# Ciberseguridad de la red sanitaria en la era de la transformación digital

Incluye una entrevista especial con Silvia Piai, Directora de investigación de IDC Health Insights

IDC ANALYZE THE FUTURE

Folleto

Alcatel·Lucent Enterprise

# Resumen ejecutivo

La ciberseguridad es, desde hace tiempo, una prioridad clave para las organizaciones sanitarias. Sin embargo, las necesidades de ciberseguridad están cambiando debido a la transformación digital que se está produciendo. La transformación digital significa que las organizaciones sanitarias tienen más equipos conectados y equipos móviles en sus redes, mientras que los profesionales clínicos, partners y médicos de consulta acceden cada vez más a aplicaciones y datos de fuera de la red. A medida que el cambio se acelera, los antiguos métodos de seguridad de la red se están quedando obsoletos.

En este documento, Silvia Piai, Directora de Investigación de International Data Corporation (IDC), comparte sus ideas sobre las fuerzas que están cambiando los requisitos actuales de la ciberseguridad en la atención sanitaria y recomienda estrategias que las organizaciones sanitarias pueden adoptar y tecnologías que pueden desplegar para mantener los datos y sistemas seguros en la era de la transformación digital. Alcatel-Lucent Enterprise compartirá cómo su solución Digital Age Networking (DAN) satisface las demandas de una empresa transformada digitalmente. Con un enfoque multifacético de la ciberseguridad, DAN mantiene la confianza con un acceso seguro y basado en políticas a los dispositivos médicos conectados, los datos de los pacientes y las aplicaciones de software en todo el ecosistema sanitario.

# Situación actual de la ciberseguridad en la sanidad

Las organizaciones sanitarias invirtieron **5 500 millones de dólares a nivel mundial** en ciberseguridad durante el año 2019.

En una encuesta posterior a otra realizada por IDC, las organizaciones sanitarias afirman que la ciberseguridad es una prioridad absoluta.[1] Esto no es sorprendente. La sanidad ha sido, y sigue siendo, uno de los sectores más atacados por los hackers. Y el problema sigue creciendo. En 2018, el sector de la asistencia sanitaria vio comprometidas 15 millones de historias clínicas de pacientes en 503 infracciones, tres veces más que en 2017, según el barómetro de infracciones de Protenus [2]

Las filtraciones se producen porque los datos sanitarios son extremadamente valiosos. Los expedientes individuales de los pacientes contienen todo, incluido el nombre, las direcciones actuales y anteriores, el historial laboral, los nombres y las edades de los familiares de la persona y la información financiera, como las tarjetas de crédito y los números bancarios.[3]

Las brechas de ciberseguridad no solo derivan en el robo de datos. También pueden dar lugar a interrupciones operativas, daños a la reputación del hospital y multas por violaciones de normativas como la Ley de Transferibilidad y Responsabilidad del Seguro Sanitario (HIPAA) en Estados Unidos y el Reglamento General de Protección de Datos (RGPD) en la Unión Europea. Una situación aún peor es la posibilidad de que los pacientes sufran daños. Por ejemplo, una bomba puede suministrar una cantidad incorrecta de insulina. O puede que la información no se entregue al médico mientras está tratando al paciente, por lo que no sabrá las alergias que tiene el paciente o si está tomando otros medicamentos.

IDC estima que las organizaciones sanitarias invirtieron 5 500 millones de dólares a nivel mundial en ciberseguridad en 2019 para mitigar estos riesgos. Desde hoy y hasta 2022, IDC proyecta un crecimiento anual compuesto del gasto en ciberseguridad en la sanidad del 8,7 %, una cantidad similar a la de otros sectores.[4]

A pesar de estas inversiones, la ciberseguridad en la sanidad sigue presentando carencias desde hace mucho tiempo. Aunque muchas organizaciones dicen que la ciberseguridad es una prioridad, a menudo sigue siendo una idea tardía en la práctica diaria. Al fin y al cabo, los profesionales clínicos se dedican a curar a las personas, no a pensar en la ciberseguridad. Además, los profesionales clínicos pueden resistirse activamente a los esfuerzos por imponer la ciberseguridad si ésta obstaculiza los flujos de trabajo clínicos. Por ejemplo, si los médicos, las enfermeras y los profesionales clínicos tienen que dedicar mucho tiempo a autenticarse para acceder a la historia clínica electrónica o al sistema de registro sanitario (EMR/EHR), buscarán atajos para ahorrar un tiempo que les es muy preciado. Además, muchos profesionales clínicos simplemente no son lo suficientemente conscientes de las amenazas y los impactos de la ciberseguridad.

