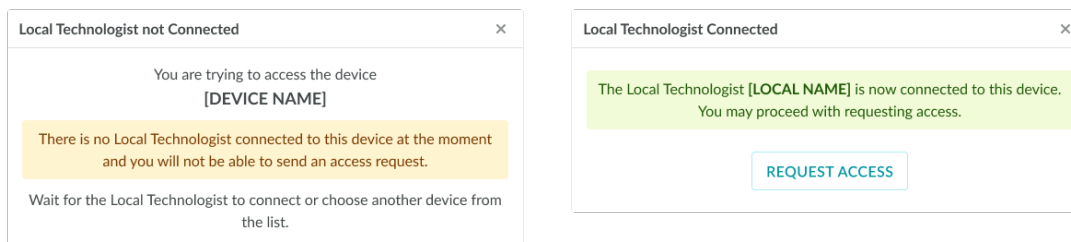


Figura 17: Advertencias del técnico remoto sobre el estado de la conexión del técnico local
Izquierda - Notificación que indica que se ha intentado acceder al dispositivo, pero actualmente no hay ningún técnico local conectado.
Derecha - Notificación que confirma que el técnico local se ha conectado al dispositivo después de no haberse conectado previamente.

3.5.2. Barra de transmisión

La barra de transmisión muestra información clave y controles relacionados con la sesión de transmisión del dispositivo. Incluye los botones "Recargar transmisión" y "Resincronización del ratón", el nombre del dispositivo, la resolución de pantalla y el estado actual del ratón y el teclado de la computadora remota.

1 - Reload Streaming (Volver a cargar streaming)

Esta función permite a los técnicos remotos recuperar el acceso a los dispositivos en caso de fallo de conexión o lentitud en el rendimiento. Si experimenta algún tipo de desconexión o retraso de pantalla en la computadora del dispositivo, puede hacer clic en el icono "Recargar transmisión" ubicado en la barra de transmisión. Esto hará que la plataforma se vuelva a conectar al ordenador del dispositivo y también recargue las cámaras del sistema.

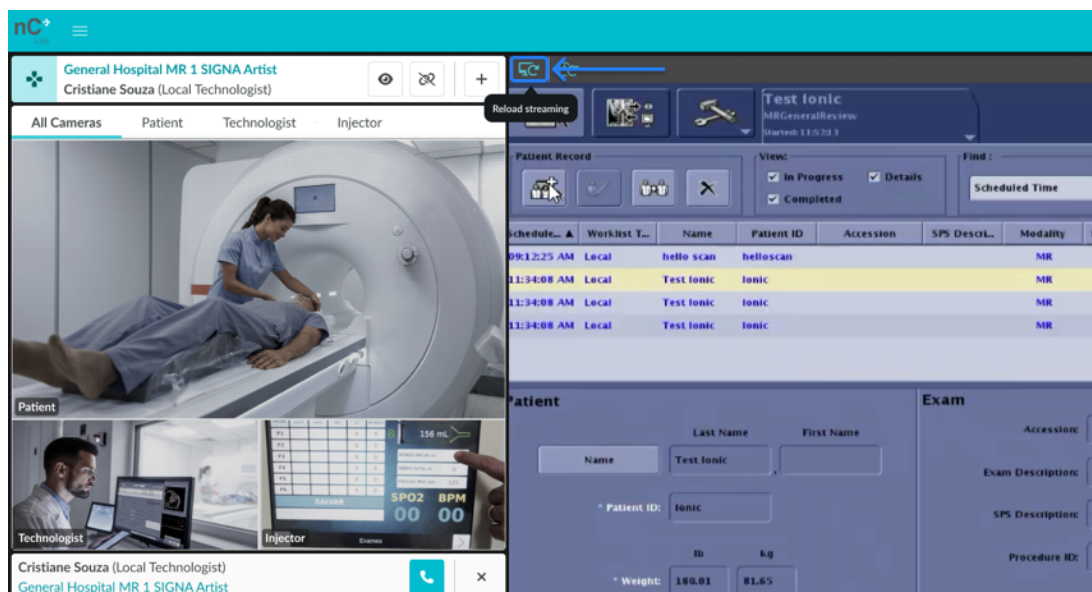


Figura 18: Botón Reload Streaming (Volver a cargar streaming)

2 - Mouse Resync (Resincronizar ratón)

Si el ratón se ralentiza o desajusta, haga clic en el botón «Mouse Resync» (Resincronizar ratón) situado en la barra encima de la ventana de transmisión para resincronizar el ratón del dispositivo con el ordenador e-KVM.

Una alternativa es mover el cursor del ratón fuera del área de transmisión y luego volver a traerlo; el sistema volverá a sincronizar automáticamente el ratón sin necesidad de ninguna otra acción. También puede hacer clic y soltar el botón de la rueda de desplazamiento del ratón (cuando esté disponible) para activar la resincronización automáticamente. Sin embargo, es posible que este método no funcione en dispositivos con dos o más pantallas si los cursores del ratón local y remoto están en pantallas diferentes.

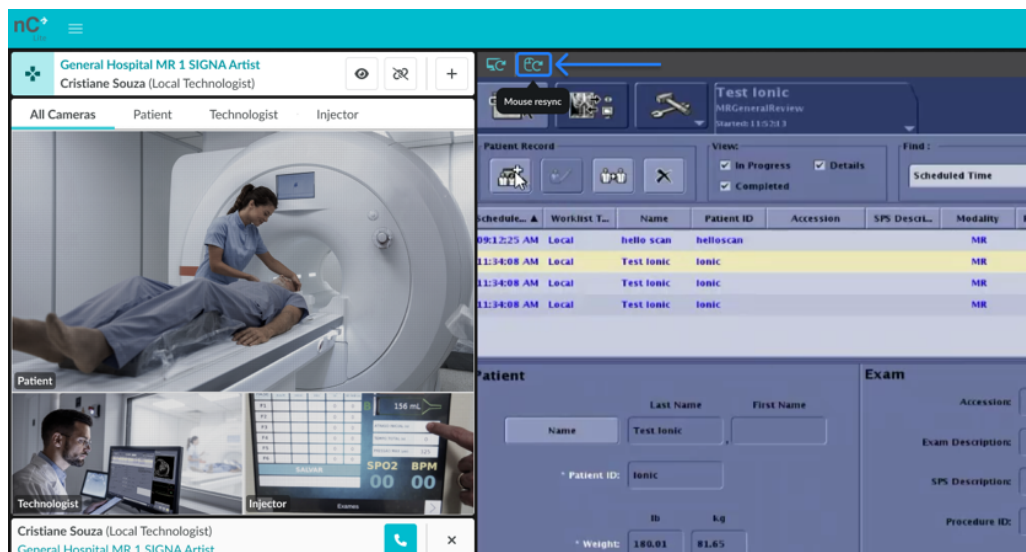


Figura 19: Botón Mouse resync (Resincronización del ratón)

3 - Pantalla de transmisión

Esta función proporciona al tecnólogo remoto información sobre la resolución de transmisión original (desde el dispositivo) y la resolución actual en píxeles que se muestra en la estación de trabajo remota.

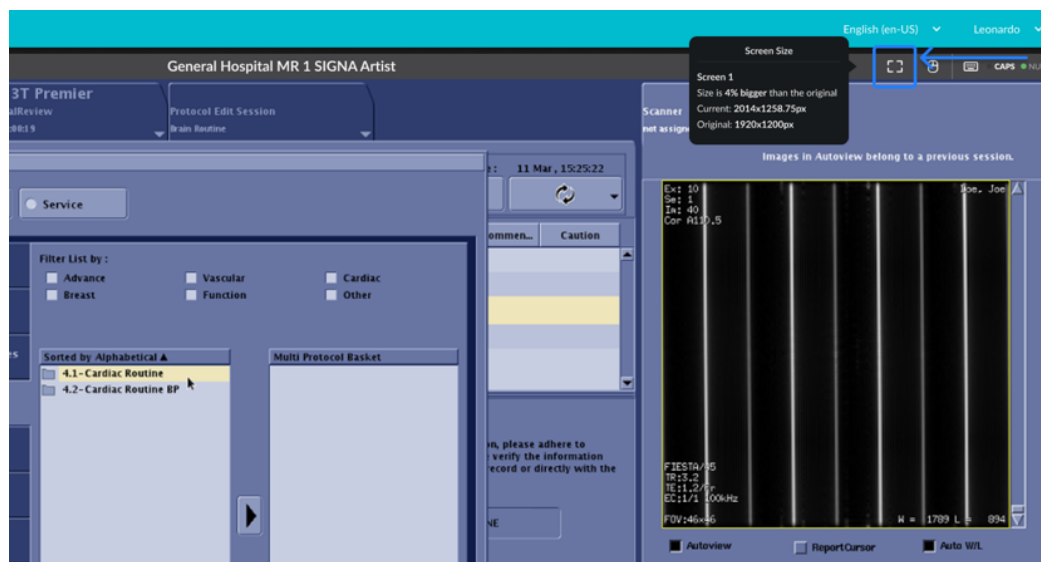


Figura 20: Mensaje emergente de información en streaming

4 - Estado del ratón y del teclado

Esta función informa al técnico remoto sobre si el ratón y el teclado funcionan correctamente. Junto con el estado del teclado, el usuario puede ver si las teclas de **bloqueo de mayúsculas** y de **bloqueo numérico** del ordenador del dispositivo están activadas o desactivadas. Sin embargo, esta funcionalidad depende del ordenador del dispositivo que proporcione esta información; en los casos en los que el sistema del dispositivo no ponga a disposición esta información, no se mostrará el estado de las teclas de **bloqueo de mayúsculas** ni **bloqueo numérico**. Los estados del ratón y del teclado se muestran solo cuando el usuario tiene el tipo de acceso de Control.

