ivanti Neurons

Informática Sanitaria, Biomedicina, Seguridad

Guía para mejorar la visibilidad y mitigar los riesgos de seguridad de los productos sanitarios

Contenido

Introducción

Los dispositivos médicos conectados representan un enorme desafío para las organizaciones de TI, biomédicas y de seguridad de la salud. Son totalmente vulnerables a las ciberamenazas y el éxito de los ciberataques puede tener consecuencias terribles, pero las medidas de ciberseguridad tradicionales no pueden aplicarse a estos dispositivos y pueden incluso correr el riesgo de interferir con las operaciones clínicas críticas.

En esta guía recorremos un proceso de tres pasos para ayudar a aumentar la visibilidad de los dispositivos médicos y mejorar la mitigación de los riesgos de seguridad. El establecimiento de capas de ciberseguridad para los dispositivos médicos es un proceso continuo de varias etapas, que puede tener éxito cuando se parte de una base sólida y se adopta un enfoque metódico y sistemático.

Aprenda a descubrir, evaluar y mitigar los riesgos de ciberseguridad asociados a los dispositivos médicos conectados. Las tres fases que presentamos en esta guía no son un proceso único, sino que deben tratarse como un ciclo. Los equipos de TI y de seguridad de los centros sanitarios deben llevar a cabo estas fases de forma continuada, estudiando el entorno, evaluando los riesgos y abordando los problemas de seguridad que descubren día a día.

¿Cuál es la vulnerabilidad de los dispositivos médicos a los ciberataques?

Cada vez existen más dispositivos médicos conectados a redes o a otros dispositivos, lo que crea una importante vulnerabilidad de seguridad para los hospitales y los proveedores de atención sanitaria. Muchos de estos dispositivos no son seguros y no se gestionan activamente, lo que abre la puerta a una amplia gama de amenazas de ciberseguridad.

¿Por qué son vulnerables los dispositivos médicos?

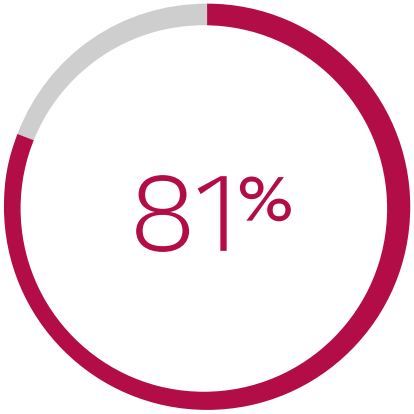
- El código del software no ha sido sometido a una revisión de seguridad.
- La autenticación es débil o inexistente.
- Los canales de transferencia de datos suelen ser inseguros y no están cifrados.
- Visibilidad limitada sobre los dispositivos que se utilizan activamente.
- Imposibilidad de controlar la actividad de los dispositivos y los incidentes de seguridad.
- Los dispositivos retirados no se eliminan de forma segura.
- Las actualizaciones de software no están disponibles, o rara vez se despliegan.

Comprender el entorno
Descubrir qué dispositivos informáticos y médicos existen, clasificarlos con precisión, comprender su contexto clínico e identificar sus necesidades de red.

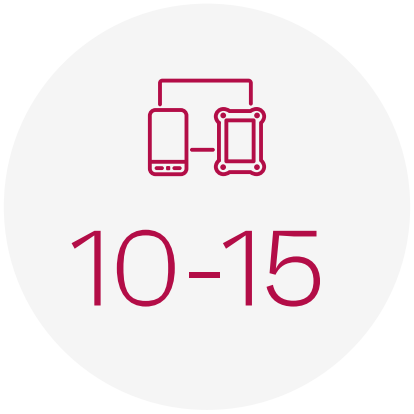
Evaluar los riesgos
Identificar las vulnerabilidades de los dispositivos y los riesgos relacionados con la red, asignando a cada dispositivo un índice de riesgo y proporcionando recomendaciones para su corrección.

Proteger los dispositivos
Abordar la seguridad a nivel de dispositivos, aislando los dispositivos dentro de la LAN y evitando la comunicación no deseada a través de la LAN/WAN, y preparar una estrategia para detectar los incidentes de seguridad cuando se produzcan.