1 Por ejemplo: Prioridades, estrategias e inversiones: superar los retos de la DX en la sanidad europea https://www.idc.com/getdoc.jsp?containerId=EMEA44355219

2 https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2019-so-far

3 https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#2bb1f96b50cf

4 Guía Semestral de gasto en seguridad de IDC a nivel mundial https://www.idc.com/getdoc.jsp?containerId=IDC_P33461

# Cambios en las amenazas de ciberseguridad

Al mismo tiempo, la naturaleza de las amenazas a la ciberseguridad está cambiando. Los hackers están utilizando la inteligencia artificial (IA) y el aprendizaje automático (ML, Machine Learning) para crear ataques más sofisticados y automatizados. Las nuevas técnicas de ingeniería social permiten a los delincuentes conectar las rutas de información encontradas en las redes sociales para crear muy buenos perfiles de las personas o de los datos que poseen las organizaciones sanitarias.

La transformación digital en el sector sanitario está cambiando aún más los requisitos de ciberseguridad, lo que resulta en una mayor complejidad, un mayor uso de dispositivos conectados y un perímetro que está desapareciendo, todo ello a un ritmo acelerado.

## Mayor complejidad

Las organizaciones sanitarias están adoptando nuevas tecnologías, como la nube, el móvil, la IoT, el Big Data y la analítica avanzada. Estas nuevas soluciones aportan un nuevo nivel de complejidad que requiere una nueva forma de ver la seguridad.

## Aumento del uso de dispositivos conectados

En 2022, el 97 % de las enfermeras de cabecera, el 98 % de los médicos, el 96 % de los farmacéuticos y el 94 % de las enfermeras de urgencias utilizarán dispositivos móviles.[5] A medida que las organizaciones sanitarias y los pacientes utilizan cada vez más dispositivos móviles, de IoT y de salud en el hogar, como los Fitbits, han surgido nuevas vulnerabilidades.

Por ejemplo, la primera generación de dispositivos médicos conectados no requería contraseñas. Como estos dispositivos estaban conectados a la red, los hackers podían utilizarlos como puerta de entrada a la red. En la actualidad, la FDA (organismo de EE.UU. sobre alimentos y medicamentos) y sus equivalentes europeos como la Agencia Europea del Medicamento exigen elementos de seguridad como las contraseñas codificadas. Sin embargo, las infracciones siguen siendo

Para 2022, el 97 % de las enfermeras de planta, el 98 % de los médicos, el 96 % de los farmacéuticos y el 94 % de las enfermeras de emergencias estarán utilizando dispositivos móviles

5 https://www.aiin.healthcare/topics/connected-care/over-90-nurses-physicians-will-use-mobile-devices-2022

inevitables y, cuando se producen, los hackers pueden acceder a toda la red. La investigación de IDC muestra que solo el 6 % de los proveedores de servicios sanitarios europeos tienen una estrategia de seguridad para dispositivos médicos conectados integrada en su arquitectura de seguridad empresarial y, lo que es más preocupante, el 16 % aún no ha empezado a evaluar las posibles amenazas a los dispositivos médicos conectados en red.[6] De hecho, los ponentes de la quinta conferencia sobre seguridad en la sanidad electrónica de la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) estimaron que se ha producido un aumento del 600 % en los ataques a los dispositivos de IoT, concretamente a los dispositivos médicos.[7]

Únicamente el 6 % de los proveedores de servicios sanitarios europeos cuentan con una estrategia de seguridad para los dispositivos médicos conectados.

## El perímetro está desapareciendo

Durante mucho tiempo, la mayoría de las organizaciones han delimitado claramente tanto los usuarios como los recursos dentro y fuera de la red.

Sin embargo, a medida que las organizaciones sanitarias adoptan la transformación digital, se abren más a los intercambios con el ecosistema más amplio, incluidos los pacientes, los socios, los pagadores, las autoridades sanitarias gubernamentales y otros proveedores en un entorno de atención integrada/colaborativa. Los usuarios acceden a los recursos desde el perímetro de la red y pueden estar en cualquier lugar. Los cirujanos podrían intercambiar información con los médicos de atención primaria de otra red. Los hospitales podrían controlar a los pacientes a distancia tras el alta hospitalaria. Los médicos podrían utilizar los datos de los dispositivos sanitarios personales de los pacientes para ayudar en el diagnóstico y la atención.

