Whitepaper
Confidentiality

ALMA

OPERACIÓN DE RED SEGURA Y DE ALTA DISPONIBILIDAD, AL SERVICIO DE LA COMUNIDAD CIENTÍFICA INTERNACIONAL.

LA ENTIDAD

En el desierto de Atacama, en Chile, se ubica el Atacama Large Millimeter/submillimeter Array (ALMA), el radiotelescopio más grande del mundo; cuya construcción, financiamiento y operación se basa en un esfuerzo colaborativo internacional encabezado por cuatro entidades principales: el Observatorio Europeo Austral (ESO), la Fundación Nacional de Ciencia de Estados Unidos (NSF), los Institutos Nacionales de Ciencias Naturales de Japón (NINS), así como la República de Chile.

Ubicado a 5 mil metros de altura sobre el nivel del mar, y en medio del desierto de Atacama -en las cercanías de San Pedro de Atacama- este radiotelescopio está integrado por 66 antenas, la mayoría de ellas de 12 metros de diámetro (en el rango de un edificio de 3 a 4 pisos) y con un peso de más de 100 toneladas cada una. Su conjunto principal de 50 antenas actúa coordinadamente como si fuese un solo telescopio gigante; además, gracias a transportadores fabricados especialmente a la medida, las antenas pueden moverse de acuerdo a las necesidades de observación, ubicándose a distancias máximas de 16 km entre las antenas más distantes.

Como ejemplo de la gran potencia de este radiotelescopio, en abril de 2019, ALMA fue parte de la alianza astronómica mundial "Event Horizon Telescope" que obtuvo la primera imagen de un agujero negro. *"ALMA era imprescindible en dicho proyecto. Podía fallar otro elemento de la iniciativa, pero no nuestro observatorio. Sin ALMA no hubiéramos conseguido esa imagen"*, señala Christian Saldias, IT Manager de *ALMA*.

5 **MIL METROS**
SOBRE EL NIVEL
DEL MAR

“En nuestra historia, cada metro cuenta.”

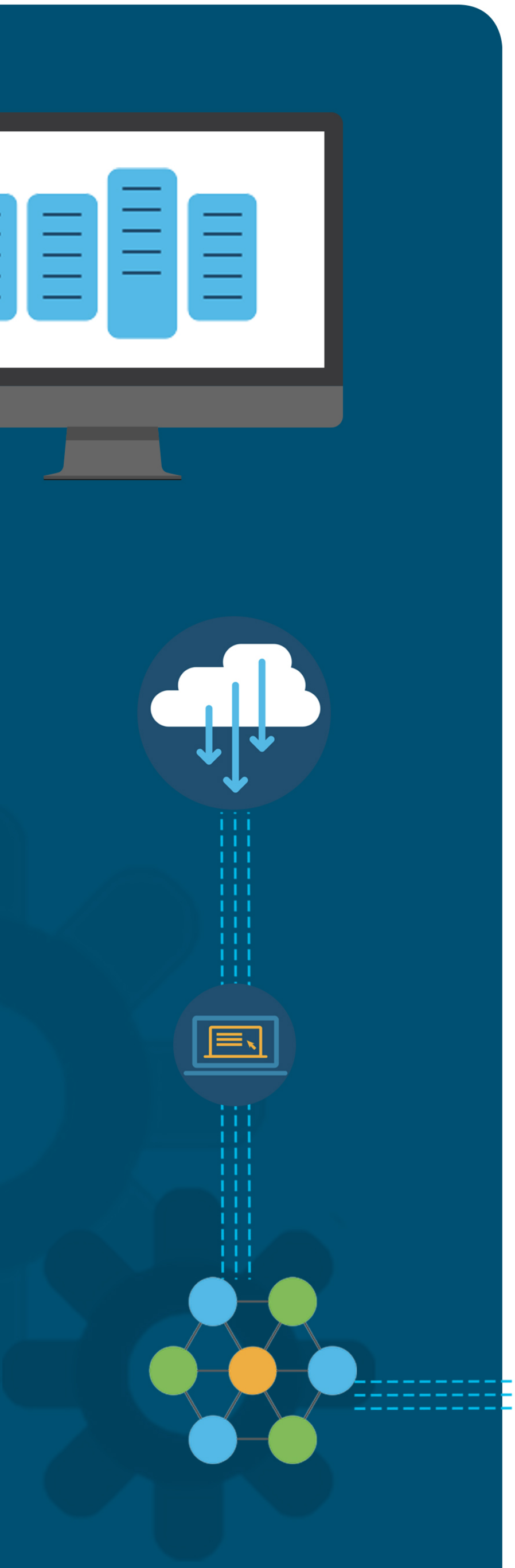
Cristóbal Achermann,
IT Project Manager de ALMA.