Cuando se conecta a un dispositivo, una falta de coincidencia entre los indicadores de **bloqueo de mayúsculas** y **bloqueo numérico** del ordenador remoto y el dispositivo puede provocar un comportamiento de escritura incoherente. Si los indicadores aparecen activados en el dispositivo pero no están realmente activos en el ordenador remoto, el usuario puede escribir en mayúsculas en el dispositivo mientras el texto aparece en minúsculas en el chat, o viceversa. De forma similar, si el **bloqueo de mayúsculas** está activado en el ordenador remoto pero desactivado en el dispositivo, se producirá el mismo problema de forma invertida.

Para evitar este problema, asegúrese de que el **bloqueo de mayúsculas** y el **bloqueo numérico** estén activados o desactivados antes de iniciar sesión en el dispositivo. Si se produce una discrepancia, el usuario debe desconectarse del dispositivo, ajustar el estado de la tecla en el ordenador remoto y, a continuación, volver a conectar.

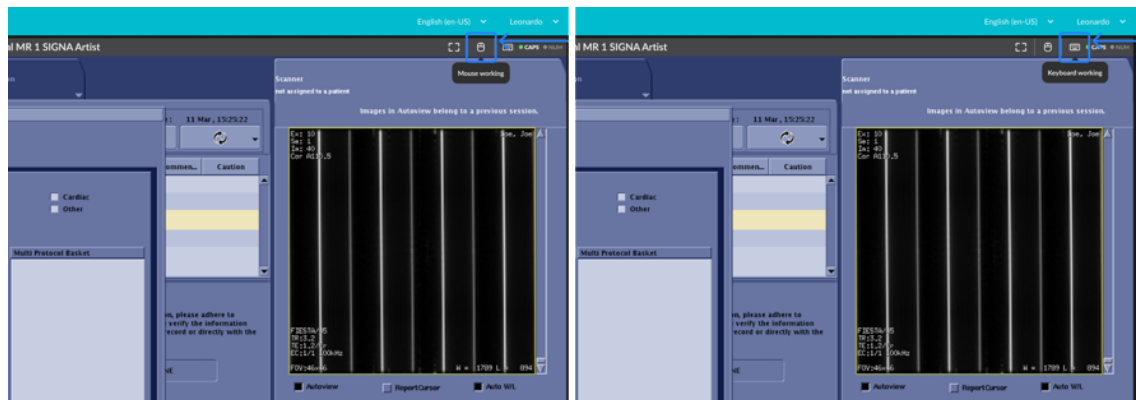


Figura 21: Barra de transmisión

Izquierda - Información sobre las herramientas de estado del ratón

Derecha - Información sobre las herramientas de estado del teclado

3.5.3. Multicámara

Esta función permite al técnico remoto ver varias cámaras al mismo tiempo. Si hay más de una cámara disponible, es posible ver solo una y cambiar entre estas haciendo clic en el menú con el nombre designado para cada cámara. Al seleccionar «ALL CAMERAS» (TODAS LAS CÁMARAS), todas las cámaras disponibles se mostrarán en el marco, con una de estas resaltada. Para cambiar la cámara resaltada, simplemente pase el ratón sobre una de las cámaras en el marco más pequeño y haga clic en «SWITCH CAMERA» (CAMBIAR CÁMARA).

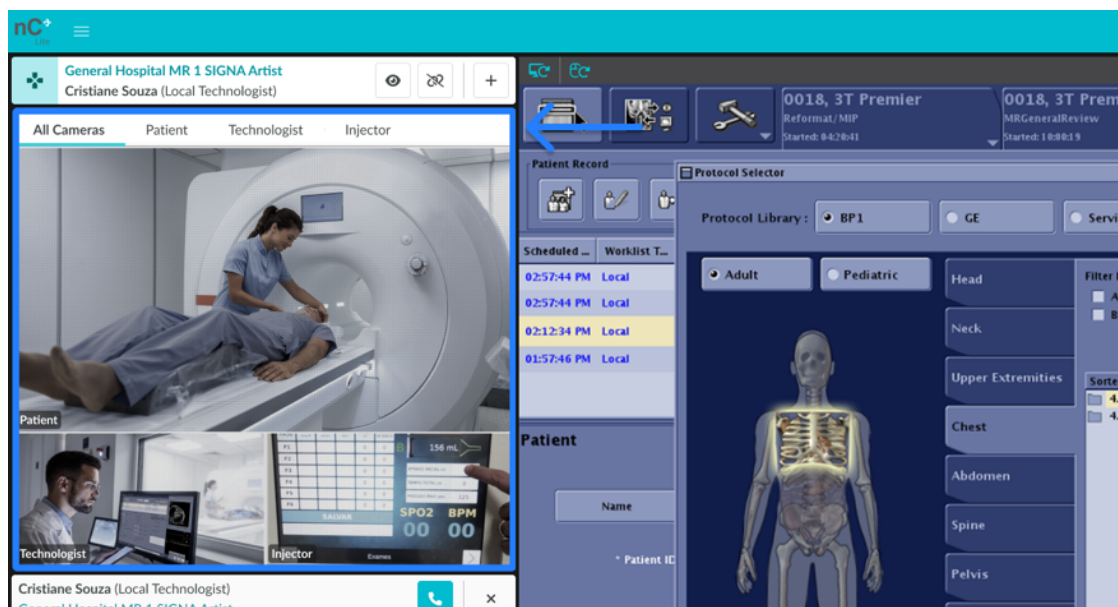


Figura 22: Vista de marco multicámara

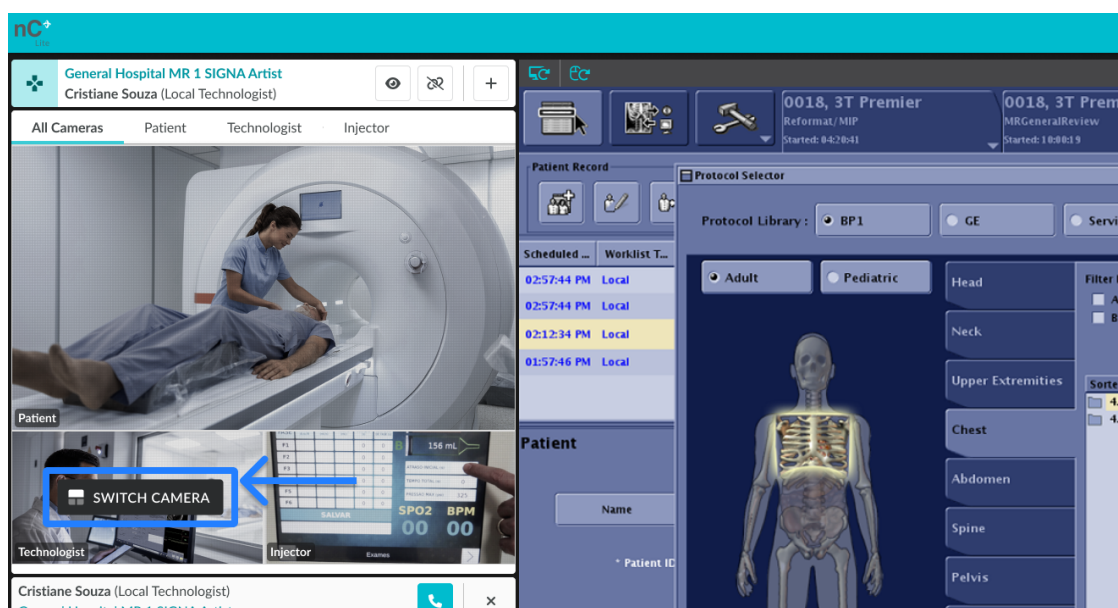


Figura 23: Botón "SWITCH CAMERA" (CAMBIAR CÁMARA) flotante de la opción multicámara

Durante una sesión remota activa, si el técnico remoto está accediendo en el modo **Vista**, existe la opción de apagar una o más cámaras pasando el ratón por encima de la cámara elegida y haciendo clic en «TURN OFF CAMERA» (APAGAR CÁMARA). Para volver a ver la cámara, simplemente repita el proceso y haga clic en «TURN ON CAMERA» (ENCENDER CÁMARA).

NOTA: la opción de apagar las cámaras solo está disponible en el modo Vista; en el modo Control, no es posible apagar las cámaras.

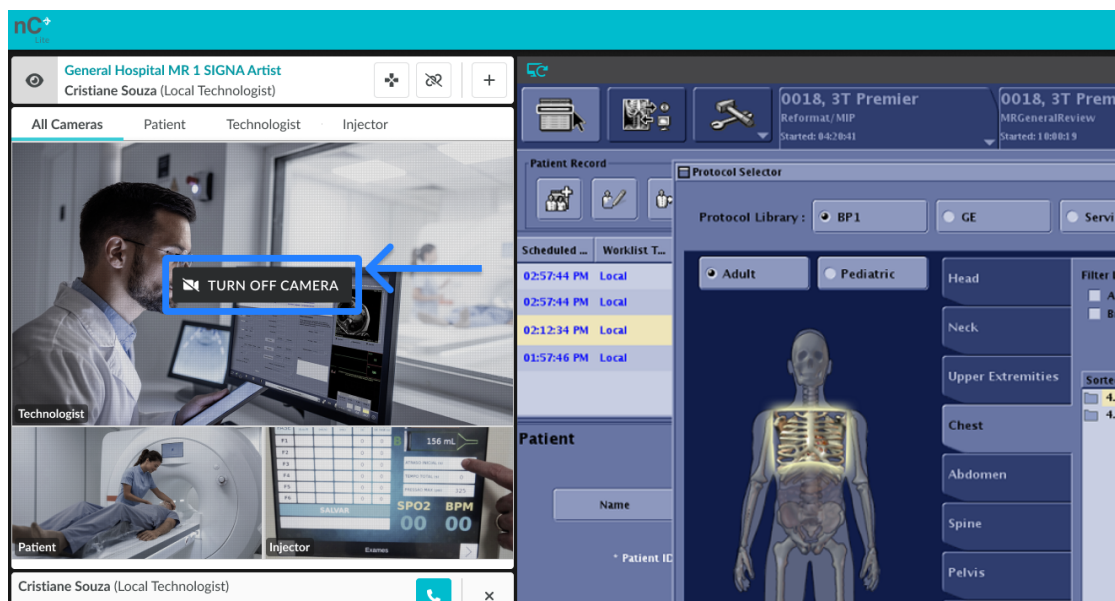


Figura 24: Botón "TURN OFF CAMERA" (APAGAR CÁMARA) de la opción multicámara en modo Vista