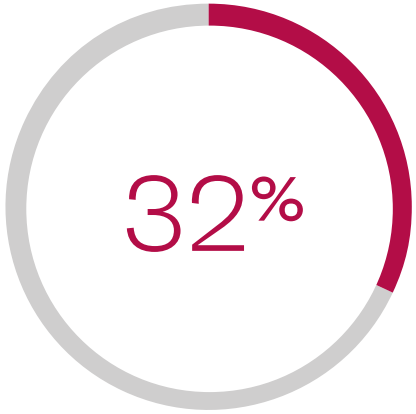
¿Cuál es la magnitud del problema?



El 81 % de las organizaciones sanitarias ha asegurado haber sufrido un ciberataque en los últimos dos años.



Los hospitales mantienen entre 10 y 15 dispositivos médicos conectados por cama, con más de 3,7 millones de dispositivos en uso activo.



El 32 % de las organizaciones sanitarias asegura que los dispositivos médicos son su principal preocupación en materia de seguridad.

Fuente: KPMG, Wired

¿Qué vectores de amenaza afectan a los dispositivos médicos?

Programas malignos
Los dispositivos médicos no suelen tener protección de punto final y son especialmente vulnerables a los programas malignos.

Amenazas internas
Debido a la debilidad de la autenticación, las personas malintencionadas pueden obtener fácilmente un acceso no autorizado y manipular los dispositivos.

Ataques a aplicaciones web
Algunos dispositivos médicos se pueden gestionar a través de una interfaz web, lo que crea una serie de riesgos cibernéticos como la inyección de código, la secuencia de comandos en sitios cruzados (XSS por sus siglas en inglés) y el cruce de directorio.

Uso indebido del dispositivo
Los dispositivos médicos conectados se basan a menudo en PC con Windows. El personal del hospital puede utilizar las máquinas para navegar en la red o instalar un software, creando un riesgo adicional.

¿Cómo se puede evaluar el riesgo de ciberseguridad y el impacto de un ataque?

Las directrices de la FDA para los productos sanitarios ofrecen una útil clasificación de los niveles de riesgo de los productos.

Nivel 1: Mayor riesgo de ciberseguridad	Nivel 2: Riesgo de ciberseguridad estándar
El dispositivo es:	**El dispositivo es:**
Capaz de conectarse a otro producto médico o no médico, a una red o a Internet O Un incidente de ciberseguridad que afecte al dispositivo podría perjudicar directamente a uno o más pacientes.	Capaz de conectarse a otro dispositivo o red, pero no puede perjudicar directamente a los pacientes O Capaz de dañar directamente a los pacientes pero no puede conectarse a una red.

Para obtener una evaluación más detallada del riesgo, utilice un marco como el cálculo de riesgo CVSS. Teniendo en cuenta los siguientes factores al evaluar el riesgo de ciberseguridad:

- Vulnerabilidades del software
- Seguridad del paciente
- Autenticación
- Privacidad
- Red de contactos
- Interrupción del servicio

Fase I:

Comprender el entorno de los dispositivos conectados

El primer paso para resolver un problema es reconocer que existe y comprender su alcance. El problema de los dispositivos médicos conectados no es bien comprendido por los equipos de TI, biomédicos y de seguridad de los hospitales y organizaciones sanitarias debido a su visibilidad extremadamente limitada.

Los equipos de seguridad ven los dispositivos médicos como cajas negras, o no los ven en absoluto

La seguridad de los dispositivos médicos se está convirtiendo en una responsabilidad compartida por los equipos de ingeniería clínica y los departamentos de TI. Aunque la información sobre estos dispositivos existe en las organizaciones sanitarias, los equipos de seguridad no pueden acceder a ella fácilmente.

Las siguientes preguntas importantes quedan sin respuesta:

1. ¿Cuántos dispositivos hay conectados?
2. ¿De qué tipo de dispositivos se trata?
3. ¿Con qué otros dispositivos o redes se comunican?
4. ¿El comportamiento de la red es normal y esperado o irregular?

¿Por qué es difícil crear un inventario de dispositivos médicos conectados?