Un reto de origen

Desde su origen, este observatorio astronómico representó un desafío enorme. En primer término, ALMA se localizaría a 5 mil metros de altura sobre el nivel del mar, una escala sin precedentes en el contexto chileno (otros observatorios en la zona se ubican en el rango de los 3 mil metros de altitud) y con impactos claros en el funcionamiento de la tecnología. En dicha área, pleno desierto de Atacama, ALMA despliega sus 66 antenas, todas conectadas a un edificio técnico donde se ubica el supercomputador que digitaliza y unifica las señales captadas. Dicha sala protegida por generador, UPS y aire acondicionado, pero que no está presurizada.

A una altitud de 5 mil metros, con una densidad de aire muy baja, muchos componentes tecnológicos (diseñados para trabajar al nivel del mar) tienen dificultades para operar correctamente. Por ejemplo, los ventiladores de las fuentes de poder de los equipos presentan fallas, causando calentamiento excesivo que daña los sistemas. *“En nuestra historia, cada metro cuenta”, apunta Cristóbal Achermann, IT Project Manager de ALMA.*

La relación con Cisco y su partner Dimension Data se inicia en tales circunstancias. Hacia 2008, ALMA, Cisco y Dimension Data prueban y adaptan equipos con el fin de construir una infraestructura de red que pueda operar eficientemente en semejantes condiciones ambientales. ALMA optó por basar su plataforma -switching, routing, Wifi, videoconferencia, telefonía IP, etc.- en soluciones de Cisco. La decisión de optar por Cisco, no fue sólo tecnológica, sino que se basa en dos hechos fundamentales.



Por un lado, la dupla Cisco-Dimension Data garantizaba disponibilidad local de soporte, repuestos y expertise en ingeniería. En instalaciones como ALMA, ubicadas en zonas remotas y con actividades 7x24, es indispensable el acceso -rápido y sencillo- a equipos de reemplazo y al conocimiento experto que ayuda a obtener el máximo provecho de las soluciones. "Necesitábamos tecnología robusta, pero también un soporte igual de robusto", comenta Achermann.

Al mismo tiempo, al elegir a Cisco, ALMA podría aprovechar un ecosistema de productos y soluciones integradas, con capacidades de administración centralizada, compatibilidad entre equipos, inteligencia, automatización de tareas, previsión de fallas, misma gestión de soporte y licencias, etc. Esto evitaría el tener que lidiar con múltiples proveedores y equipos, lo que siempre causa dificultades -operativas y técnicas- a la hora de gestionar una plataforma tecnológica.

En ese sentido, vale la pena señalar que la infraestructura de conectividad de ALMA tiene características excepcionales. La información del Universo captada por las antenas (que operan en una red aislada) es digitalizada y enviada -vía fibra óptica- a un correlacionador (supercomputadora), el cual combina las señales de todas las antenas y genera datos científicos. Esta información se envía a un centro de operaciones (Data Center) en Santiago de Chile, y tras ser procesada (calibrada y optimizada), se distribuye a las organizaciones científicas afiliadas en Europa, Norteamérica y Asia.

“La disponibilidad de nuestra plataforma es crítica, no puede ser amenazada por un ciberataque.”