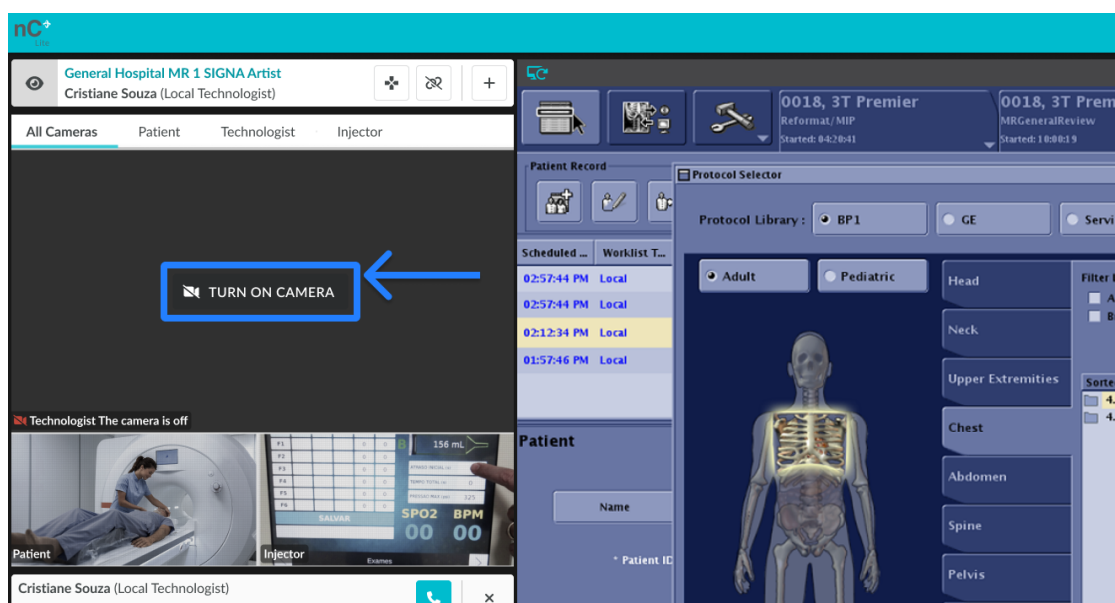


Figura 25: Botón "TURN ON CAMERA" (ENCENDER CÁMARA) de la opción multicámara en modo Vista

3.5.4. Abrir otro dispositivo

Permite al técnico remoto abrir una nueva pestaña del navegador de nCommand Lite, lo que permite al usuario seleccionar un nuevo dispositivo para realizar más de una exploración remota simultáneamente. Para abrir un nuevo dispositivo al que acceder, solo tiene que hacer clic en el botón «Open Another Device» (Abrir otro dispositivo) y se mostrará una advertencia para que pueda realizar esta operación de forma segura y simultánea. Debe leer la advertencia antes de acceder a esta nueva ventana.

NOTA: para una mejor visualización durante el acceso simultáneo, se recomienda que, después de hacer clic en «OPEN ANOTHER DEVICE» (ABRIR OTRO DISPOSITIVO) y hacer clic en «OK» (ACEPTAR) en las advertencias, arrastre la nueva pestaña a otro monitor disponible.



¡ADVERTENCIA!

Advertencia de seguridad para el acceso a varios dispositivos

- **Exigencia de concentración intensa:** el acceso simultáneo requiere una intensa concentración y comunicación con los equipos locales.
- **Selecciona diferentes diseños:** evite acceder al mismo tiempo a dispositivos con diseños idénticos o a exploraciones de la misma región anatómica.
- **Arrastra la pestaña a otro monitor:** al acceder a un dispositivo adicional, se abrirá una nueva pestaña. Arrastre esta pestaña a un segundo monitor, ya que el sistema está diseñado para utilizarse con una pantalla independiente para cada dispositivo.
- **Preste atención a los avisos:** preste mucha atención a todos los avisos del sistema, ya que son cruciales para un funcionamiento seguro.
- **Control de uno en uno:** puede ver varias pantallas, pero el control se limita a un solo dispositivo al mismo tiempo.
- **Abrir chat:** inicie siempre el chat cuando esté conectado a un dispositivo para mantener una comunicación clara.
- **Llamadas de una en una:** los avisos de llamadas de voz aparecen en la pantalla del dispositivo asociado; solo puede haber una llamada activa al mismo tiempo.
- **Seguridad y alerta:** dé prioridad a la seguridad y manténgase alerta durante todas las operaciones.

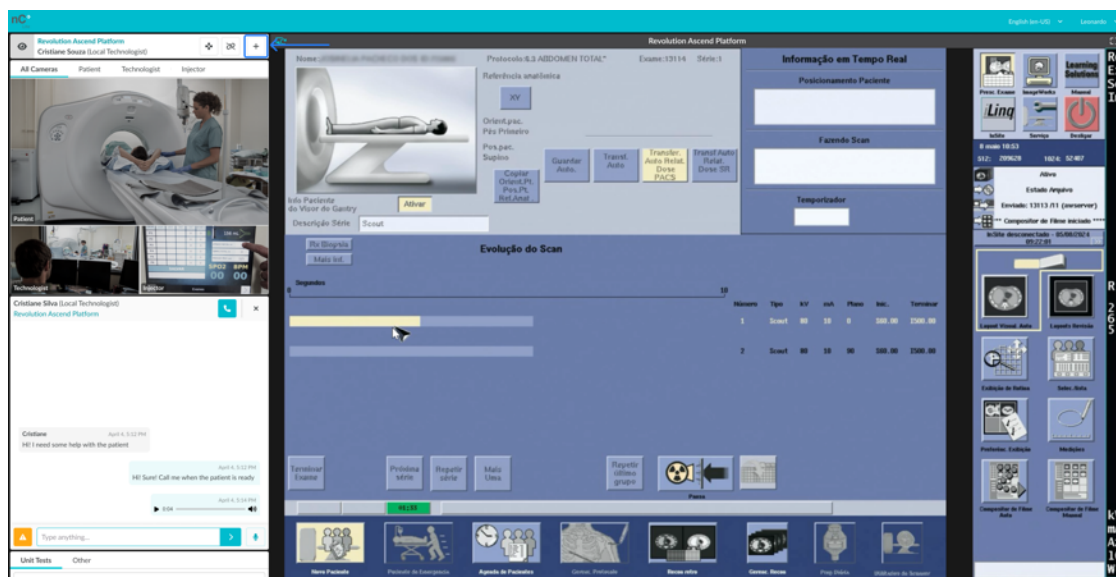


Figura 26: Botón “Open Another Device” (+) (Abrir otro dispositivo)

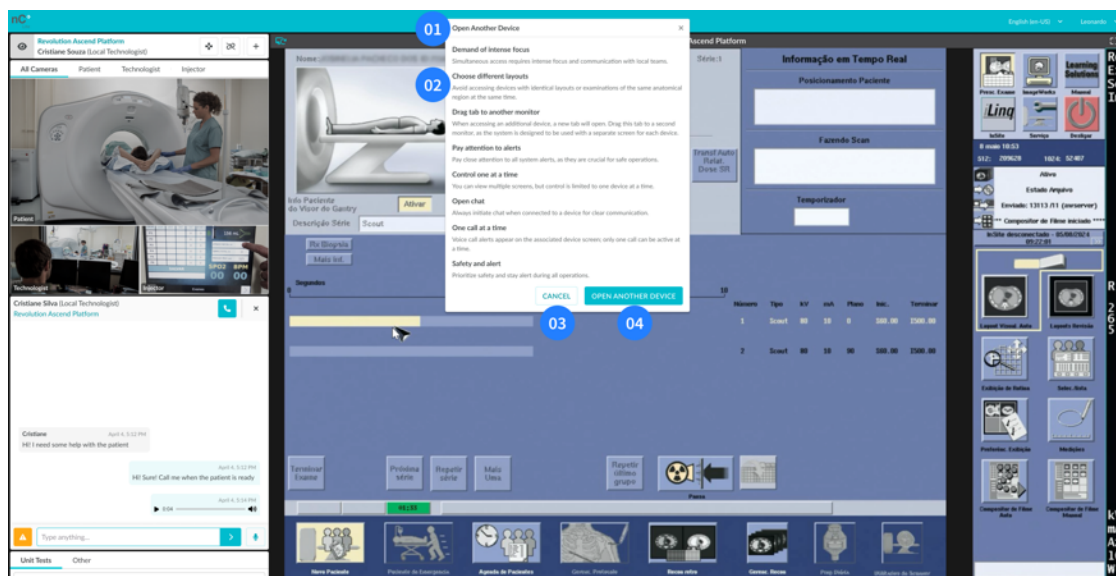


Figura 27: Advertencias de acceso a múltiples dispositivos

- 01** – Título (Open Another Device [Abrir otro dispositivo]); **02** – Advertencias de seguridad operativa; **03** – Botón Cancel (Cancelar); **04** – Botón Abrir otro dispositivo

3.5.5. Verificación del sistema

La función Verificación del sistema ayuda a verificar que el dispositivo, la red y la conectividad a internet actuales cumplen con los requisitos para utilizar nCommand Lite correctamente. Realiza una prueba automática rápida que verifica elementos esenciales como la calidad de la conexión a internet, el acceso a los servidores requeridos y la estabilidad de la conexión. Esta herramienta puede utilizarse antes de iniciar una sesión, durante la instalación o cuando se sospeche de algún problema de conexión. Ayuda a garantizar que la plataforma funcione como se espera y brinda asistencia al equipo técnico si es necesario realizar tareas para solucionar problemas.

