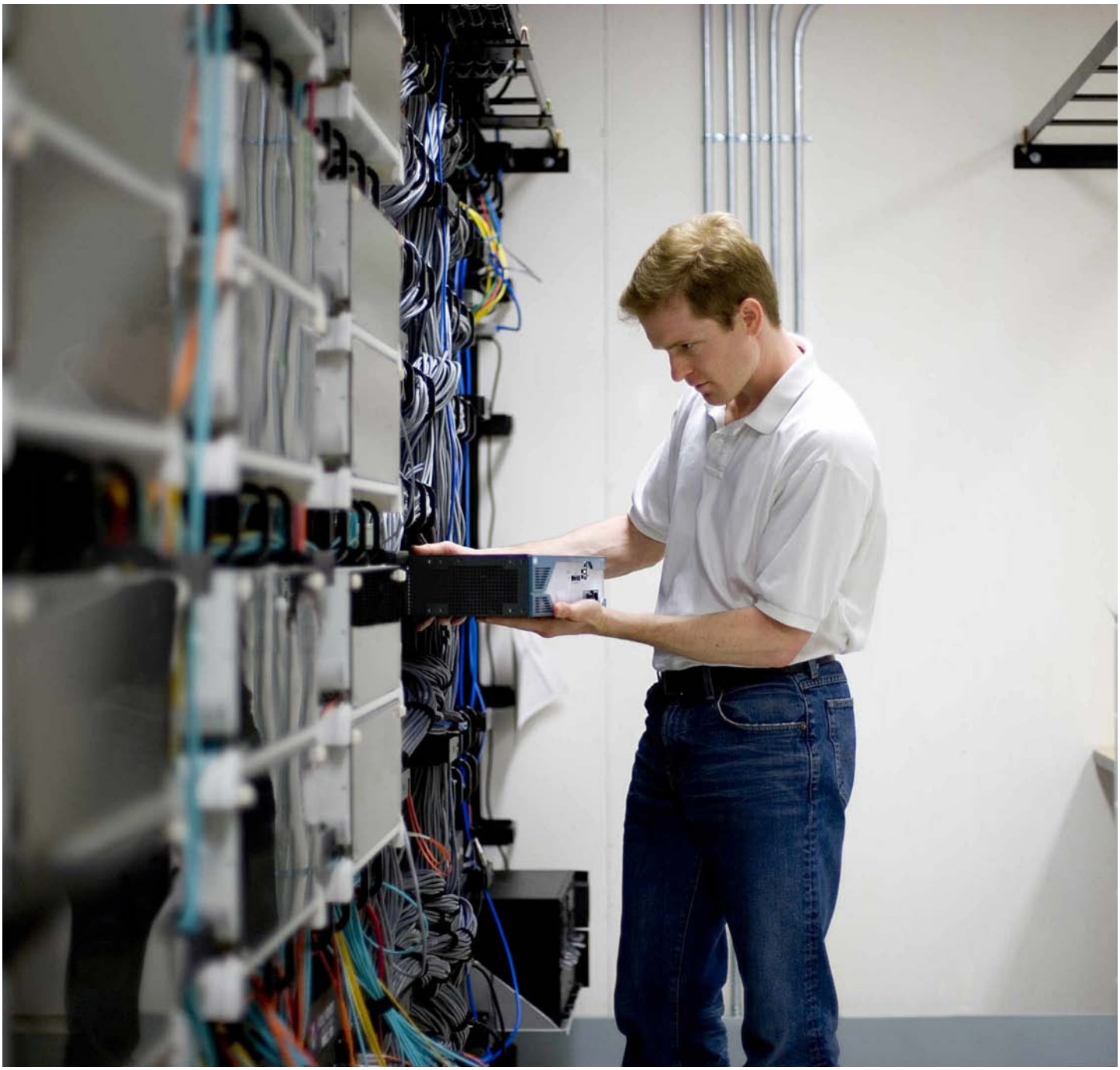
REDES AUTODEFENSIVAS
CISCO SYSTEMS LATINOAMÉRICA 2006



REDES AUTODEFENSIVAS
CISCO SYSTEMS LATINOAMÉRICA 2006

En la medida que las empresas de todos los tamaños asignan una importancia cada vez mayor a sus redes informáticas y de telecomunicaciones, unidas bajo el signo de la convergencia; que incursionan en operaciones de negocio a negocio; que necesitan descentralizar y dinamizar sus funciones; que crean procesos online, y que deben competir globalmente sin importar su tamaño, la seguridad de redes se convierte en un factor vital. A continuación analizamos los conceptos básicos, tecnologías y desafíos que viven las organizaciones en materia de seguridad, y cómo enfrentarlos con la estrategia de seguridad de Cisco, Redes Autodefensivas.

La preocupación por una red segura crece día a día en empresas de todos los tamaños y sectores. La velocidad de propagación de los virus y gusanos, así como los ataques y robos de información, pueden poner en jaque los sistemas empresariales.

Cada vez más las empresas están usando aplicaciones que son determinantes para el funcionamiento y productividad de sus negocios. El éxito de las compañías, y su supervivencia, dependen de estas aplicaciones y de la productividad que pueden obtener implementándolas. De esta manera, la disponibilidad, la confiabilidad y la integridad de los datos, son fundamentales para el negocio.