Simplemente realizar un escaneo de la red e identificar los dispositivos médicos como se haría en una red de TI normal no es posible:

- Los dispositivos son sensibles: la exploración activa de la red puede interrumpir el funcionamiento de los dispositivos médicos, por lo que debe utilizar la detección pasiva.
- Invisible para las herramientas de detección de redes: las herramientas tradicionales no descubrirán la gran mayoría de los dispositivos médicos conectados, o pueden indicar falsamente que el dispositivo es una estación de trabajo de Windows. La mayoría de los dispositivos médicos conectados no anuncian su información y detectarlos a través de la red requiere un cuidadoso análisis del tráfico en la capa de aplicación.
- Gran número y variedad de dispositivos: puede haber decenas de miles de dispositivos de diferentes tipos, proveedores y versiones.
- Flujo continuo: los dispositivos se añaden, sustituyen o eliminan constantemente de la red, a menudo sin la participación del departamento de TI, por lo que la detección y el inventario deben ser un proceso continuo.

Paso 1. Detección

Procure crear una base de datos de dispositivos médicos con datos sobre cada uno de ellos. Céntrese en datos de alta calidad que puedan ayudarle a determinar los riesgos y las vulnerabilidades. En particular:

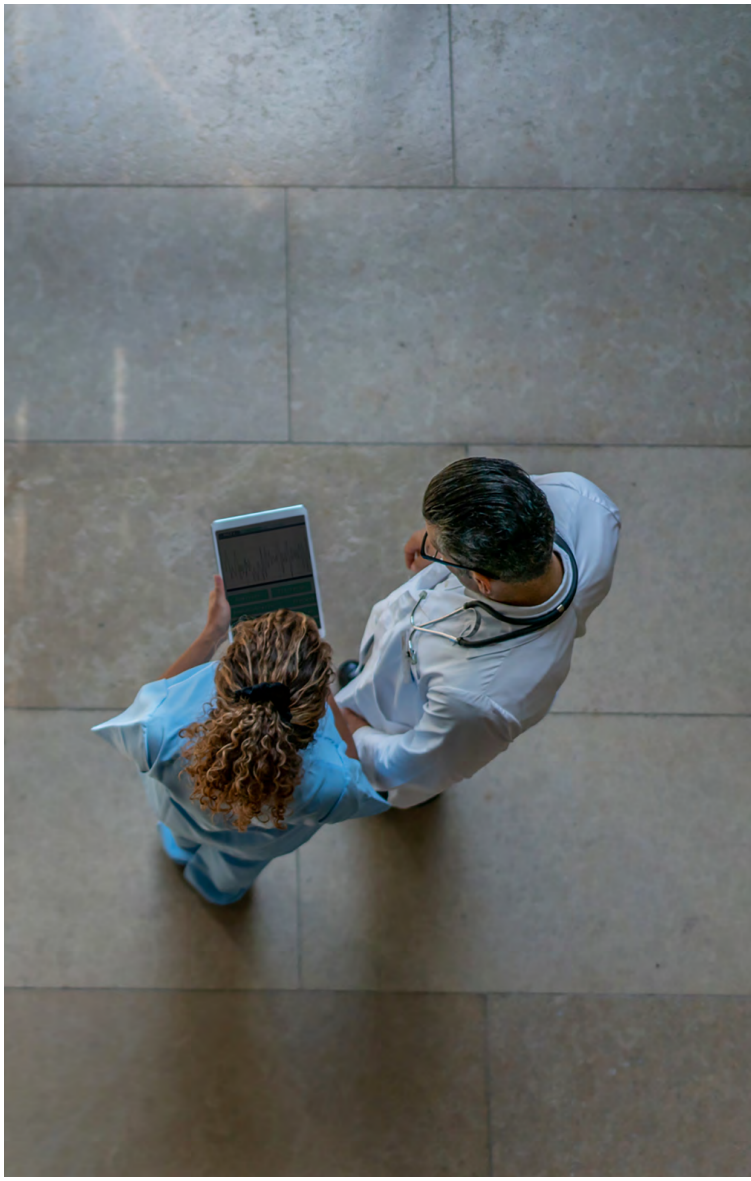
- Tipo de dispositivo
- Departamento y sala
- Proveedor
- Modelo
- Dirección IP
- Sistema operativo
- Versión del software de aplicación
- Último parche de seguridad

Paso 2. Mapa de la red y contexto clínico

Comprender el comportamiento de la red de un dispositivo le permite visibilizar cómo está expuesto a las amenazas externas e internas. Procure obtener la siguiente información para cada uno de sus dispositivos conectados:

- ¿Con qué otros dispositivos se comunica?
- ¿Tiene este dispositivo acceso innecesario a otros dispositivos, redes o Internet?
- ¿La comunicación de red de este dispositivo está aislada en una VLAN?
- ¿Qué tipos de protocolos se llevan a cabo?
- ¿Dónde envía o recibe el dispositivo los datos de la información de salud pública (PHI) y qué tipo de PHI?
- ¿Se comunica externamente a través de Internet?
- ¿Es necesario que el dispositivo se comunique con el proveedor del mismo de forma continua?
- ¿Son habituales las comunicaciones por Internet para este tipo de dispositivos?
- ¿La comunicación por Internet de este dispositivo está aislada en un túnel VPN?