Nota: la verificación del sistema debería utilizarse preferentemente con el apoyo o a solicitud de un profesional de TI. El uso de esta herramienta sin la debida asistencia técnica puede dar lugar a una interpretación errónea de los resultados.

Para acceder a la Verificación del sistema, los técnicos locales y remotos deben abrir la opción Detalles de la Sesión desde el menú desplegable disponible bajo su nombre de usuario, ubicado en la esquina superior derecha de la pantalla principal. Luego, haga clic en **Open** (Abrir) junto a la herramienta **System Check** (Verificación del sistema). Una vez que se muestre la página de la herramienta, haga clic en **Run Test** (Ejecutar prueba) para iniciar el proceso de verificación.

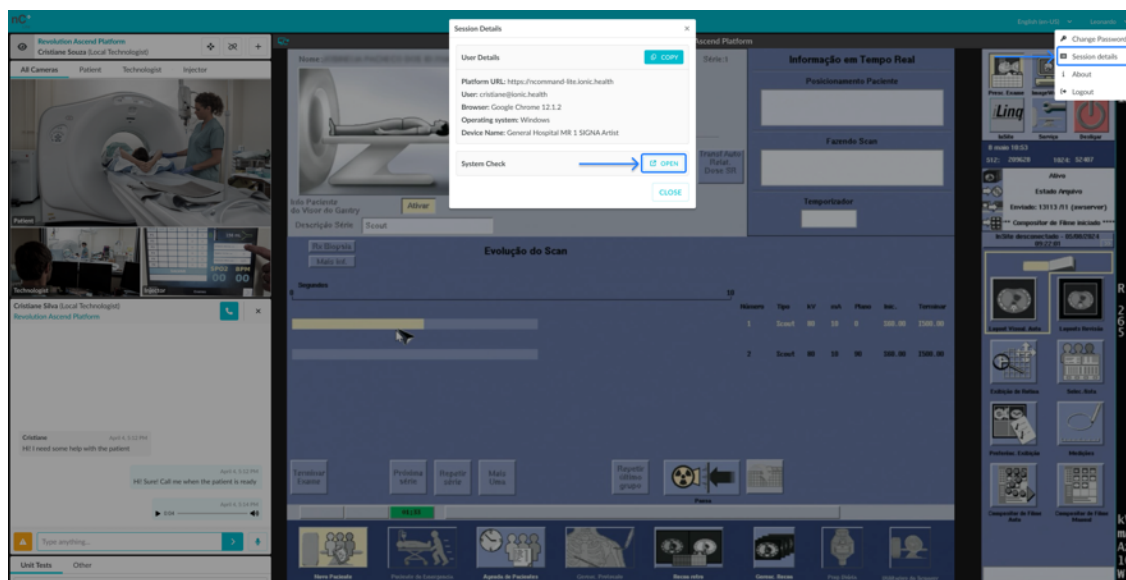


Figura 28: Acceso a Verificación del sistema

Al utilizar el técnico remoto, es posible seleccionar un dispositivo en la pantalla principal de la herramienta para que se incluya en los resultados de la prueba.



¡ADVERTENCIA!

Antes de comenzar la prueba, asegúrese de que el dispositivo seleccionado no esté en uso actualmente.

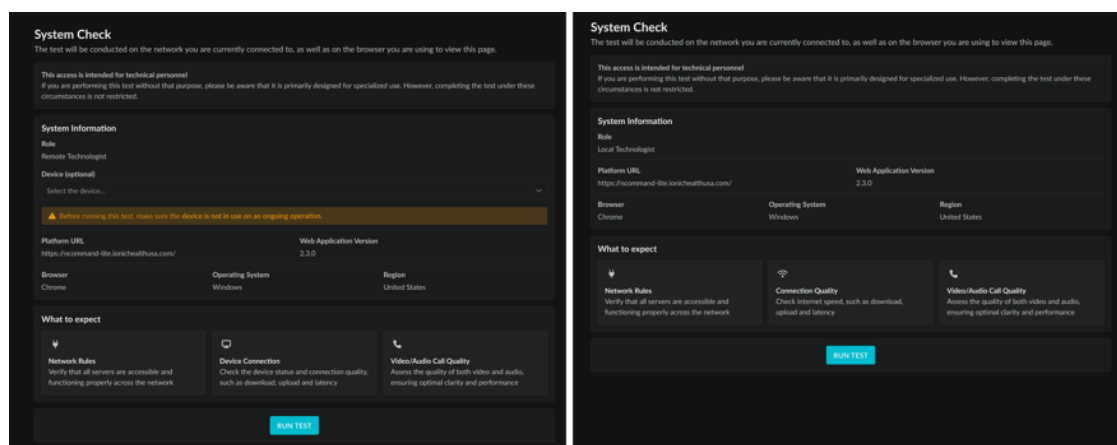


Figura 29: Pantalla principal de Verificación del sistema
Izquierda - Técnico remoto / Derecha - Técnico local

Una vez que se completa la prueba, se muestra un resumen de los resultados en la pantalla. Los profesionales de TI pueden revisar esta información para identificar posibles problemas que afecten al rendimiento del sistema.

Sección 3.6 - Chat

La plataforma ofrece una función de chat y llamada en tiempo real con funciones de voz y vídeo, que se utiliza para una comunicación eficaz entre técnicos autorizados. A través de estas funciones, los técnicos con licencia pueden interactuar con respecto a todos los asuntos relacionados con el flujo de trabajo de la sesión, utilizando comunicación directa de voz y texto.

**¡ADVERTENCIA!**

En caso de fallo, llame al técnico local por teléfono.

Al conectarse a un dispositivo, tendrá acceso inmediato a la lista de usuarios del chat, organizada en dos pestañas. Para los clientes de varios sitios, cada sucursal se puede configurar como un contrato independiente. Cuando está habilitado, los usuarios se agrupan por contrato, y los usuarios de otros contratos aparecen en la pestaña "Otros".

Para iniciar una conversación, haga doble clic en el nombre de un usuario para abrir la interfaz de chat, que admite mensajes de texto y llamadas de voz. Asegúrese de que la sesión seleccionada corresponda al dispositivo correcto. La plataforma notifica a los usuarios si la conexión de red se vuelve lenta o inestable.

**¡ADVERTENCIA!**

Antes de iniciar el contacto, verifique el nombre del dispositivo que se muestra debajo del nombre del usuario, ya que algunos técnicos remotos pueden estar conectados a varios dispositivos.

Estas son las herramientas disponibles para la comunicación dentro de la plataforma:

1. **Llamadas de voz y vídeo:** haga clic en el icono para iniciar una llamada de voz y vídeo de hasta 60 minutos entre un técnico remoto y un técnico local. No se admiten conexiones entre usuarios con el mismo perfil (Local-Local o Remoto-Remoto).

Cuando un técnico local inicia una llamada, el técnico remoto puede optar por aceptarla o rechazarla. Inversamente, cuando un técnico remoto inicia la llamada, esta se conecta automáticamente y se notifica al técnico local—esto funciona como un mecanismo de seguridad para garantizar que el técnico remoto siempre pueda comunicarse con quien esté físicamente presente en el sitio, como si estuviera allí en persona.

De forma predeterminada, el micrófono está activo al inicio de la llamada, mientras que la cámara permanece apagada. Cada técnico puede encender o apagar manualmente su micrófono y cámara en cualquier momento.

Para establecer una llamada con éxito, ambos usuarios deben tener un micrófono y una salida de audio que funcionen, con los permisos del navegador debidamente habilitados. Si falta alguno de estos componentes, el sistema notificará a ambos usuarios y la llamada no se completará. Una cámara es opcional: si no está disponible o no se detecta, el sistema actualizará el icono para reflejar que el vídeo no es compatible.

Solo se permite una llamada activa por usuario. Si un técnico intenta iniciar una nueva llamada mientras hay otra activa, el sistema bloqueará el intento y mostrará una notificación. Del mismo modo, si un usuario ya está en una llamada y recibe otra llamada entrante, se informará a la persona que llama de que el destinatario no está disponible actualmente, y el usuario de la llamada en curso recibirá una alerta que indica que alguien ha intentado ponerse en contacto con él/ella.

2. **Cierre de chats:** cuando uno de los usuarios cierra el chat haciendo clic en el botón Close (Cerrar), se envía un mensaje automático al otro usuario y se cierra la pestaña de chat. Esto garantiza que se informe a ambas partes de que la conversación ha terminado. Cuando la ventana de chat está cerrada, todos los mensajes desaparecen. Si lo vuelve a abrir durante la sesión, la conversación se reinicia sin los mensajes anteriores.
3. **Mensajes de texto:** envíe mensajes de texto en el campo designado. Cuando se envía un mensaje, aparece un icono con una marca de verificación gris y, cuando el destinatario recibe el mensaje, se muestra otro icono con dos marcas de verificación azules. Esto permite una comunicación por escrito segura, clara y concisa entre las dos partes.
4. **Llamar la atención:** atraiga la atención del otro usuario haciendo clic en el botón con un signo de exclamación. Esta acción aplica un efecto de vibración visual en la ventana del otro usuario durante unos segundos y se envía automáticamente un mensaje que indica urgencia o importancia.
5. **Mensajes de audio:** envíe mensajes de audio haciendo clic en el botón del micrófono. Esto se utiliza cuando desea transmitir un mensaje de forma más personal o cuando escribir no resulta conveniente.