En la década de los 80s, los virus que existían, que se propagaban por medio de disquetes, únicamente infectaban máquinas individuales y su velocidad de propagación se medía en semanas o meses. En la década de los 90s, la segunda generación de virus se propagaba por medio de email y office macros y se empezaron a registrar incidentes limitados de hackers. El tiempo de propagación de estos ataques se medía en días y semanas y afectaba únicamente redes individuales. Los ataques modernos están basados en gusanos masivos, ataques de negación de servicio distribuidos, spyware, hacking de infraestructura, etc. El impacto es a nivel global y la velocidad de propagación puede llegar a alcanzar cientos de miles de computadores infectados en cuestión de segundos. A su vez, el tiempo que transcurre desde el conocimiento de una vulnerabilidad en un sistema, a la disponibilidad de una herramienta para aprovecharla y hacer daño, se está acortando drásticamente. De 336 días con Nimda en el 2001 a 5 días con Zotob en el 2005.

Así, la evolución de los desafíos en términos de ataques a la seguridad debido a su mayor complejidad, la rapidez en que se propagan y el incremento en conocimiento y organización que tienen quienes realizan estos ataques, hace que la seguridad ocupe un primerísimo lugar para los directivos de las empresas.

Según Gartner, por ejemplo, en el año 2002 el tema de seguridad de redes ni siquiera aparecía como un tema de preocupación para los directivos de las empresas. En el 2003 ya aparecía como preocupación número 12, y en el año 2004 pasó a ser la preocupación número uno, aún por encima de la optimización de los costos operativos y el crecimiento en ventas.

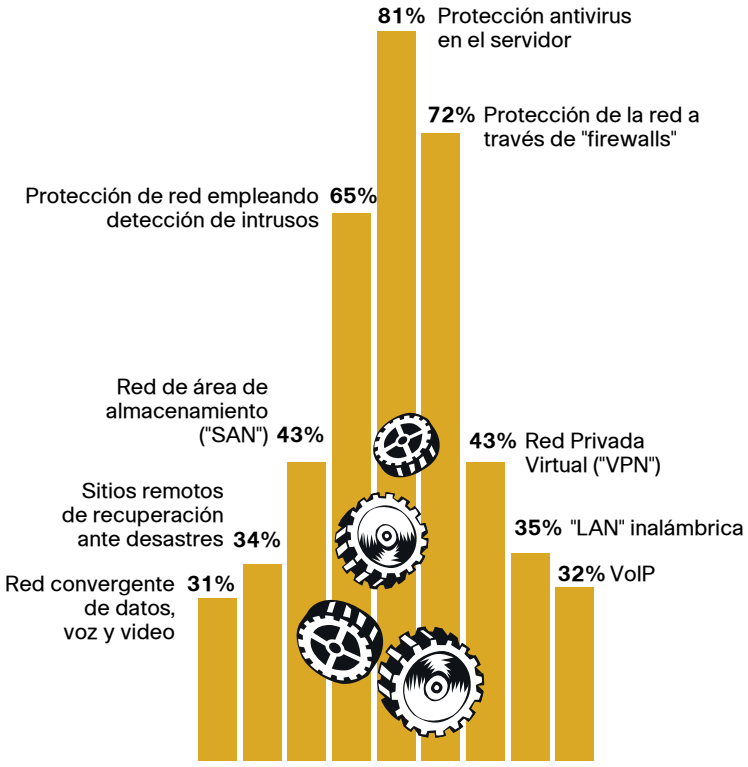
Además, las empresas están colocando más y más aplicaciones de negocio sobre sus redes. Por ejemplo, están migrando su red de voz a su red de datos; están añadiendo conectividad wireless; están añadiendo sistemas de automatización de producción, logística, facturación, y todo sobre la misma red. Y aquí la seguridad adquiere una nueva dimensión, ya que los procesos de negocios de las compañías cada vez más dependen de sus sistemas de información.

Sin una protección adecuada y efectiva, la plataforma de tecnología informática es vulnerable a actividades no autorizadas de hackers, competidores o empleados, o bien es susceptible de sufrir una brecha de seguridad.

Esta realidad es palpable en Latinoamérica. De acuerdo con el estudio Net Impact 2005, en promedio el 30 % de las empresas de la región no cuentan con ningún tipo de seguridad de redes, posible razón por la cual no abren sus redes a empleados, usuarios finales y socios de negocio, limitando así el impacto de la conectividad en aumentos de productividad y ahorros en costos.

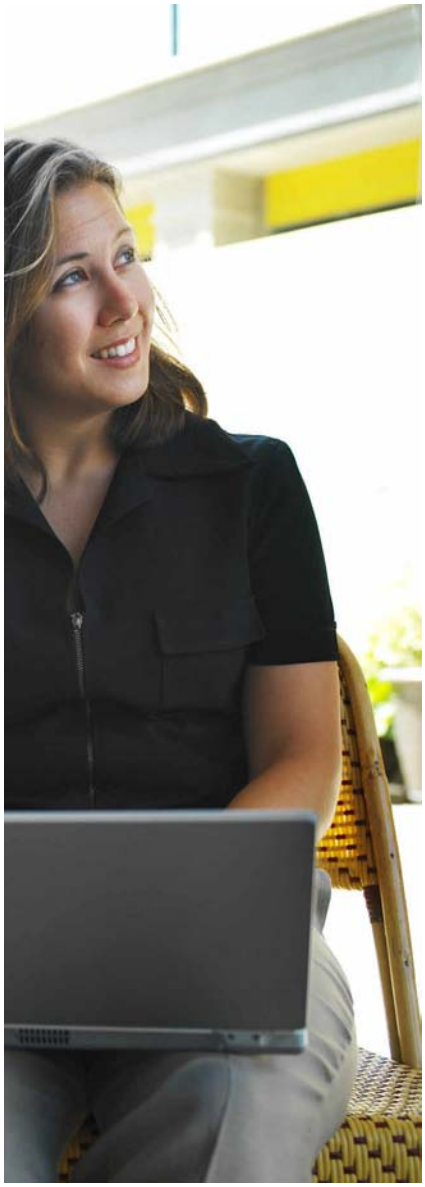
Porcentaje de Organizaciones Conectadas con las tecnologías siguientes como una parte activa de su infraestructura de red