Además, los recursos informáticos ya no se limitan al interior del perímetro. Están en las instalaciones y en la nube y se conectan a través de las API. Las organizaciones sanitarias necesitan formas modernas de proteger los recursos cuando el perímetro deja de existir.

## Aceleración del ritmo de cambio

En un mundo transformado digitalmente, todo se mueve más rápido. Las herramientas de seguridad deben ser capaces de soportar esta velocidad.

6 Seguridad de IoT en la sanidad europea https://www.idc.com/getdoc.jsp?containerId=EUR145549919

7 https://www.enisa.europa.eu/events/5th-ehealth-security-conference

## Entrevista con Silvia Piai, Directora de investigación de IDC Health Insight

Recientemente, Alcatel-Lucent Enterprise tuvo la oportunidad de hablar con Silvia Piai, Directora de investigación de IDC Health Insights, para conocer la opinión y las recomendaciones de IDC sobre la ciberseguridad en el sector sanitario.

# Recomendaciones de IDC para mejorar la ciberseguridad en la sanidad

A pesar de los nuevos retos, el enfoque de la seguridad en el sector sanitario sigue siendo tradicional. Las organizaciones sanitarias a menudo implementan la seguridad simplemente para marcar las casillas de cumplimiento y no tienen en cuenta los cambios debidos a la transformación digital que afectan a los requisitos de seguridad.

IDC recomienda que las organizaciones sanitarias adopten un enfoque holístico de la seguridad de la red que incluya la estrategia, la tecnología, el personal (por ejemplo, la formación) y los procesos (por ejemplo, cómo se integra la seguridad en los flujos de trabajo). En este documento, examinaremos la estrategia y la tecnología.

## Estrategia

En lugar de implementar la ciberseguridad mínima para lograr el cumplimiento de la normativa, las organizaciones sanitarias deberían aprovechar la oportunidad para desarrollar un plan de seguridad estratégico que gestione el riesgo de tal manera que cumpla con las exigencias del contexto de transformación digital actual. Deberían:

- **Pensar en el cumplimiento de la normativa como punto de partida.** Mientras que muchas organizaciones empiezan haciendo lo mínimo necesario para cumplir con el RGPD, u otras regulaciones equivalentes fuera de Europa, las organizaciones sanitarias deben pensar en el cumplimiento de la normativa como un punto de partida, así, reconsiderar la forma en que están gestionando y gobernando los datos dentro de sus organizaciones y con sus socios.
- **Entender que la seguridad impulsa el valor del negocio** al garantizar la continuidad del mismo. Las organizaciones sanitarias deben evitar la pérdida de ingresos (y reducir los problemas de seguridad de los pacientes) que suponen los ciberataques que hacen caer los sistemas informáticos. Alinee la seguridad con sus objetivos empresariales más amplios y conviértala en parte de su actividad diaria.

- **Seguir un enfoque de seguridad por diseño.** El riesgo acompaña los flujos de trabajo empresariales, que evolucionan constantemente junto con las tecnologías. Las organizaciones sanitarias deben incorporar la seguridad a los flujos de trabajo desde el principio. La seguridad debe ser un valor empresarial fundamental y complementar todas las decisiones empresariales de las organizaciones sanitarias.
- **Trabajar con el ecosistema.** Las organizaciones sanitarias ya no tienen un perímetro claro que defender cuando integran la atención sanitaria de otras organizaciones para sus pacientes y socios. Deben trabajar con el ecosistema para mantener la ciberseguridad.

## Tecnología

La creación de un ecosistema conectado seguro es fundamental a medida que las organizaciones sanitarias transforman digitalmente sus operaciones. Este ecosistema requiere un enfoque por capas que sitúe las cuatro disciplinas fundamentales de la seguridad (gestión de la identidad, gestión de la vulnerabilidad, gestión de las amenazas y gestión de la confianza) en una nueva dimensión que permita la escalabilidad, la velocidad, la inteligencia y la automatización. Este enfoque debe estar en consonancia con el entorno digital más amplio de la empresa y con los resultados que la organización desea conseguir.

Los aspectos clave de la tecnología de seguridad de la red en capas deben incluir:

- **Seguridad de los extremos**: para gestionar las vulnerabilidades de los dispositivos individuales.
- **Gestión de identidades**: para autenticar a los usuarios y controlar el acceso. La solución debe proporcionar capacidades de autenticación de usuarios y políticas de seguridad detalladas que concedan a los usuarios el nivel adecuado de acceso únicamente a la información que necesitan.