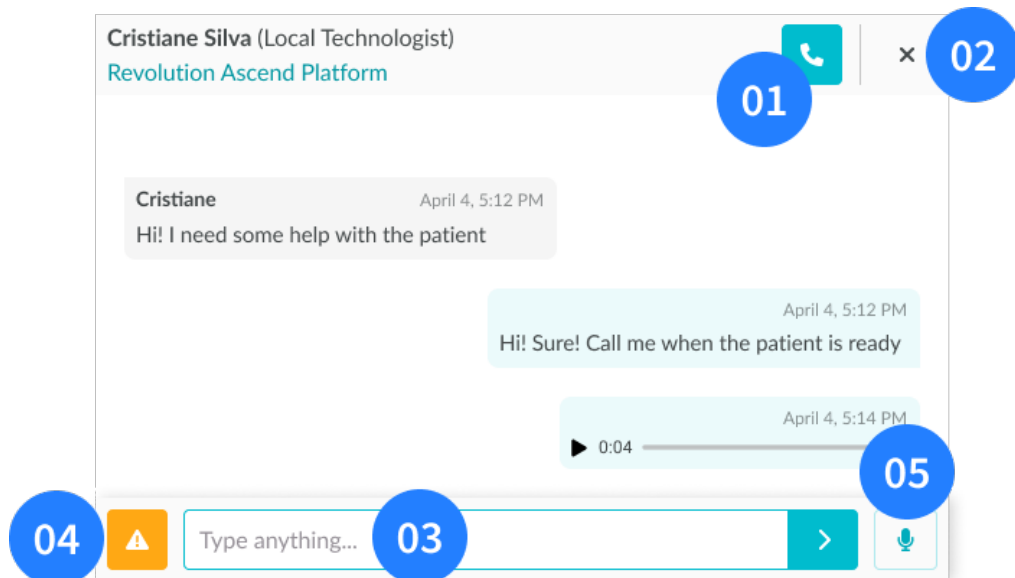


Figura 30: Vista de la ventana de chat

01 – Botón de llamada de voz y vídeo; **02** - Botón Cerrar chat; **03** – Cuadro de texto del mensaje;
04 – Botón de llamada de atención; **05** – Botón de grabación Mensaje de audio

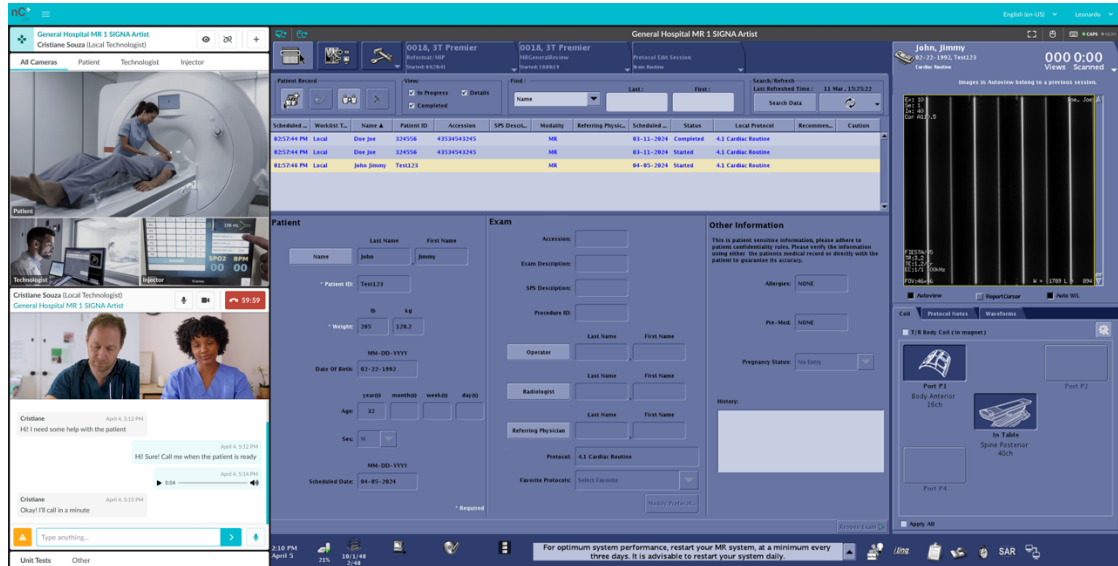


Figura 31: Pantalla principal del técnico remoto - Ventana de chat (esquina inferior izquierda)

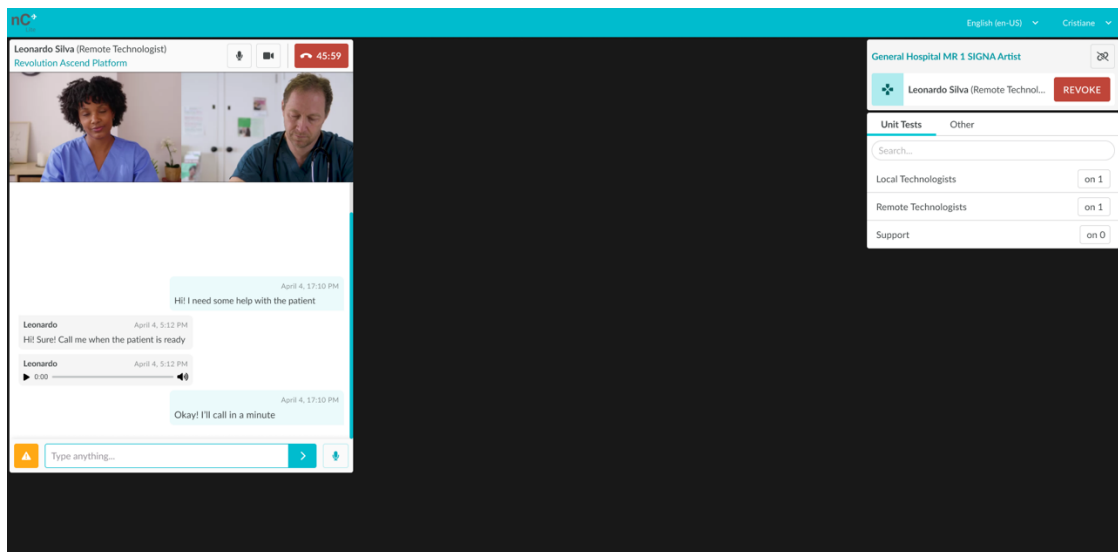


Figura 32: Pantalla principal del técnico local - Ventana de chat

Problemas de conexión a Internet: cuando uno de los técnicos tiene problemas de conexión de red, el sistema muestra un mensaje e intenta volver a conectar. Si se restablece la conexión, el sistema mostrará el mensaje **ONLINE (EN LÍNEA)** y la sesión remota continuará de la manera habitual. Sin embargo, en caso de que la conexión no se reestablezca después de varios intentos de reconexión, el sistema finalizará la sesión activa y notificará al técnico que se ha producido una desconexión debido a problemas de Internet. Al mismo tiempo, también notificará al otro técnico que su homólogo ha sido desconectado debido a problemas de Internet.

Sección 3.7 - Finalización de la sesión en la plataforma

Al final de su turno, el técnico autorizado debe desconectarse del dispositivo y cerrar la sesión de la plataforma.



¡ADVERTENCIA!

Los técnicos autorizados no deben olvidarse de cerrar la sesión en la plataforma antes de que finalice su turno.

Para desconectarse del dispositivo, necesita hacer clic en el icono de desconexión situado en el Cuadro del dispositivo. Nota: si está trabajando como técnico local, asegúrese de que ha revocado cualquier acceso de técnico remoto antes de desconectarse del dispositivo.

Para garantizar la seguridad, recibirá una notificación para confirmar que desea desconectarse del dispositivo. Después de confirmarlo, se le redirigirá a la pantalla de inicio, sin ningún dispositivo seleccionado.

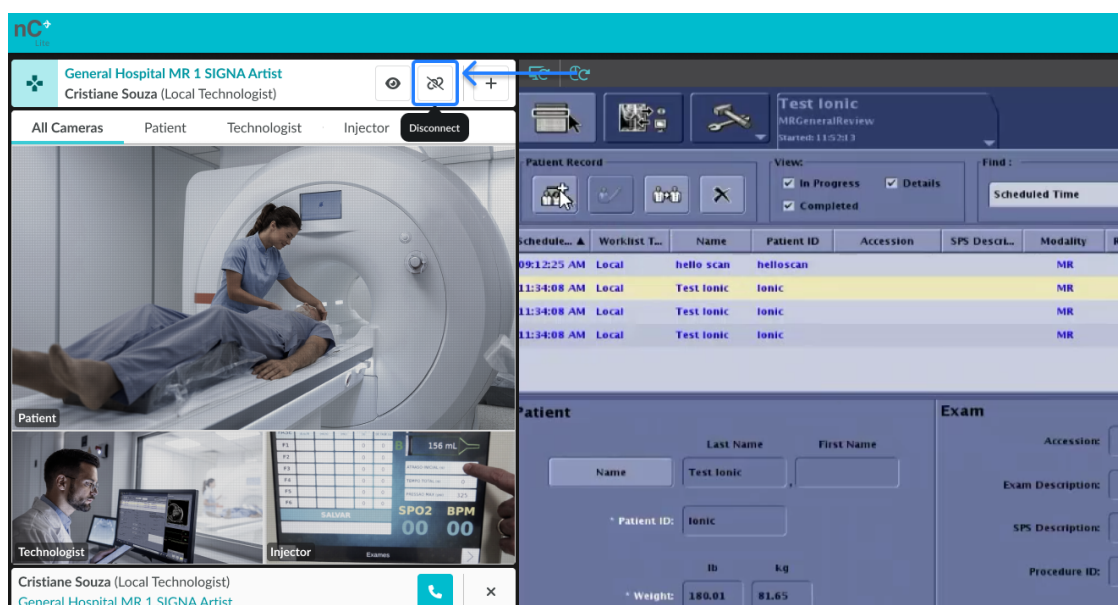


Figura 33: Pantalla principal del técnico remoto con el botón “Disconnect” (Desconectar)