NET IMPACT 2005 LATINOAMERICA



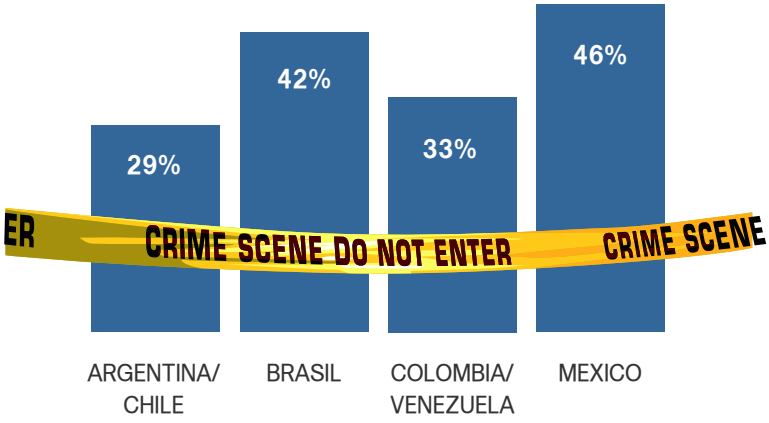
Fuente: Momentum Research

Por otro lado, según el estudio "Actitudes de los gerentes de IT de Latinoamérica respecto a la seguridad" realizado por la firma de investigación independiente Kaagan Research and Associates, y patrocinado por Cisco Systems e IBM (Diciembre 2005), los incidentes de seguridad informáticas en las empresas latinoamericanas continúan aumentando al igual que el riesgo de ataques futuros, mientras disminuye la confidencia de los ejecutivos de poder enfrentarlos.



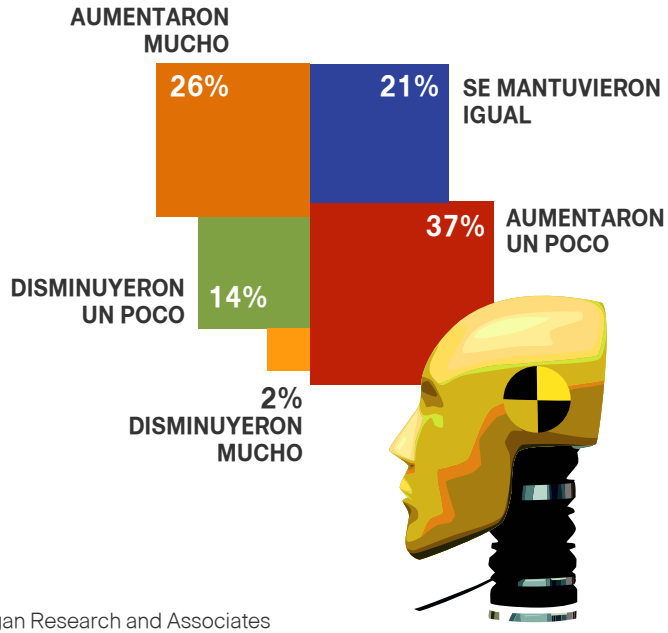
38 % de los ejecutivos entrevistados manifestaron haber sufrido un ataque a la seguridad informática durante el último año, siendo las compañías mexicanas y las brasileras las más afectadas (46 y 42 % respectivamente). Paralelamente, 63% de los ejecutivos entrevistados manifestaron que los riesgos en seguridad informática habían experimentado un "aumento dramático" o habían "aumentado de alguna manera" en los últimos 3 años. Sin embargo, es Brasil donde más ejecutivos (47 %) perciben un "aumento dramático" en los riesgos a la seguridad informática.

Brecha en los sistemas de seguridad de tecnologías de la información, durante el año pasado