Definir el uso clínico de cada dispositivo y, por consiguiente, su exposición a los riesgos. Estos datos pueden ser extremadamente difíciles de obtener sin la ayuda de herramientas automatizadas.



Fase II:

Evaluar los riesgos

En cuanto conozca mejor sus dispositivos médicos conectados y haya elaborado un inventario de los dispositivos, su contexto y su comportamiento en la red, podrá utilizar este inventario para evaluar los riesgos que afectan a cada dispositivo y su impacto en la organización.

Paso 1. Identificar las vulnerabilidades de los dispositivos y las oportunidades de corrección

Recopile datos sobre las vulnerabilidades de cada uno de sus modelos de dispositivos, sistemas operativos y versiones de aplicaciones. Igual de importante es descubrir al propietario del dispositivo y su nivel de acceso para solucionar los problemas de seguridad.

Impacto de las vulnerabilidades del software
Utilice el cálculo de riesgo CVSS para identificar el impacto de las vulnerabilidades de software conocidas en sus dispositivos conectados.

Desconfiguración
Compruebe si hay vulnerabilidades generales, como contraseñas codificadas o por defecto, sistemas operativos o software sin parches.

Punto de contacto
¿Quién gestiona el dispositivo: la ingeniería clínica, la informática, el fabricante o un contratista externo?

Facilidad de acceso
¿Tiene el equipo de seguridad acceso a este dispositivo para aplicar controles de seguridad o responder a incidentes?

Autenticación de dispositivos
Identifique si el dispositivo dispone de autenticación y, en caso afirmativo, su grado de solidez y si se han establecido contraseñas seguras.

Copia de seguridad
¿Tiene el dispositivo copia de seguridad o redundancia, y cuál es el impacto de la interrupción del servicio?

Paso 2. Identificar los riesgos a nivel de red

Medical device vulnerabilities are only one aspect of the risk. Analyze network connectivity and identify vectors by which attackers can connect to your devices.

Conexión a Internet
Compruebe si el dispositivo se conecta a otros sistemas a través de Internet, por ejemplo a una empresa externa o al fabricante para el mantenimiento o las actualizaciones.

Conexiones a dispositivos menos seguros
Compruebe si el dispositivo puede conectarse a un dispositivo o punto final menos seguro, como la estación de trabajo de un médico, y si expone servicios de gestión o datos como FTP o SSH.

Codificación
Compruebe si el dispositivo transmite o recibe flujos de datos sin cifrar.

Protocolos no seguros
Compruebe si el dispositivo utiliza protocolos que ofrecen una autenticación débil, ninguna autenticación o tienen vulnerabilidades.

Paso 3. Identificar la gravedad del riesgo

Pregúntese: ¿Cuál sería el impacto de un ciberataque con éxito en cada uno de sus dispositivos? A diferencia de los ataques a los sistemas informáticos sanitarios, el impacto de un ataque a los dispositivos conectados no se limita a la seguridad y la privacidad de los datos. Un ciberataque exitoso podría interrumpir la atención clínica y causar daños directos a los pacientes.

Recomendamos identificar la gravedad del riesgo según las tres métricas de impacto en el cálculo del riesgo CVSS:

- Confidencialidad: corresponde al riesgo de exposición de la información sanitaria protegida (PHI) almacenada o transmitida por el dispositivo.
- Integridad: corresponde al riesgo para la seguridad del paciente en el caso de los dispositivos utilizados directamente en la atención al paciente.
- Disponibilidad: corresponde al riesgo de interrupción del servicio.