- **Intercambio seguro de datos**: el uso de protocolos de encriptación e intercambio seguro de archivos debe salvaguardar los datos en movimiento.
- **Contenerización**: para evitar que las amenazas salten de un sistema a otro una vez que la amenaza haya accedido a la red, la solución debe utilizar la contenerización y la segmentación de la red para aislar los sistemas individuales.
- **Gestión de la confianza**: las organizaciones sanitarias necesitan un enfoque de gestión de riesgos que contemple el hecho de que los usuarios y los recursos pueden ubicarse fuera del perímetro de la red. Una forma de establecer la confianza en un entorno de este tipo es entender qué constituye un comportamiento normal y anormal en la red. Las herramientas habilitadas por la inteligencia artificial (IA) para la gestión de la identidad y la autorización le permiten establecer una línea de base normal para el comportamiento en la red. Estas herramientas pueden evaluar cada usuario y dispositivo, así como sus requisitos de aplicación, seguridad y calidad de servicio para establecer un comportamiento de referencia normal. A partir de entonces, la IA puede identificar rápidamente cualquier acontecimiento o acción inusual, como un sistema de vigilancia que intervenga en un RME o HCE, y los análisis que ayuden a determinar por qué ha cambiado algo.
- **Una arquitectura definida por software**: una solución de gestión de red automatizada puede proporcionar la velocidad necesaria para seguir el ritmo de la transformación digital.

# La solución de Alcatel-Lucent Enterprise

La solución Digital Age Networking de Alcatel-Lucent Enterprise es un enfoque polifacético de la ciberseguridad para redes sanitarias que proporciona seguridad exhaustiva a los dispositivos y aplicaciones conectados del sector sanitario a través de múltiples capas de seguridad.

## Conectividad flexible a través de una Service Defined Network

Nuestro enfoque comienza con una Service Defined Network, una red definida por servicios flexible que agiliza y facilita la configuración de las políticas de red y de ciberseguridad para el gran número de usuarios, dispositivos y aplicaciones conectados que alimentan la transformación digital.

En el pasado, la TI ha sido una operación de romper y arreglar. El departamento de TI instalaba nuevos equipos, los ponía en marcha y gestionaba la red mediante tediosos procesos manuales. Una DAN es una red inteligente y automatizada que facilita la conexión de los usuarios y los dispositivos a sus aplicaciones específicas de manera segura. Construida con la tecnología Alcatel-Lucent Enterprise Intelligent Fabric (iFab), DAN incluye nuestro Intelligent Fabric de fabricación propia combinado con la conexión de ruta más corta (SPB) estándar del sector. En combinación, estas tecnologías simplifican la creación y la configuración de las redes, al tiempo que permiten el enrutamiento multirruta y la adición de enlaces para combinar varias conexiones de red en paralelo y, de este modo, aumentar el rendimiento y proporcionar redundancia.

Con la estrategia de ALE, los equipos de TI definen los servicios de red, la arquitectura, las políticas de acceso y los contenedores de IoT, y la red se construye automáticamente. Una vez diseñada la red, si se mueve, cambia o añade algo, entonces la red realiza los ajustes necesarios de forma automática e indetectable. Por ejemplo, si un conmutador está fuera de servicio, la red se redirige automáticamente alrededor de ese conmutador.

Al utilizar una red definida por servicios, las organizaciones sanitarias se benefician de una automatización que reduce los errores de configuración manual y les ayuda a seguir el ritmo acelerado de los cambios que se dan en sus organizaciones. Dado que la automatización elimina el trabajo manual, las TI se convierten en un motor del negocio.

## Control de acceso integral mediante políticas inteligentes y automatizadas

Las organizaciones sanitarias pueden utilizar ALE DAN para definir las normas y políticas de acceso de los usuarios que determinan las aplicaciones y los dispositivos que los usuarios pueden utilizar y a los que pueden acceder; asimismo, pueden utilizar esta solución para seguir a los usuarios dondequiera que vayan. Por ejemplo, pueden establecer políticas que proporcionen:

- Acceso de los médicos a todos los sistemas, excepto los financieros
- Acceso de los pacientes a los servicios de Internet
- Una política basada en los contratistas a las empresas de ciencias de la vida u otros socios

ALE también ofrece servicios basados en la ubicación, como la orientación en interiores, el seguimiento de bienes y personas, que permite a las organizaciones sanitarias establecer políticas que tengan en cuenta la ubicación del usuario.