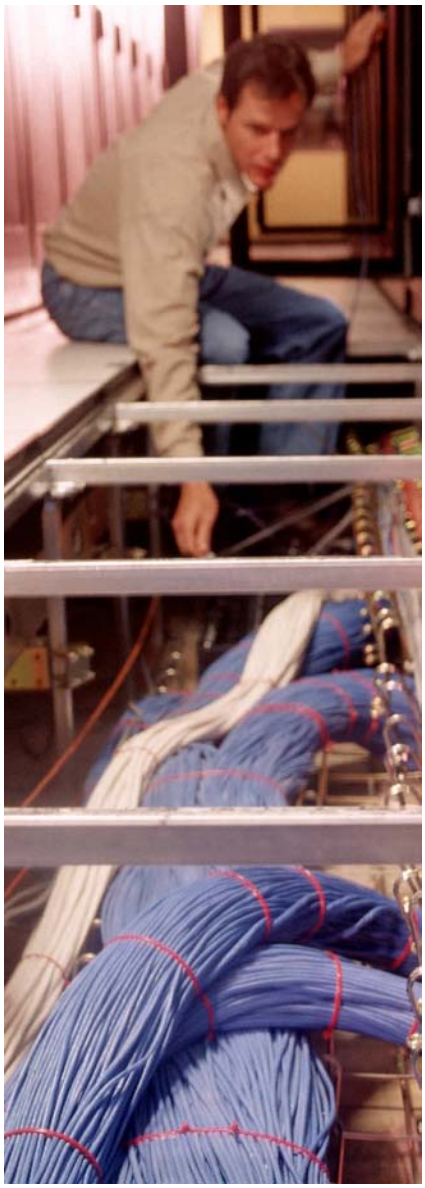


Fuente: Kaagan Research and Associates

Cómo cambiaron los riesgos de IS en los últimos tres años

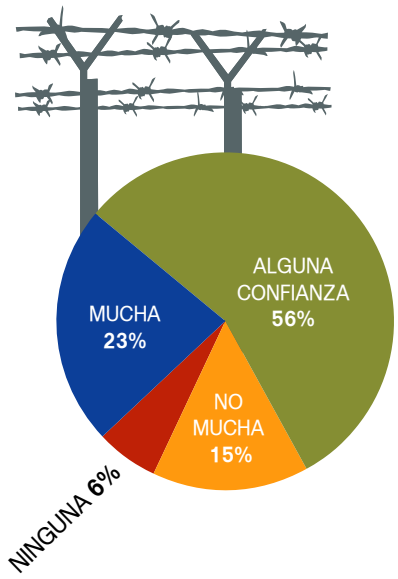


Fuente: Kaagan Research and Associates



Sólo un pequeño porcentaje de ejecutivos IT entrevistados están confiados de que sus empresas están protegidas ante las amenazas internas y externas a la seguridad. 18 % están "muy confiados" de que sus empresas están protegidas ante las amenazas internas y 23 % están "muy confiados" de que sus empresas están protegidas ante las amenazas externas.

Confianza en que la organización está protegida ante amenazas externas.



Fuente: Kaagan Research and Associates

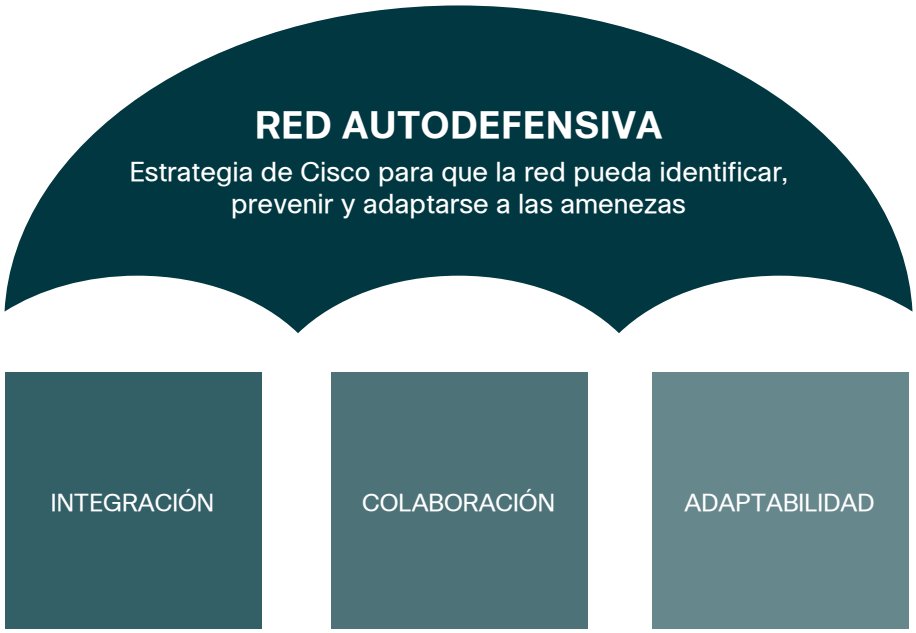
"La encuesta reconfirma que la seguridad de los sistemas informáticos ocupa un primerísimo lugar en las prioridades de los ejecutivos de IT de Latinoamérica", dijo Gastón Tanoira, Gerente de Sistemas de Seguridad de Cisco Systems en Latinoamérica. "Sin embargo, las acciones para enfrentar estas amenazas no se corresponden con los riesgos percibidos".

"En Cisco estamos trabajando en informar y educar sobre la necesidad de contar con una arquitectura de red que identifique, prevenga y se adapte de manera proactiva y automática a las amenazas de seguridad", dijo Tanoira. "La única defensa viable a los ataques modernos de seguridad, debido a su complejidad y rapidez de expansión, es mitigar estos riesgos en la propia red. No se puede depender de dispositivos puntuales que estén en la periferia sino que la red en sí misma debe defenderse".