Seguridad del paciente	Privacidad	Interrupción del servicio
BAJO: Dispositivo médico de clase I de la FDA, riesgo de nivel bajo a moderado para el paciente o el usuario.	**BAJA:** El dispositivo no almacena PHI.	**BAJA:** El fallo del dispositivo no puede interrumpir la atención al paciente.
MEDIO: Dispositivo médico de clase II de la FDA, riesgo de nivel moderado a alto.	**MEDIO:** El dispositivo almacena una pequeña cantidad de PHI durante un período de tiempo limitado en torno a una prueba o tratamiento.	**MEDIO:** El fallo del dispositivo puede interrumpir la atención al paciente, pero no el tratamiento médico crítico.
ALTO: Dispositivo de clase III de la FDA, riesgo nivel alto, dispositivos que mantienen o apoyan la vida, se implantan o presentan un alto riesgo de enfermedad o lesión.	**ALTO:** El dispositivo almacena grandes cantidades de PHI durante varias pruebas o tratamientos.	**ALTO:** El fallo de un dispositivo puede interrumpir un tratamiento médico crítico, como una intervención quirúrgica, un equipo respiratorio o la administración de medicación de mantenimiento de la vida.

Fase III:

Roteger los dispositivos médicos conectados

La ventaja de nuestro proceso estructurado de descubrimiento y evaluación de riesgos se halla en la capacidad de clasificar los dispositivos en función de los riesgos que representan. Cada dispositivo debe tener una puntuación de impacto de riesgo (para la seguridad del paciente, la privacidad y la interrupción del servicio).

Su organización puede definir un nivel de riesgo aceptable. El equipo de seguridad puede centrarse en la protección de los dispositivos cuya puntuación de riesgo esté por encima del nivel aceptable y puede aplicar las medidas de seguridad adecuadas a los dispositivos con diferentes puntuaciones de riesgo.

Aconsejamos proteger los dispositivos médicos conectados en cuatro pasos:

1. Protección de la capa del dispositivo: parches, desactivación de servicios vulnerables, adopción de las mejores prácticas de configuración.
2. Protección de la capa de red: aislamiento a nivel de LAN, bloqueando la comunicación innecesaria dentro de la red local, y aislamiento a nivel de WAN, permitiendo que el dispositivo se comunique sólo con entidades externas conocidas.
3. Detección de incidentes: contar con una estrategia para detectar incidentes de seguridad cuando se produzcan.
4. Métricas y análisis: análisis continuo de los resultados del programa de seguridad, ajustes y mejoras.

Paso 1. Protección de los dispositivos

Al igual que con cualquier dispositivo informático, debe asegurarse de que los dispositivos médicos conectados tengan los últimos parches de seguridad y actualizaciones de software. La configuración debe solidificarse para permitir una autenticación segura. Cierre los puertos no utilizados, limite las funciones innecesarias y, en general, reduzca la superficie de ataque.

La mayoría de los dispositivos médicos funcionan con un sistema operativo Windows. Sin embargo, aplicar un parche no es tan sencillo como con una estación de trabajo o un servidor Windows.

Desafíos del endurecimiento de los dispositivos médicos

- Los parches de seguridad de Windows deben ser verificados y aprobados por el fabricante del dispositivo.
- La ingeniería clínica debe verificar los parches o actualizaciones que no afecten a la funcionalidad del producto sanitario.

Normas

- No conseguir desplegar todos los parches de seguridad ni endurecer todos los dispositivos.
- Centrarse en los dispositivos que tienen una puntuación de alto riesgo.
- Dar prioridad a los parches de seguridad o a los cambios de configuración que abordan las vulnerabilidades conocidas que identificó en su evaluación de riesgos.

Paso 2. Aislamiento de la red

Una estrategia clave para asegurar los dispositivos médicos conectados es aislarlos, en la medida de lo posible, de la comunicación clínica no crítica, para limitar la superficie de ataque. Esto tiene dos componentes:

- Definir la segmentación de la red para garantizar que los dispositivos médicos conectados sólo puedan comunicarse con los dispositivos o sistemas que forman parte de su proceso clínico.
- Bloqueo de la comunicación externa para garantizar que los dispositivos médicos conectados nunca se conecten a Internet, a menos que sea necesario para comunicarse con el proveedor del dispositivo u otras entidades conocidas.

Consideraciones a la hora de aislar los productos sanitarios

- Aislar los flujos de datos clínicos de los no clínicos.
- La comunicación clínica es esencial, pero cualquier otra comunicación debe ser bloqueada.