Cristóbal Achermann,
IT Project Manager de ALMA.

Esta plataforma tecnológica, con más de 3 mil dispositivos de red, es atendida por un equipo de TI que está integrado por sólo cuatro especialistas. Considerando el personal que trabaja en la base de operaciones ubicado en las cercanias de San Pedro de Atacama, así como los que laboran en las oficinas centrales en Santiago, ALMA cuenta con alrededor de 300 colaboradores. En tal contexto, los valores de integración, inteligencia y proactividad de las soluciones de Cisco resultaron sumamente convenientes.

El reto de seguridad: no puede fallar

Aunque su vocación sea observar el Universo, ALMA no podía ignorar el entorno donde opera. En materia de ciberseguridad, esto planteaba varios riesgos importantes.
A diferencia de lo que ocurre en un banco o comercio, en donde un ciberataque busca una recompensa evidente (dinero, datos personales, secuestro de equipos, fraude, etc.), la información científica recopilada por ALMA parecería de poco interés para los cibercriminales. Sin embargo, el observatorio astronómico pronto entendió que su mayor amenaza radicaba en otro aspecto: la potencia de su infraestructura tecnológica.

“Tenemos una enorme capacidad de cómputo instalada. En ese sentido, además de los riesgos que enfrenta cualquier organización -robo de datos, ransomware, virus-, nuestra potencia tecnológica puede resultar muy tentadora para quienes realizan actividades como Criptomining o Botnets. A esas personas les gustaría aprovechar una infraestructura como la de ALMA”, señala Saldías.

© José Luis Stephens

Así, desde hace tres años, de la mano de Cisco y su partner Dimension Data, ALMA ha implementado las siguientes soluciones:

- Firewalls, Firepower para visibilidad completa de la red, y detección y protección avanzada contra amenazas, así como prevención de intrusiones.
- Umbrella (DNS): primera línea de defensa de la red contra amenazas a través de manejo del tráfico DNS, permitiendo visibilidad de las actividades en la web para detener amenazas antes de que lleguen a la red o sus endpoints. Por su forma de trabajar, es capaz de proteger desde la red de antenas, hasta los usuarios dentro y, eventualmente, fuera de la red de ALMA.
- Cisco ISE: para controlar el acceso a la red y, colaborar con las otras soluciones, con capacidad de contención automática de amenazas.
- Email Security: para proteger los correos electrónicos de los funcionarios y colaboradores.
- Switches
- Routers
- Border Firewalls & VPN (ASA)
- Firewalls virtuales para aplicaciones internas (protección de redes OT).

Además, en el caso del Observatorio ALMA en pleno desierto chileno, la seguridad es un aspecto íntimamente ligado a la operación. Si un ciberataque logra afectar la disponibilidad de la infraestructura, el daño sería verdaderamente grave. Como lo resaltan Achermann y Saldias, el activo principal de ALMA es la observación; si no tiene la capacidad para realizar observaciones astronómicas, pierde la habilidad de generar los datos que necesita la comunidad científica mundial.

Peor aún, la falla en la disponibilidad puede resultar desastrosa para el avance de la ciencia: hay fenómenos astronómicos que sólo pueden observarse en un momento específico (un minuto u hora particular) y quizá no se repitan sino hasta dentro de 100 o 200 años -o nunca. Hay otros eventos que implican coordinación de investigadores y observatorios a nivel mundial en un momento preciso, por lo que un atraso podría afectar la realización de dichos proyectos. *“Por tanto, la disponibilidad de nuestra plataforma es crítica, no puede ser amenazada por un ciberataque”, señala Achermann.*

Asimismo, el intercambio de información en el contexto interno y con los asociados en otras partes del planeta tiene que estar protegido contra los ataques conocidos -virus, ransomware, hackeos a servidores o páginas web, spam, etc.- que podrían frenar la operación de la red.