ESTRATEGIA DE SEGURIDAD DE CISCO

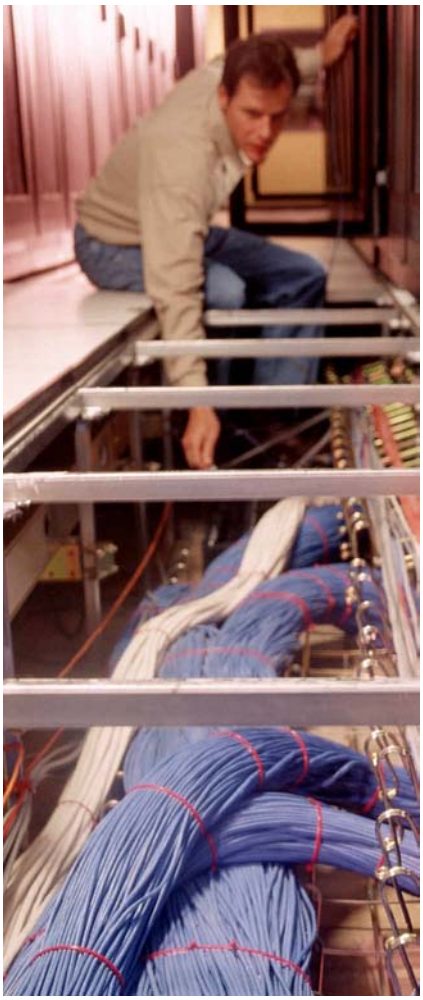
La estrategia de seguridad de Cisco está basada en el concepto de Redes Autodefensivas que significa que la red tiene la habilidad de identificar, prevenir y adaptarse a las amenazas de seguridad. Cisco entiende que la única defensa viable a los ataques modernos de seguridad, debido a su complejidad y rapidez de expansión, es mitigar estos riesgos en la propia red. No se puede depender de dispositivos puntuales que estén en la periferia sino que la red en sí misma debe defenderse.

Estrategia de Seguridad de Cisco



El primer elemento de la estrategia de seguridad de Cisco es la integración. La seguridad de la red debe estar integrada a nivel del sistema. Todos los componentes de la red tienen que ser punto de defensa e interactuar entre sí mismos. Los routers tienen que hablar y trabajar con los switches, los firewalls, los sistemas de prevención de intrusos, servidores, PCs, los puntos de acceso inalámbricos, etc. Todo debe trabajar como un sistema unificado y cada punto de la red debe tener la posibilidad de actuar como agente de seguridad.

La Colaboración es el segundo de los elementos. Cisco lanzó la iniciativa Control de Admisión de la Red (NAC, por sus siglas en inglés) a la cual se han sumado los principales proveedores de seguridad (Trend Micro, IBM, Network Associates, Symantec, Microsoft), para crear una plataforma donde convergen todas las tecnologías que hacen que las redes sean más seguras. De esta manera se obtiene colaboración entre las empresas, y se tienen dispositivos que trabajan en coordinación para mitigar los ataques.



Como tercer y último elemento está la Adaptabilidad. La seguridad debe tener un enfoque proactivo y no reactivo, donde la red se adapta a la evolución de los nuevos ataques. De esta manera la red puede identificar comportamientos sospechosos de los distintos dispositivos conectados a una red, independientemente que el ataque sea conocido o no.

Cisco concibe la infraestructura de TI como un ser viviente, donde la red es el sistema inmunológico. Los seres vivientes estamos expuestos a virus y enfermedades en nuestra vida diaria, pero a pesar de esto el cuerpo se defiende solo, sin que nos enteremos. En las ocasiones que el virus traspasa las primeras defensas, las funciones vitales siguen trabajando. De esta misma forma las redes deben autodefenderse para proteger sus aplicaciones de misión crítica.

Por otra parte, Cisco es la única compañía que cuenta con un enfoque completo e integrado a la seguridad de redes para defender y proteger los procesos de negocio de las organizaciones.

Hoy en día la seguridad no es opcional, es una necesidad. Igual a como sucede en la industria automotriz. Los coches tienen integrados sistemas de seguridad como ABS, Airbags, barras antivuelco, columna del volante colapsable, cinturones de seguridad, que se incorporan desde el mismo diseño del auto y no se añaden una vez fabricado el auto, en la línea de producción.

La oferta de seguridad de Cisco es un diseño a nivel de arquitectura de red que actúa como un sistema unificado, incorporado en el ADN mismo de la red, a diferencia de una solución basada en productos puntuales. Los beneficios de este enfoque sistemático son reducción de la complejidad de los sistemas, mayor integración entre la red y las aplicaciones que corren sobre ella, mayor facilidad en su implementación y administración y menores costos de operación.

Este enfoque permite mover recursos que anteriormente se usaban para la administración e implementación de las redes, hacia la creación de sistemas y aplicaciones que contribuyan a la generación de nuevos clientes, oportunidades de negocio y mercados.

RED AUTODEFENSIVA DE CISCO

La Red Autodefensiva de Cisco consta de tres pilares para responder a las nuevas amenazas. El primer pilar, Seguridad integrada, se incorporan elementos de seguridad en componentes de la red como switches y routers. En el segundo pilar, Seguridad colaborativa, se construyen vínculos entre los elementos de seguridad de la red y se extiende la presencia de la red hasta los puntos terminales que se conectan a ella. En el tercer pilar se introducen funciones de Adaptabilidad, las cuales incrementan la capacidad de la red para responder a amenazas tanto conocidas como desconocidas sobre la base de un conjunto nuevo de tecnologías Anti-X.

Estas han sido las principales etapas de la estrategia de seguridad de Cisco Systems, que ha ido evolucionando para hacer frente a los cambios en los retos de seguridad:

Protección de puntos terminales: una de las realidades de los virus y gusanos es que suelen congestionar la red como consecuencia de su rápida propagación y la infección de los puntos terminales. Cisco comprendió que podía comenzar a resolver estos dos problemas ofreciendo a sus clientes una solución de prevención de intrusiones de puntos terminales denominada Cisco Security Agent. Esta solución utiliza novedosos métodos de seguridad basados en el comportamiento para detectar e impedir que virus y gusanos ingresen a un sistema de puntos terminales, y previene que estos virus y gusanos se propaguen a través de la red. Cisco Security Agent es un amortiguador de primer orden del efecto de propagación de virus y gusanos. Por otra parte, Cisco Security Agent crea una presencia en los puntos terminales que puede utilizarse para establecer un circuito de información entre el punto terminal y la red, por lo que ésta se adapta con rapidez a las nuevas amenazas.