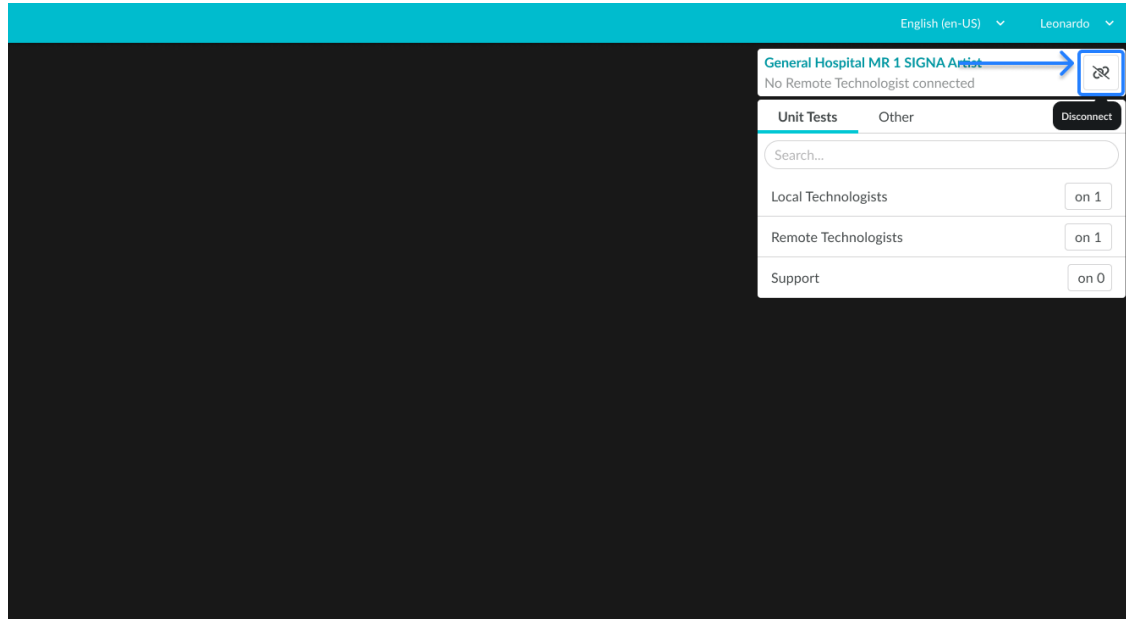


Figura 34: Pantalla principal del técnico local con el botón “Disconnect” (Desconectar)



¡ADVERTENCIA!

Antes de cerrar la sesión, asegúrese de que todas las pestañas adicionales que se abrieron estén cerradas.

Para finalizar su sesión en la plataforma, haga clic en su nombre de usuario situado en la esquina superior derecha de la pantalla y seleccione la opción «Logout» (Cerrar sesión). Recibirá una notificación para confirmar que desea salir del centro médico donde estaba trabajando. Tras la confirmación, se le redirigirá a la página de inicio de sesión de la aplicación, finalizando así de forma segura su jornada de trabajo.

nCommand Lite no controla la sesión del usuario en el IdP externo y, por lo tanto, no puede realizar un cierre de sesión en el nivel de IdP. En escenarios en los que los usuarios comparten la misma máquina y utilizan el inicio de sesión único (SSO), se recomienda que cada usuario seleccione la opción “no permanecer conectado” durante el inicio de sesión del IdP externo (si está disponible) o cierre la sesión del IdP después de cerrar sesión en nCommand Lite. Esto garantiza que ningún usuario posterior en el mismo dispositivo pueda reutilizar involuntariamente una sesión activa.

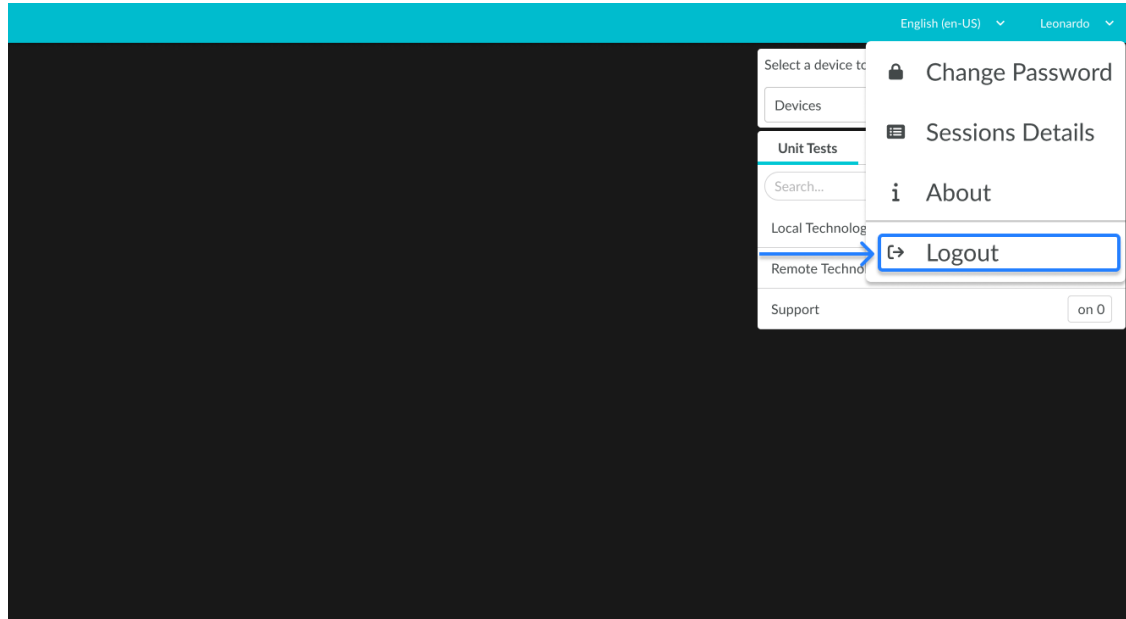


Figura 35: Elemento del menú desplegable Logout (Cerrar sesión)



¡ADVERTENCIA!

Cuando utilice un proveedor de identidad externo en un equipo compartido o público, después de cerrar sesión en la plataforma, cierre también la sesión del proveedor de identidad. Para obtener más información sobre cómo proceder, póngase en contacto con el equipo de soporte técnico de TI de su organización.

Sección 3.8 - Entrenamiento operativo

La participación en el programa de formación es obligatoria para todos los usuarios del Sistema nCommand Lite. El registro de usuarios en la plataforma lo gestiona el equipo de IONIC Health y solo se inicia tras la confirmación de que el usuario ha completado con éxito la formación requerida en el LMS y está debidamente cualificado para operar la plataforma. Este proceso garantiza que todos los usuarios posean un conocimiento profundo de las funcionalidades del sistema y estén preparados para utilizar la plataforma de forma eficiente y segura. Para iniciar el proceso de inscripción en la formación, póngase en contacto con su representante de ventas.

Sección 3.9 - Directrices para la solución de problemas

USUARIO Y CONTRASEÑA	
Cambio de contraseña	Valide que se han cumplido los requisitos de la contraseña: esta debe ser robusta y segura, tener al menos 8 caracteres e incluir al menos una letra minúscula, una letra mayúscula y un carácter especial.
Olvidé mi contraseña	Compruebe su bandeja de entrada de correo electrónico: asegúrese de que está utilizando la dirección de correo electrónico correcta y de que el correo electrónico de recuperación de contraseña no se ha filtrado en su carpeta de correo no deseado. Inténtelo de nuevo: espere unos minutos y solicite otro correo electrónico de recuperación de contraseña haciendo clic en «Did you Forget your password?» (¿Olvidó su contraseña?). Compruebe la conexión a Internet: asegúrese de que está conectado a Internet.
Correo electrónico de bienvenida no recibido	Compruebe si el correo electrónico está en su carpeta de correo no deseado. Si no está ahí, póngase en contacto con un usuario administrador para asegurarse de que el correo electrónico proporcionado en su registro es correcto. Si no es correcto, el administrador debe actualizarlo y reenviar el correo electrónico de bienvenida.
Código de autenticación de dos factores no recibido	Haga clic en «Resend Code» (Reenviar código) y compruebe su carpeta de correo no deseado. Si no lo recibe, póngase en contacto con un usuario administrador para verificar si el correo electrónico registrado en el control de acceso es correcto.
Se han superado los intentos de inicio de sesión	Si supera el número permitido de intentos de inicio de sesión, debe esperar un periodo antes de intentarlo de nuevo.
PROVEEDOR DE IDENTIDAD EXTERNO	

Problemas al iniciar sesión en el producto	Si tiene problemas de inicio de sesión mientras utiliza un proveedor de identidad (IdP) externo, tenga en cuenta que el proceso de autenticación es gestionado completamente por el IdP y no por el proveedor del producto, es decir: Ionic Health. Como tal, el producto no puede ayudar con las credenciales de la cuenta, las políticas de acceso, los errores de autenticación o el bloqueo de la cuenta. En estos casos, debe ponerse en contacto con el equipo de soporte técnico de TI de su organización, que puede revisar la configuración del IdP y ayudar a resolver el problema.
Problemas de credenciales	Cualquier problema relacionado con las credenciales (<i>por ej.</i> , olvido de la contraseña, cambio de contraseña) debe resolverse directamente con el equipo de soporte de TI de su organización. Ellos pueden revisar la configuración del IdP y proporcionar la asistencia necesaria.
Problemas con el autenticador multifactor (MFA)	Cualquier problema relacionado con el autenticador multifactor (MFA) (<i>por ej.</i> , problemas de caducidad del MFA, MFA que no funciona, inicio de sesión sin solicitar MFA) debe resolverse directamente con el equipo de soporte de TI de su organización. Ellos pueden revisar la configuración del IdP y proporcionar la asistencia necesaria.
Las credenciales no funcionan en la plataforma	Cuando utilice proveedores de identidad (IdP) externos, inicie sesión en el producto solo con el IdP. El uso de las credenciales del IdP directamente en la página de inicio de sesión del producto dará como resultado un inicio de sesión incorrecto.
MONITOR DE ORDENADOR DE ESCÁNER	
No se enciende	Compruebe las conexiones del monitor al ordenador y a la toma de corriente. Pueden producirse desconexiones. Pulse de nuevo el botón de encendido del monitor.
PLATAFORMA	
Inaccesible	Compruebe la conexión de red. Compruebe si la plataforma se ha