Las funciones de gestión de políticas unificadas aplican las políticas automáticamente cada vez que un usuario se conecta, garantizando que los usuarios solamente tengan los privilegios de acceso permitidos. Una vez que los usuarios se conectan a la red con un PC/portátil/dispositivo móvil y se validan sus credenciales, no necesitan seguir autenticándose. Permanecen conectados si el dispositivo está encendido y el sistema aplica automáticamente la política para ese usuario.

Las políticas garantizan que todos los usuarios, dentro o fuera de la organización, tengan acceso exclusivamente a las áreas permitidas y que estos controles de acceso se apliquen de forma coherente. También simplifican los flujos de trabajo de los hospitales al tiempo que refuerzan la ciberseguridad. Los profesionales clínicos pueden acceder rápidamente a los sistemas y a la información que necesitan para atender a los pacientes sin necesidad de realizar costosos procedimientos de acceso a la seguridad.

## Reducción de la vulnerabilidad mediante la contenerización y la segmentación

Las organizaciones sanitarias utilizan muchos dispositivos IoT, como máquinas de resonancia magnética, monitores de pacientes, bombas de infusión, robots dispensadores de recetas, así como cámaras de vídeo, sistemas de climatización, sistemas de rociadores, sistemas de detección de intrusos y muchos otros. La solución

Alcatel-Lucent Enterprise DAN permite a las organizaciones sanitarias contener cada dispositivo, creando un segmento de red virtual con el fin de evitar que cualquier dispositivo se convierta en un vector de ataque. La contenerización dentro de DAN hace que haya múltiples redes virtuales a partir de una única red física, que es administrada por un único sistema de gestión.

La contenerización es fácil de implementar para los equipos de TI. La solución DAN detecta de manera automática cada dispositivo de la red. Cuando un dispositivo se conecta a la red, el sistema de gestión de redes Alcatel-Lucent OmniVista® 2500, disponible en las instalaciones o en la nube, intenta identificar ese dispositivo. Si el sistema de gestión no tiene el dispositivo en su base de datos, consultará una base de datos en la nube con más de 17 millones de dispositivos.

Una vez identificado el dispositivo, el sistema lo clasificará, por ejemplo, como una cámara de seguridad. Si ese dispositivo está en la lista de proveedores aprobados para cámaras de seguridad, se conectará a la red. De lo contrario, no se conectará. A continuación, la solución se instala en un contenedor virtual para el dispositivo, segmentándolo del resto de la red. Si alguien ataca cualquier dispositivo conectado a la red, ese atacante no podrá utilizar ese dispositivo para acceder al resto de la red.

## Mejora de la confianza mediante inteligencia artificial

Una vez que los dispositivos están conectados, deben ser supervisados continuamente para identificar cualquier amenaza y mantener la confianza. El análisis y la visibilidad de la aplicación de ALE permiten que los administradores de la red vean lo que está pasando en la red para cada dispositivo. El análisis identifica patrones de comportamiento normales y esperados de la red, así como cualquier patrón atípico cuando surge. Podemos observar el comportamiento de las aplicaciones en el límite de la red para decidir si nos conectamos a esa aplicación, así como un comportamiento inusual en las aplicaciones permitidas, como una cámara de vídeo que está generando más datos de los que debería.

Si se produce una anomalía o un comportamiento inusual en el dispositivo, los análisis lo mostrarán para que el gestor de seguridad de la red pueda intervenir. Actualmente, la investigación debe realizarse de forma manual, pero ALE está trabajando en la automatización de la respuesta utilizando la inteligencia artificial y el aprendizaje automático.

Las capacidades de la IA también apoyan los servicios remotos para pacientes. ALE está desarrollando equipos que permiten a los hospitales controlar de manera remota a los pacientes mientras están en su casa recuperándose de una dolencia o

una operación. El equipo debe comunicar de forma segura los datos del dispositivo al hospital. La IA puede supervisar la actividad de los dispositivos IoT remotos para garantizar que su comportamiento es coherente con el esperado. Además, los pacientes utilizan cada vez más aplicaciones para controlar su salud. Si un profesional clínico puede supervisar un Apple Watch® u otro dispositivo de monitorización que lleve un paciente, puede mejorar el compromiso del paciente y realizar mejores diagnósticos. Con Alcatel-Lucent Enterprise IA, las organizaciones sanitarias tendrán visibilidad para saber si una aplicación o actividad dentro de ella es de confianza.