Control de admisión: una de de las iniciativas de la Red Autodefensiva de Cisco de más alto perfil hasta la fecha es el programa de Control de la red o NAC. El NAC permite a los clientes determinar el nivel de acceso a la red que desean otorgar a un punto terminal según su posición de seguridad, la cual se basa en el estado de seguridad del sistema operativo y de las aplicaciones relacionadas. Además de controlar el acceso, el NAC le entrega a los administradores de TI un instrumento para crear zonas de cuarentena y corregir automáticamente los puntos terminales que no cumplen con los requisitos de conformidad. El control de los puntos terminales para garantizar que cuentan con los parches del sistema operativo y las actualizaciones del software antivirus correspondientes es un amortiguador eficaz de segundo orden del efecto de propagación de virus y gusanos. Asimismo, puede concebirse al NAC como una herramienta de gestión de parches y evaluación de puntos vulnerables. El NAC se distingue porque ofrece interfaces de AAA cliente y del sistema principal "backend" que permiten a los clientes conectar los productos de seguridad y políticas de puntos terminales de sus proveedores preferidos. En la actualidad, son más de 60 los fabricantes líderes de la industria que están integrando el NAC en sus tecnologías.

Contención de infecciones: las políticas rigurosas de admisión a la red no son una panacea y no eliminan la necesidad de seguir supervisando los dispositivos una vez que ingresan a una red. Ciertos atacantes pueden evadir con facilidad cualquier control de admisión y la red no puede basarse o confiar en que un elemento infectado se rendirá por sí solo. Los dispositivos que cumplen con los requisitos de conformidad también pueden infectarse mediante diversos vectores una vez que ingresan a la red, por ejemplo, una clave USB con contenido infectado. Para brindar mayor protección aún, la Red Autodefensiva de Cisco está diseñada para extender las comprobaciones de seguridad que se realizan en la admisión al período de duración de la conexión a la red. Asimismo, la Red de autodefensa puede depender de otros elementos de la red, incluidos otros puntos terminales, para detectar cuándo un punto terminal deja de ser confiable, al igual que la policía controla si se cometen delitos en una comunidad mediante el centro de llamadas de emergencia. Cisco considera a la contención de infecciones como un amortiguador de tercer orden del efecto de propagación de virus y gusanos.

Correlación inteligente y respuesta a incidentes: para que los mecanismos de realimentación estables como la contención de infecciones funcionen con eficacia, la Red Autodefensiva de Cisco debe proporcionar servicios tales como correlación de eventos en tiempo real, evaluación rápida del impacto que tiene un evento en la seguridad, la capacidad de determinar las medidas que deben adoptarse y de identificar el punto de control más cercano a fin de implementar una respuesta. La familia de productos MARS de Cisco ofrece métodos para superponer la información proveniente de diversos puntos de presencia (POP) en la red (firewalls, sistemas de detección de instrusiones en la red [NIDS], routers, switches y hosts) con el contexto que obtiene al determinar la topología de la red L2 y L3. Gracias a esta función el equipo de respuesta a incidentes de seguridad puede identificar con rapidez el lugar en el que se produce un ataque en la red.

IDS en línea y detección de anomalías: dada su importancia, Cisco se ha dedicado a desarrollar los sistemas de detección de intrusiones en la red (NIDS). Una de las primeras innovaciones en esta área fue integrar el NIDS en sus plataformas de enrutamiento y switching. Pero para que el NIDS alcance su máximo potencial es necesario que se transforme en un sistema de prevención de intrusiones (IPS) con funciones de filtrado en línea. Éste proporciona un mecanismo para eliminar el tráfico no deseado con motores de clasificación programables de alta definición.

Seguridad de aplicaciones y defensa Anti-X: durante los últimos años, surgieron varios productos nuevos de red en la capa de aplicaciones para ayudar a hacer frente a las nuevas clases de amenazas que los firewalls y productos NIDS clásicos no podían abordar de manera adecuada, como por ejemplo virus y gusanos, spam y phishing por correo electrónico, spyware, abuso de servicios en la Web, abuso de telefonía IP o actividades no autorizadas entre iguales. Cisco desarrolló la próxima generación de servicios de seguridad de inspección de paquetes y contenido a fin de resolver los problemas que plantean estos tipos de amenazas y actividades indebidas. Esta convergencia incorpora los servicios de inspección granular del tráfico a los puntos cruciales de cumplimiento de seguridad de la red, lo que permite contener el tráfico malicioso antes de que se propague a través de la red.

MEJORES PRÁCTICAS DE SEGURIDAD

Las empresas deben afrontar el tema de seguridad de redes desde cuatro niveles diferentes. En primer lugar, debe haber una definición de las políticas de seguridad y sus procesos. La empresa debe definir cuáles son sus activos más importantes; aquellos que deben resguardar para darle continuidad y éxito a la empresa, y debe enfocar sus recursos para respaldar estos activos. La mayor parte del esfuerzo lo tienen que poner en donde se genera la mayor parte de su negocio.

En segundo lugar, debe haber educación y concientización de parte del personal en las empresas. Los empleados deben ser conscientes de las consecuencias de su actuar en sus empresas en términos de seguridad.