	iniciado y si se ha producido el inicio de sesión.
Latencia de la plataforma	Actualice la página pulsando Ctrl+F5. Compruebe si el chat de la unidad (del centro médico) está abierto en más de una pestaña. Si es así, cierre la pestaña que no se esté utilizando. Si el problema persiste, intente cerrar sesión en la plataforma, borrar la caché, cerrar el navegador y volver a iniciar sesión.
Funciones con fallos	Antes de intentar otros procedimientos de solución de problemas, borre la memoria caché del navegador (busque instrucciones en su navegador actual) después de iniciar sesión, luego cierre y vuelva a abrir el navegador, vuelva a iniciar sesión en la plataforma y vuelva a intentar la acción.
Actualizar	Una vez que se haya actualizado la plataforma, borre la memoria caché de su navegador (consulte las instrucciones de su navegador) antes de iniciar sesión en la nueva versión.
AUDIO	
No hay sonido	Asegúrese de que los volúmenes del micrófono y del altavoz de la unidad (centro médico) estén ajustados a los niveles adecuados. Compruebe si el navegador tiene permiso para utilizar el audio y el micrófono. Compruebe si los auriculares están conectados y funcionan correctamente.
Latencia de sonido	Compruebe las conexiones eléctricas y de red del equipo. Actualice la página del navegador pulsando Ctrl+F5 e inicie sesión de nuevo. Si el problema persiste, intente cerrar sesión en la plataforma, borrar la caché, cerrar el navegador y volver a iniciar sesión.

CHAT	
El chat no aparece	Asegúrese de que el navegador no esté minimizado. De lo contrario, abra el chat después de iniciar sesión en la plataforma nCommand Lite. Compruebe que se ha seleccionado la unidad (centro médico) y que el usuario está autorizado a habilitar la comunicación por chat. Asegúrese de que se acepten los permisos de audio y micrófono de su navegador. Compruebe las conexiones de los cables, que pueden estar desconectadas. Actualice la página del navegador pulsando Ctrl+F5 y vuelva a conectarla a la plataforma. Compruebe si el chat del centro está abierto en más de una pestaña. Si es así, cierre la pestaña que no se esté utilizando.
Retraso del chat	Actualice la página del navegador pulsando Ctrl+F5 y vuelva a conectarla a la plataforma. Si el problema persiste, intente cerrar sesión en la plataforma, borrar la caché, cerrar el navegador y volver a iniciar sesión. Compruebe las conexiones de los cables, que pueden estar desconectadas.
Problemas al enviar mensajes de audio	Compruebe los permisos del navegador para audio y micrófono y asegúrese de que tanto el micrófono como los dispositivos de audio estén conectados al ordenador. Si es necesario ajustar los permisos del navegador, pulse Ctrl+F5 para indicar al navegador que reconozca los cambios al volver a cargar la página.

Error al iniciar la llamada de voz	Compruebe su conexión a Internet y vea si se ha mostrado alguna notificación que explique el motivo por el que la llamada no se inició. Asegúrese de que tiene un dispositivo de audio conectado y de que los permisos de audio y micrófono están permitidos en el navegador. Si el problema persiste, actualice la página con Ctrl+F5 para intentarlo de nuevo.
Usuario no encontrado en chat	Si no puede localizar un usuario en el chat, haga clic en la pestaña «Others» (Otros) para asegurarse de que no esté incluido allí. Los usuarios asociados a otros contratos aparecen por separado en la lista de contactos. Si su usuario no aparece en la lista de contactos después de seleccionar el dispositivo, pulse Ctrl+F5 para actualizar la pantalla y seleccione de nuevo. Asegúrese de tener una conexión a Internet.
SOLICITUD DE ACCESO AL DISPOSITIVO	
La plataforma no ha reconocido que el técnico local está conectado	Marque la opción «Others» (Otros) para confirmar si el usuario local está conectado. Si el usuario está conectado pero sigue recibiendo el mensaje de que el usuario local no está conectado al escáner, actualice la pantalla pulsando Ctrl+F5 y pida al usuario local que repita la misma instrucción. A continuación, seleccione el dispositivo de nuevo y pida al usuario local que seleccione el dispositivo de nuevo también. Si el problema persiste, póngase en contacto con el servicio técnico para comprobar la red.
No se está enviando la solicitud de acceso	Actualice la página pulsando Ctrl+F5 y confirme con el usuario local por chat si se está recibiendo la solicitud de acceso. Si el problema persiste, póngase en contacto con el servicio técnico para obtener más ayuda.
DISPOSITIVO DE TRANSMISIÓN (ORDENADOR e-KVM)	
El dispositivo de transmisión (ORDENADOR e-KVM) no funciona	Haga clic en el botón «Reload streaming» (Recargar transmisión) de la plataforma.

	Asegúrese de que la fuente de alimentación ininterrumpible y estabilizada (centro médico) y/o el dispositivo de transmisión estén correctamente conectados y encendidos. Apague el dispositivo de transmisión y todos los demás equipos y vuelva a encenderlo. Actualice la plataforma.
Dispositivo de transmisión lento	Haga clic en el botón «Reload streaming» (Recargar transmisión) de la plataforma. Actualice la página con Ctrl+F5 y vuelva a conectarla a la plataforma. Compruebe la calidad de la conexión de red. Para validar el estado de la red, es posible realizar una prueba de ping al dispositivo para comprobar la pérdida de paquetes. Después de los problemas de Internet, es posible que la plataforma no funcione según lo previsto. Actualice la página web y solicite de nuevo acceso al usuario local.
Pérdida de salida de vídeo	Cabe la posibilidad de que una descarga electrostática provoque una pérdida de imagen. Después de reiniciar el sistema, la comunicación y la transmisión de vídeo deben restablecerse automáticamente.

Sección 3.10 - Métodos de limpieza del hardware

- Antes de iniciar el proceso de limpieza, asegúrese de que todo el equipo esté desconectado de la toma de corriente.
- No utilice productos abrasivos.
- No sumerja ningún equipo o periférico en ningún tipo de líquido.
- Deseche los materiales de limpieza de acuerdo con las normativas para la eliminación de residuos peligrosos.
- No se recomienda utilizar desinfectante en aerosol, ya que podría entrar vapor en el equipo y provocar un cortocircuito o corrosión.
- Este producto no es estéril.

Capítulo 4 Seguridad informática y privacidad

Sección 4.1 - Riesgos de seguridad y privacidad

El **Sistema nCommand Lite** implementa varias medidas técnicas y organizativas para proteger la información tratada.

El sistema ha sido certificado bajo ISO/IEC 27001 e ISO/IEC 27701 y sigue un enfoque de privacidad por diseño. Garantiza la conformidad con la legislación sobre protección de datos en el ámbito sanitario y con las regulaciones de ciberseguridad vigentes en la Unión Europea, Estados Unidos, Reino Unido, Suiza, Brasil, Emiratos Árabes Unidos, Arabia Saudita, Australia y Nueva Zelanda.

Sin embargo, los usuarios deben adoptar las mejores prácticas para evitar la exposición innecesaria de datos confidenciales.

- Evite compartir información personal o confidencial a menos que sea estrictamente necesario.
- Asegúrese de que las comunicaciones y el acceso al sistema se realicen en entornos seguros.
- Si sospecha de alguna actividad maliciosa, notifique de inmediato al equipo responsable.

Sección 4.2 - Protección de datos personales (cumplimiento con el RGPD/la HIPAA)

El sistema **nCommand Lite** cumple con todas las leyes y regulaciones aplicables de privacidad y protección de datos en las regiones donde opera, incluidas, entre otras, los requisitos de GDPR, HIPAA, LGPD y la norma ISO/IEC 27701. Todas las actividades de procesamiento de datos se rigen bajo los roles de "**Procesador**" y "**Subprocesador**" según lo definido por el GDPR, con una estricta segregación regional de datos para garantizar el cumplimiento normativo y evitar transferencias no autorizadas de datos transfronterizos

¿Qué datos se recopilan?

- **Usuarios:** nombre, dirección de correo electrónico y empresa (estrictamente para la autenticación y la gestión de acceso).
- **Datos del paciente:** únicamente transmisiones de exámenes médicos mediante streaming a tiempo real, sin almacenamiento de datos

¿Cómo se utilizan y protegen los datos?

- Los datos se usan exclusivamente con fines de **autenticación, control del acceso y trazabilidad de la sesión**.
- La transmisión de la información se protege mediante **cifrado AES-256 para el almacenamiento y TLS 1.3 para datos en tránsito**.
- **El acceso está restringido** y sigue el **principio del menor privilegio (RBAC)**.

- Cifrado de extremo a extremo garantizado para video P2P y flujos de control a través de WebRTC.
- Los proveedores de nube autorizados (por ejemplo, Microsoft Azure) procesan datos limitados bajo estrictas protecciones contractuales.

Se conceden los siguientes derechos a los usuarios:

- **Acceso y corrección** de información personal.
- **Solicitud de eliminación de datos**, cuando corresponda.

Si tiene alguna pregunta, envíe un mensaje de correo electrónico a privacy@ionic.health para comunicarse con el responsable de privacidad de los datos de Ionic Health. Todas las solicitudes se gestionan en un plazo de 30 días, prorrogable de acuerdo con el RGPD.

Sección 4.3 - Gestión y autenticación del acceso

Los usuarios son responsables de definir **roles y permisos de acceso** para sus equipos, y de garantizar la revisión y documentación periódica del acceso otorgado.