## Un equipo de red seguro reduce las vulnerabilidades

Hoy en día, las organizaciones sanitarias son conscientes de la necesidad de asegurar los dispositivos de IoT en la red. Sin embargo, no tienen en cuenta los dispositivos que forman la base de la red, como los conmutadores y los puntos de acceso.

ALE emplea muchas tecnologías para reducir la amenaza derivada de esos dispositivos. Nuestras soluciones:

- Reforzar el software del sistema operativo para proporcionar un código seguro y diversificado
- Enviar el software del sistema operativo para la verificación y validación de terceros para corroborar que no tiene puntos de entrada o puertas traseras sencillas
- Asegurar que cada vez que se arranca un conmutador, la memoria se compila y se actualiza de una manera diferente. Aunque los conmutadores funcionan de forma idéntica, no hay dos que tengan la misma configuración de memoria internamente. Si alguien violara uno de nuestros conmutadores, no podría acceder a otro conmutador de la misma manera.
- Proporcionar protección integrada de Denegación de servicio (DoS). Nuestra CPU puede detectar cantidades inusuales de tráfico de red y apagar automáticamente la CPU si es necesario.
- Múltiples certificaciones de seguridad completas, como JDIC y FIPS.
- Realizar actualizaciones continuas del software.

## Conexiones seguras para el tráfico entrante y saliente

Para el tráfico entrante, las funciones VPN de Alcatel-Lucent Enterprise proporcionan una conexión cifrada a la red local, mientras que el tráfico de extremo a extremo está protegido mediante el cifrado MACsec (también conocido como IEEE 802.1AE) para proteger la información a medida que recorre la red; además la capacidad de volver a cargar los servicios, como TKS y HTTPS, sin necesidad de reinicio garantiza que no se interrumpe la red.

### Presentación de informes

La presentación de informes de Alcatel-Lucent Enterprise permite que diferentes personas accedan a información sobre el estado, la situación y el rendimiento de la red, el funcionamiento de las aplicaciones y la satisfacción de los usuarios. Por ejemplo, el equipo de TI puede ver datos sobre el rendimiento y las operaciones de la red. Las unidades del negocio pueden garantizar que los equipos, como los sistemas de imágenes (IRM, rayos X) transmiten datos a los servidores y las tabletas sin ningún problema. Los CXOs pueden determinar si la red está prestando servicios que permiten a los profesionales clínicos pasar más tiempo con los pacientes y si están sacando el máximo provecho de la red.

# Conclusión

La transformación digital está cambiando profundamente las necesidades en ciberseguridad de los hospitales a medida que el número de dispositivos conectados aumenta, el perímetro de la red desaparece y los cambios se siguen produciendo de manera acelerada. La solución Digital Age Networking in para sanidad de Alcatel-Lucent Enterprise mantiene la seguridad de sus activos de TI y de los datos de los pacientes en la actual era de la transformación digital. A través de esta solución, puede gestionar estrechamente el acceso de los usuarios, reducir las vulnerabilidades creadas por los dispositivos IoT, móviles y de red, impedir que la inevitable brecha se convierta en un vector de ataque y comunicarse en todo el ecosistema sanitario desde una posición de confianza.

**Somos Alcatel-Lucent Enterprise.**

Somos ALE. Le ayudamos a conectar a sus pacientes, a su personal y a su ecosistema de atención sanitaria, mediante el uso de una tecnología que funciona en sus instalaciones y fuera de ellas.

**www.al-enterprise.com/es-es/industries/healthcare**

**www.al-enterprise.com/es-es/** El nombre y el logotipo de Alcatel-Lucent son marcas registradas de Nokia que se utilizan bajo licencia por ALE. Para conocer otras marcas registradas utilizadas por las empresas asociadas de ALE Holding, visite: www.al-enterprise.com/en/legal/trademarks-copyright. Todas las demás marcas registradas son propiedad de sus respectivos propietarios. La presente información puede sufrir cambios sin previo aviso. Ni ALE Holding ni ninguna de sus filiales asumen responsabilidad alguna por las posibles inexactitudes del presente contenido. © Copyright 2021 ALE International, ALE USA Inc.
Todos los derechos reservados en todos los países. DID20021001ES (mayo de 2021)

Alcatel·Lucent
Enterprise