Como tercer nivel se encuentra la tecnología en sí, que debe ser de tal modo que las empresas puedan guardar sus sistemas de información de manera efectiva, con el fin de requerir la menor participación humana posible. Debe ser auto-defensiva y tener la habilidad para adaptarse a las evoluciones de seguridad de hoy y de mañana.

Por último, es vital el gerenciamiento de las plataformas de seguridad. Las empresas deben tener sistemas que faciliten el trabajo al equipo responsable por la seguridad para poder hacer auditorías y confirmar que las personas actúen de acuerdo con las políticas preestablecidas por cada compañía. Es vital que haya un panorama claro del estado de los sistemas, de dónde viene el ataque, qué tipo de ataque es, cómo afecta esto al sistema y cómo poder mitigarlo de la mejor manera posible.

Estas son algunas prácticas a tener en cuenta:

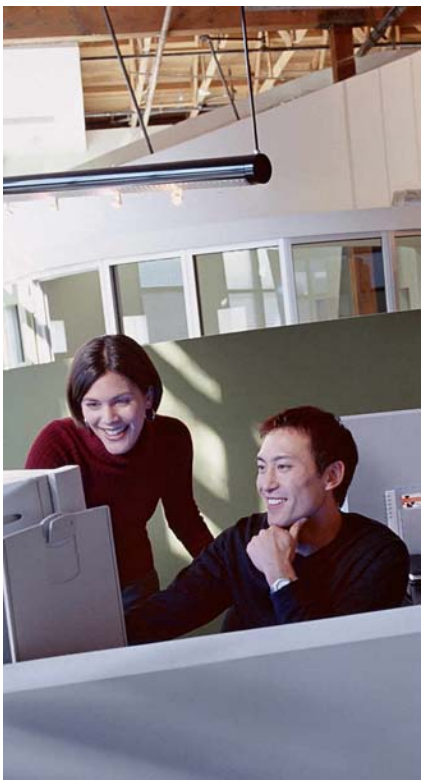
- **Participación del nivel gerencial.** Los decisores y gerentes deben creer que la seguridad es importante. Primero, porque la estrategia de seguridad debería siempre ser una función de la estrategia de negocios. Es simple: el propósito de las funciones de seguridad es hacer que la operación de los negocios sea continua y esté protegida. Por otra parte, de esta manera la política queda en el tope, y se garantiza la participación de todos los empleados.

- **Aproximación proporcional.** Resumidas cuentas, tener en cuenta que el valor del sistema de protección debe costar una proporción razonable del valor que se pretende proteger.

· **Nombrar un experto en Seguridad.** En general, las organizaciones pequeñas no disponen de personal dedicado específicamente a la seguridad. A pesar del bajo presupuesto que puedan tener, y que no les permite contratar un equipo de seguridad, una persona (o incluso parte de una persona) es mejor que nada. Algunos ubican este rol dentro del organigrama de TI y otros dentro del sector financiero, o bien reportando al CEO. Este experto debería dedicar una porción de su tiempo a reflexionar sobre los problemas de seguridad, y se le debe otorgar autoridad en tareas relacionadas con esa materia dentro de la empresa. Debe identificar, en base al diálogo con las instancias gerenciales, los riesgos más importantes y debe realizar planes (acotados en tiempo y presupuesto) para minimizarlos.

· **La seguridad es el camino, no el destino.** La seguridad es una materia de grados en lugar de un estado absoluto. De modo que no hay un único producto, persona o política que pueda proveer seguridad. La aproximación correcta debe ser incremental. Según los expertos, es posible mejorar el nivel de seguridad aplicando lo siguiente: desarrollando políticas y requisitos, implementando soluciones y auditando resultados.

· **Elección inteligente del proveedor de seguridad.** Se puede lograr una mayor seguridad a un menor costo eligiendo un proveedor que piense en una seguridad de amplio espectro y que provea equipamiento y software que interopere sin inconvenientes en todas las áreas de la red, incluyendo firewalls, redes internas, componentes, equipos de escritorio, VPNs y más.



Soluciones de Seguridad de Cisco

DISPOSITIVOS DE SEGURIDAD DE MÚLTIPLES FUNCIONES

ASA 5500. Este es un dispositivo de seguridad adaptativa de alto desempeño y de múltiples funciones y el cual entrega firewall, IPS, anti virus de red y servicios VPN. Es un componente clave de la Red Autodefensita de Cisco y ofrece mitigación proactiva a amenazas antes de que los ataques se propaguen por la red, controles de actividad de red y de tráfico de aplicaciones y entrega conectividad VPN flexible de manera costo efectiva y fácil de administrar.

FIREWALL, VPNS Y PROTECCIÓN CONTRA INTRUSOS

Cisco PIX 500. Es un firewall confiable, escalable y con capacidades sin igual en la industria. Se entregan como dispositivos dedicados o como módulos integrados en los switches Catalyst de Cisco. Los PIX de Cisco presentan una arquitectura de seguridad híbrida innovadora, que incluye inspección de paquetes que conserva su información de estado y funciones VPN con IPSec integrada. Ofrecen los niveles más elevados de seguridad y rendimiento, y admiten más conexiones simultáneas que cualquier otro firewall a una velocidad inigualable.