Mejores prácticas y controles

- Siga el **principio del menor privilegio (RBAC)** para garantizar que los usuarios tengan únicamente el nivel de acceso necesario.
- La **autenticación multifactor (MFA)** es obligatoria para el acceso administrativo y se recomienda para todos los usuarios.
- Se requieren **contraseñas fuertes** de al menos **8 caracteres, lo que incluye letras mayúsculas y minúsculas, números y símbolos**.
- **No comparta nunca credenciales.**
- Los permisos de acceso se supervisan y revisan periódicamente.

Supervisión: el acceso, las modificaciones de permisos y las actividades importantes se documentan en los registros de seguridad del sistema. Los registros se conservan durante un mínimo de 7 años, de acuerdo con la HIPAA, el GDPR y otras regulaciones aplicables. Estos admiten auditorías internas, análisis forenses e informes regulatorios. Los registros están protegidos contra la manipulación y se almacenan en entornos seguros con control de acceso.

Sección 4.4 - Control de acceso a la verificación del sistema

La función de verificación del sistema está disponible únicamente mediante la **aplicación web de nCommand Lite** y requiere credenciales válidas para el inicio de sesión. El acceso está restringido únicamente a roles autorizados: *técnico remoto*, *técnico local*, *administrador*, *supervisor de roles* y *usuario de verificación del sistema*.

El rol del *usuario de verificación del sistema* está diseñado con permisos restringidos, y permite el acceso únicamente a funciones de diagnóstico relacionadas con la validación de red y la verificación de conectividad. Esto garantiza que los detalles de la red, la información de listas blancas y las métricas del sistema nunca se expongan a personas no autorizadas.

Todas las solicitudes de acceso se autentican mediante Azure AD B2C, con Autenticación Multifactor (MFA) y políticas de acceso condicional adaptativo gestionadas por Microsoft Entra ID. La complejidad de la contraseña sigue la política de seguridad de la organización, exigiendo al menos ocho caracteres, que incluyan letras mayúsculas y minúsculas, números y símbolos. Las contraseñas caducan cada 90 días y las sesiones se cierran automáticamente después de 24 horas de inactividad, con posibilidad de extenderse hasta 90 días con uso continuo.

Sección 4.5 - Segregación regional de datos y retención de registros

La plataforma **nCommand Lite** aplica una rigurosa segregación regional de datos para evitar transferencias internacionales no autorizadas o innecesarias. Los entornos están aislados por región, lo que garantiza el cumplimiento de las normativas correspondientes.

Todos los registros de acceso, registros de actividad y eventos de seguridad se conservan durante un mínimo de siete (7) años, de conformidad con las normativas correspondientes de protección de datos y sanidad. Los registros se almacenan en entornos seguros y con control de acceso, y están protegidos contra manipulaciones. Esta información sirve de apoyo para investigaciones forenses, auditorías de cumplimiento normativo e informes regulatorios.

Sección 4.6 - Seguridad e integridad de los datos

El **Sistema nCommand Lite** garantiza la confidencialidad, integridad y disponibilidad de los datos mediante prácticas de seguridad estándares para el sector.

Los usuarios deben garantizar el cumplimiento con los protocolos de seguridad, revisar periódicamente las políticas de acceso e informar sobre cualquier anomalía. El sistema supervisa continuamente las actividades, y los administradores deben hacer cumplir las políticas de seguridad para mantener una defensa robusta contra posibles amenazas.

El sistema está protegido por monitorización 24/7 a través de un Centro de Operaciones de Seguridad (SOC) específico con capacidades SIEM para la detección y respuesta de amenazas.

Sección 4.7 - Respuesta ante incidentes de seguridad

El sistema incluye un Plan de Respuesta a Incidentes documentado, alineado con ISO 27035 y NIST CSF.

En caso de incidentes de seguridad, como acceso no autorizado o fallos del sistema, los usuarios deben seguir estos pasos:

¿Cómo identificar un incidente?

- Se detecta un **acceso no autorizado** en los registros de actividad.
- **Intentos de inicio de sesión sospechosos** o fallos repetidos en la autenticación.
- **Comportamiento inusual del sistema**, como acciones inesperadas o mal funcionamiento.

¿Cómo informar un incidente?

Registre inmediatamente el evento a través de los canales de asistencia técnica disponibles (Capítulo 5).

Si se confirma una violación de datos personales, IONIC, en calidad de subprocesador, notificará a GE como Procesador en un plazo de 48 horas, proporcionando todas las pruebas pertinentes, detalles de impacto y medidas de mitigación. GE, a su vez, es responsable de notificar al Controlador (el cliente) conforme a los requisitos legales y contractuales correspondientes.

Capítulo 5 Canales de servicio

Tanto si necesita ayuda con un problema técnico, un paso poco claro en el proceso o más orientación, nuestro equipo está listo para ayudarle. Puede ponerse en contacto con nosotros por teléfono, correo electrónico o la plataforma ITSM, lo que le resulte más cómodo. Nuestros especialistas están formados para ofrecer asistencia personalizada, garantizando que cualquier problema se resuelva de forma rápida y eficiente.

Números de teléfono

Estados Unidos de América	+1 (216) 2421223
Brasil	+55 12 3600 0181
Europa (Portugal)	+351 (300) 528 410
Australia	+1 (216) 2421223
Nueva Zelanda	+1 (216) 2421223

Plataforma ITSM

<https://ionichealth.desk.ms/?LoginPortal>

Correo electrónico

helpdesk@ionic.health



¡ADVERTENCIA!

Cualquier incidente grave relacionado con el uso de este producto debe notificarse tanto al fabricante como a las autoridades sanitarias/autoridades competentes en el lugar de instalación del producto.

Para informar al fabricante: póngase en contacto con su representante de servicio local o informe a: helpdesk@ionic.health

Proporcione la siguiente información:

- El número de versión del sistema, que se muestra en la pantalla de inicio de sesión;
- Fecha del incidente;
- Descripción del incidente, incluido cualquier impacto/lesión del paciente o usuario;
- Su información de contacto (centro, dirección, nombre de contacto, cargo y número de teléfono).

Capítulo 6 Información legal y normativa

Fabricante



nCommand Lite

IONIC HEALTH TECHNOLOGIES S.A.

Estrada Dr. Altino Bondesan, 500, Sala 1103-A
Eugênio De Melo
São José Dos Campos-SP
12247-016
Brasil

CNPJ: 35.594.747/0001-08
+55 12 3600-0181
contato@ionic.health

Responsable técnico

Alexandre Seiji Fukuda Ribas
CREA-SP: 5071085437

ANVISA

82585300004

Importador (EE.UU.)



nCommand Lite System

IONIC HEALTH USA INC.

11201 Cedar Avenue, STE 600
Cleveland, OH 44106
USA

+1 (216) 242 1223

Representante/Importador en la UE



nCommand Lite



Número de identificación del organismo
notificado: 2803

EUROPE IONIC HEALTH DIGITAL TECHNOLOGIES, LDA

Rua de Raimundo Durães Magalhães, Lote 6/9
4475-189 Maia
Portugal

+351 (300) 528 410

Representante autorizado en Suiza (CH-REP) / Importador**CH REP****REF**

nCommand Lite

FREYR LIFE SCIENCES GMBH

Bahnhofplatz
CH-6300 Zug
Suiza

Persona responsable / Importador en el Reino Unido**REF**

nCommand Lite

FREYR LIFE SCIENCES LTD

9 Greyfriars Road
Reading, Berkshire
RG1 1NU
England, United Kingdom

Patrocinador australiano**REF**

nCommand Lite

TAEVAS LIFE SCIENCES PTY LTD

46 Dora St
Blacktown NSW 2148
Australia

Patrocinador de Nueva Zelanda**REF**

nCommand Lite

TAEVAS LIFE SCIENCES LIMITED

Level 3, 1 Margaret Street
Lower Hutt 5010
New Zealand

UDI-DI BÁSICO: 7898974112NCLITE2L

Solicitud de una copia impresa

Se proporcionarán copias impresas del manual del usuario de nCommand Lite, previa solicitud, sin coste adicional. Póngase en contacto con su representante local y solicite una copia impresa del manual del usuario.

Fecha de fabricación

La fecha de la versión del software se encuentra en la página de inicio de sesión de nCommand Lite, en formato MES/AÑO.

Capítulo 7 Historial de Revisiones

Revisión	Descripción del cambio	Fecha
0	Se actualiza la versión del manual de 2.3 v1 a 2.4	25 de noviembre de 2025
1	Etiquetas del capítulo 6 actualizadas	4 de diciembre de 2025
2	Se eliminó el requisito de una dirección IP estática de la configuración del ordenador local en la subsección 1.3.11 Se actualizó el símbolo del Representante Autorizado en la UE en la subsección 1.3.12 Se ha eliminado la nota del subpunto 1.3.14 Se ha actualizado el contenido del Capítulo 2 Se ha actualizado el símbolo de Representante Autorizado en la UE en el Capítulo 6	28 de enero de 2026
3	Se revisó la traducción de «Técnico Responsable» en el Capítulo 6.	9 de febrero de 2026

APÉNDICE I - Lista de comprobación de inicio del servicio

1. Verifique las conexiones eléctricas y de red:

Asegúrese de que las conexiones eléctricas y los puntos de red estén correctamente establecidos en el ordenador e-KVM, el ordenador del escáner y el ordenador local.

2. Compruebe el estado de la alimentación:

Compruebe que la fuente de alimentación ininterrumpible y estabilizada y el ordenador e-KVM estén encendidos y funcionen correctamente.

3. Acceso rápido a la plataforma nC Lite:

Confirme la presencia del acceso directo a la plataforma nC Lite en el escritorio para un acceso rápido.

4. Acceso e inicio de sesión en la plataforma nC Lite:

Abra la plataforma nCommand e inicie sesión para garantizar un acceso completo y una funcionalidad adecuada.

5. Configuración de la aplicación de chat:

Abra la aplicación de chat dentro de la plataforma nC Lite en una sola pestaña y evite minimizarla para una comunicación sin problemas.