Normas

- Establecer políticas de acceso estrictas y una segmentación de la red para restringir la comunicación no esencial hacia/desde los dispositivos.
- Establecer una política de segmentación para abordar los riesgos y vulnerabilidades descubiertos en su análisis de impacto.
- Bloquear la conexión del dispositivo a Internet a menos que sea absolutamente necesario para su funcionamiento, y sólo a entidades conocidas.
- Cooperar estrechamente con la ingeniería clínica y la gestión de la tecnología sanitaria (HTM) para garantizar que no se interrumpen los flujos de datos críticos.

Paso 3. Detección y respuesta a incidentes

Es imposible proteger la mayoría de los dispositivos médicos conectados de todas las amenazas potenciales porque siempre habrá dispositivos críticos heredados que no pueden ser reemplazados y no pueden ser completamente parcheados o aislados, lo que significa que se puede limitar la superficie de ataque pero no eliminarla. Además, el aislamiento puede ser un proceso largo y, mientras tanto, algunos dispositivos seguirán siendo vulnerables. Por eso es fundamental supervisar los dispositivos y detectar y alertar inmediatamente cuando se produce una actividad inusual.

Consideraciones para la supervisión de incidentes de seguridad

- Utilizar la supervisión pasiva, como un TAP de red o un puerto espejo, para evitar la interrupción de las operaciones del dispositivo.
- Aprovechar la información recopilada sobre el contexto clínico de cada dispositivo para comprender lo que representa la comunicación clínica normal.
- Comparar el comportamiento actual con las especificaciones del proveedor, el comportamiento anterior y el comportamiento de un grupo de dispositivos similares en su entorno y en otras organizaciones.

Normas

- Supervisar continuamente todos los dispositivos, con especial énfasis en aquellos con una puntuación de alto riesgo.
- Establecer una estrategia para comparar la comunicación en curso con la de carácter clínico normal.
- Alertar a la seguridad sobre cualquier desviación importante del comportamiento normal.
- Integrarse con terceros que puedan ayudar a realizar una rápida corrección a través de una acción remota, como la segmentación de la red bajo demanda.

Paso 4. Métricas y analíticas

La ciberseguridad de los dispositivos médicos es un proceso largo, que debe mantenerse y mejorarse con el tiempo para adaptarse a un panorama de amenazas en continuo cambio.

El seguimiento de su progreso puede ayudarle a entender si está avanzando en la dirección correcta y a hacer correcciones si su trabajo no está mejorando la situación de seguridad. A continuación se ofrecen algunas pautas para seguir el progreso de su proyecto de seguridad de los dispositivos médicos.

- Crear un cuadro de mando para los productos sanitarios con un calendario de puntuaciones de riesgo, que garantice la reducción del riesgo a lo largo del tiempo.
- Identificar actividades y estrategias que mejoren los KPI y reduzcan los índices de riesgo global.
- Establecer indicadores clave de rendimiento (KPI) basados en el riesgo de los dispositivos importantes y supervisar las mejoras; vincular los KPI a los objetivos de la empresa, como la seguridad del paciente y la disponibilidad del servicio, para obtener la aprobación de la dirección.
- Recopilar datos sobre los índices de riesgo y el comportamiento histórico de los dispositivos, y utilizarlos para tomar mejores decisiones de compra.

Mejorar la visibilidad de los activos y la mitigación de los riesgos de seguridad para los dispositivos médicos con Ivanti Neurons for Healthcare

Ivanti® Neurons for Healthcare mejora la visibilidad de los activos y la mitigación de los riesgos de seguridad de los dispositivos médicos. La solución descubre y perfila de forma inteligente los dispositivos médicos y el Internet de las Cosas Médicas (IoMT), evaluando los riesgos de seguridad, informando de las amenazas y conciliando la información de los dispositivos en múltiples fuentes de datos. Conozca mejor los distintos dispositivos específicos de la sanidad en sus instalaciones, incluida la clasificación de los dispositivos y la información sobre su uso, con los detalles necesarios para reducir los riesgos de seguridad o atender las anomalías. Recopile y concilie los datos de los proveedores, creando una única fuente de verdad para todos sus dispositivos médicos.

Para más información, visite ivanti.es/neurons

ivanti Neurons

ivanti.es/neurons
contact@ivanti.es