“Tenemos compromisos de tiempo muy estrictos. Desde que se realiza la observación hasta la entrega de los datos al científico, hay lapsos bien acotados. Si alguien entra a la red de ALMA, aunque no dañe nada, el retraso en la entrega de información ya nos significa un problema mayor”,
afirma Saldías.

"Además, como nuestra red está sustentada en soluciones de Cisco, si aprendes a configurar un firewall, ya aprendiste a configurar todos los demás, y eso incluye tareas como la puesta a punto, los temas de licenciamiento, los procesos para levantamiento de casos de seguridad, el soporte, etc. Esta capacidad de integración ha resultado clave, de lo contrario, tendríamos que inventar la rueda con cada implementación", asegura Cristóbal Achermann, IT Project Manager de ALMA.

© ALMA (ESO/NAOJ/NRAO)

La estrategia

Consciente de las amenazas potenciales en su entorno, el equipo de TI, en primer término, decidió olvidarse de los planteamientos reactivos y optó por definir una visión estratégica de su ciberseguridad. Una postura que se benefició de dos factores: el hecho de que la red de ALMA estaba basada en soluciones de Cisco; y sobre todo, que las tecnologías de ciberseguridad de la empresa se sustentan en un modelo de arquitectura -y no de productos independientes- en el que la integración, la visibilidad y la centralización son los pilares. Esto terminaría por facilitar la centralización, sin afectar la productividad de un equipo de TI pequeño.

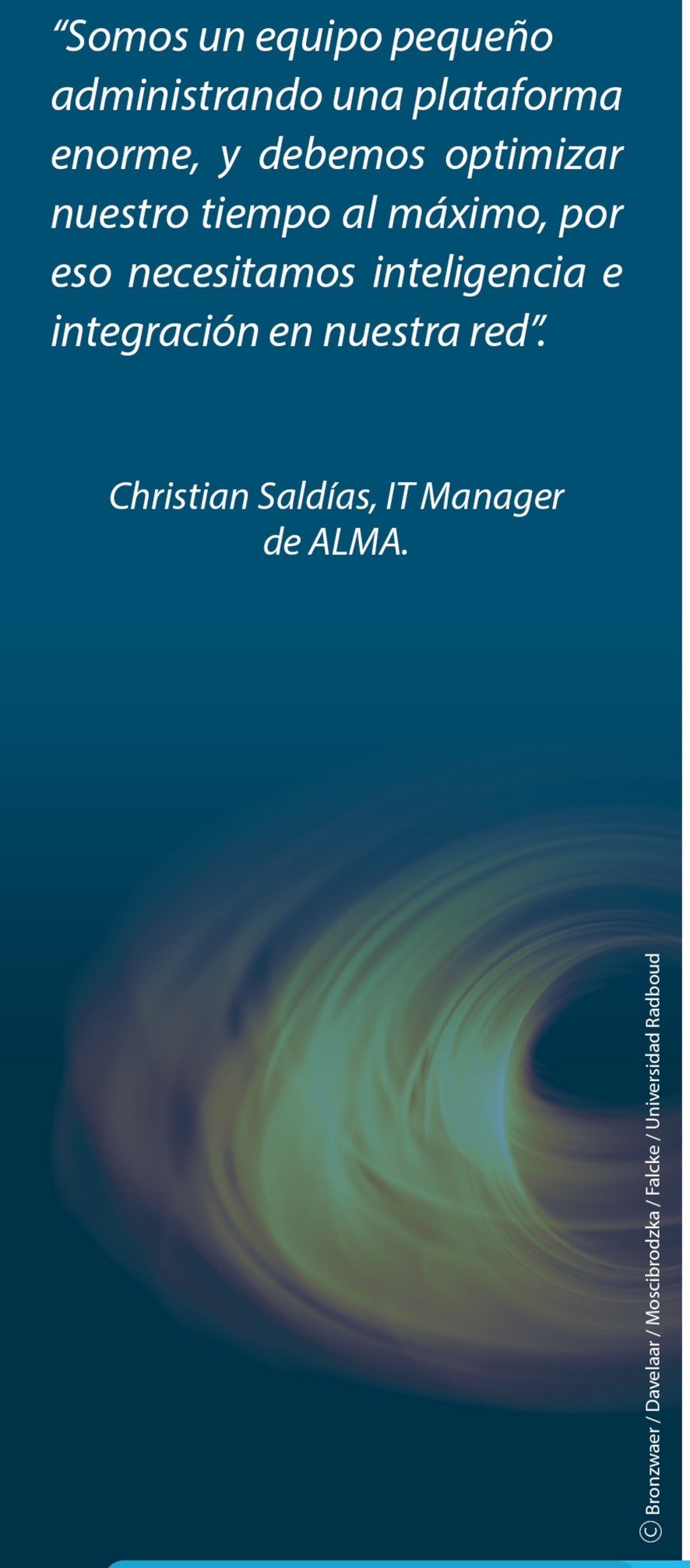
Los beneficios

Con el respaldo de Cisco y su partner Dimension Data, ALMA está consolidando una operación de red más segura y de mayor disponibilidad; no sólo mejorando su nivel de servicio a la comunidad científica nacional e internacional, sino que contribuyendo a materializar proyectos que marcarán un hito en la historia del conocimiento científico. Qué mejor ejemplo de ello que la primera imagen de un agujero negro (2019) o de la formación de planetas (2018).
Las implementaciones de seguridad -beneficiadas por operar en una infraestructura de red basada en tecnologías de Cisco- no sólo resultaron más fáciles de aplicar, sino que con el tiempo revelaron varias ventajas operativas, las cuales han sido muy valiosas para atender un gran reto de conectividad y actuar como un habilitador de servicios.

Las soluciones se integraron fácil y rápidamente entre sí, permitiendo una visión centralizada de toda la plataforma y un control estricto de cambios a las configuraciones de equipos -ambos factores, esenciales para prever amenazas y tomar medidas preventivas con agilidad.

"Somos un equipo pequeño administrando una plataforma enorme, y debemos optimizar nuestro tiempo al máximo, por eso necesitamos inteligencia e integración en nuestra red".

Christian Saldías, IT Manager de ALMA.



© Bronzwaer / Davelaar / Moscibrodzka / Falcke / Universidad Radboud

Adicionalmente, las ventajas de visibilidad y centralización, potenciadas por las capacidades proactivas de las soluciones de Cisco, están impulsando la productividad del personal de TI de ALMA podrá dedicar menos tiempo a actividades como búsqueda de virus o descarte de falsos positivos.

De hecho, ALMA y la dupla Dimension Data y Cisco ya trabajan en ampliar la automatización inteligente. A la fecha, si un científico llega a las instalaciones del observatorio ubicadas en el desierto de Atacama y desea conectar su laptop a la red, aún es necesaria la intervención de un especialista de TI, quien deberá confirmar que el equipo no tiene virus y cuenta con los parches de seguridad necesarios.

La meta en el corto plazo es que dicho proceso manual deje de ser necesario: que la red, por sí misma, realice esa revisión de seguridad y determine si el laptop cumple con los requisitos para conectarse a la plataforma; mejor todavía: si no satisface los criterios, que ayude al usuario a obtener el software y los parches necesarios para habilitar su conexión.

https://www.cisco.com/c/es_mx/products/security/solution-listing.html

Oficinas Centrales en América:
Cisco Systems, Inc.
San José, CA

Oficinas Centrales en Asia Pacífico:
Cisco Systems
Pte. Ltd. Singapur

Oficinas Centrales en Europa:
Cisco Systems
International BV Amsterdam Holanda

Argentina: 0800 555 3456 · Bolivia: 800 10 0682 · Chile: 1230 020 5546 · Colombia: 1 800 518 1068 · Costa Rica: 0800 011 1137
República Dominicana: 866 777 6252 · El Salvador: 800 6600
Guatemala: 1 800 288 0131 · México: 001 888 443 2447 · Perú: 0800 53967 · Venezuela: 0800 102 9109