Routers de seguridad Cisco y switches Catalyst de Cisco. Cisco ha integrado directamente la seguridad en la infraestructura de la red por medio de funciones de seguridad mejoradas en los routers de Cisco y en los switches Catalyst de Cisco, lo que proporciona una flexibilidad y ahorro de costos sin igual para las instalaciones de seguridad. Al aprovechar estos dispositivos de red, las organizaciones pueden aplicar políticas de seguridad sofisticadas, de extremo a extremo, optimizando sus inversiones en infraestructura Cisco. El software Cisco IOS que se ejecuta en routers Cisco y en switches Catalyst de Cisco incluye compatibilidad con VPN IPSec y MPLS con todas sus funciones, basados en estándares para la conectividad de sucursales y de acceso remoto. Los routers y switches Catalyst de Cisco incluyen además un robusto firewall con inspección de paquetes que conserva su información de estado y un sistema de detección de intrusiones (IDS), con capacidad para escalar el rendimiento por medio de módulos de aceleración tipo plug-in. Y por último, los routers de Cisco y los switches Catalyst de Cisco son los mecanismos de control de acceso principales que permiten o desautorizan la conectividad de los puntos terminales a los recursos conectados en red.

Cisco IDS. Cisco IDS ofrece protección contra intrusiones en tiempo real para el perímetro de la red, las redes externas y la red interna. El sistema utiliza sensores, equipos de red de alta velocidad que analizan paquetes individuales y detectan cualquier actividad sospechosa. Si el flujo de datos presenta una actividad no autorizada o un ataque a la red, los sensores pueden detectar la actividad indebida en tiempo real, enviar alarmas a un administrador y aislar al atacante de la red.

Cisco ICS. El Sistema de Control de Incidentes de Cisco, Cisco Incident Control System (ICS), previene nuevos gusanos y ataques de virus al permitirle a la red adaptarse rápidamente y entregar una respuesta distribuida. Debido a que el tiempo que le toma a un gusado o virus desplegarse a nivel mundial ha pasado de días a minutos, se requiere una respuesta proactiva minutos luego de la infección, sin importar su localización para asegurar la seguridad de las redes. El ICS de Cisco entrega una solución de defensa a través de toda la red minutos después de que haya sucedido un ataque en cualquier parte del mundo. Utilizando la capacidad de monitoreo global TrendLabs, Cisco ICS colabora con los dispositivos de red de Cisco y con los dispositivos de seguridad para distribuir rápidamente capacidades de inmunización de virus y gusanos a través de la red. Este enfoque proactivo y rápido previene que los gusanos y los virus se establezcan en la red.

NETWORK ADMISSION CONTROL (NAC)

NAC o El Control de Admisión de Red, es un conjunto de tecnologías y soluciones construidas sobre una iniciativa liderada por Cisco Systems, la cual usa la infraestructura de red para hacer cumplir las políticas de seguridad en todos los dispositivos que buscan tener acceso a los recursos de cómputo de la red limitando de esta manera los daños de las nuevas amenazas a la seguridad. Los clientes que usan NAC permiten acceso a la red solamente a los dispositivos finales (PCs, servidores, PDAs por ejemplo) reconocidos y que cumplan con las políticas y puede restringir el acceso a los dispositivos que no las cumplan. NAC se ofrece de dos maneras:

- Tecnología de Dispositivo NAC, basada en la línea de productos Cisco Clean Access, que ofrece un despliegue rápido de evaluación dentro del dispositivo final, administración de políticas y reasignación de servicios.

- Tecnología NAC Framework a través del Programa de Control de Admisión de Red de Cisco que integra infraestructura de red con soluciones de más de 60 fabricantes de antivirus y software de administración.

SOLUCIONES DE ADMINISTRACIÓN DE IDENTIDAD DE CISCO

Cisco Secure ACS: es un servidor de control de acceso altamente escalable, de alto rendimiento que funciona como sistema de servidor RADIUS o TACACS+ centralizado. Controla las funciones de AAA para los usuarios que acceden a los recursos de la compañía a través de una red. Al usar Cisco Secure ACS, los administradores de red pueden controlar el acceso de los usuarios a la red, autorizar diferentes servicios de red para usuarios o grupos de usuarios y mantener un registro de todas las actividades realizadas por los usuarios en la red. Asimismo, los administradores de la red pueden usar la misma estructura de AAA para gestionar (mediante TACACS+) las tareas administrativas y los grupos, y controlar cómo cambian, acceden a la red y la configuran a nivel interno. Como motor de creación de políticas de la solución de Control de admisión a la red de Cisco, Cisco Secure ACS proporciona la inteligencia y el control que sustenta la política de seguridad de una organización.

SOLUCIONES DE SEGURIDAD EN PUNTOS TERMINALES

Cisco Security Agent, CSA: es un software de protección de puntos terminales que reside en equipos personales y servidores. CSA identifica e impide comportamientos maliciosos antes que éstos se produzcan, eliminando así los riesgos potenciales de seguridad conocidos y desconocidos ("Día cero") como los gusanos que se propagan a través de Internet.

SOLUCIONES VPN DE ACCESO REMOTO

Concentrador VPN 3000. Los concentradores de la serie Cisco VPN 3000 son plataformas VPN de acceso remoto que combinan alta disponibilidad, alto rendimiento y escalabilidad con las técnicas de autenticación y cifrado más avanzadas existentes. El uso de la tecnología VPN reduce enormemente el costo de las comunicaciones. Los concentradores de la serie Cisco VPN 3000 son las únicas plataformas escalables que ofrecen componentes ampliables por el cliente y que se pueden intercambiar sobre el terreno. Estos componentes, denominados módulos de Procesamiento de cifrado escalable (SEP), permiten a los usuarios agregar capacidades y flujo de procesamiento fácilmente. La flexibilidad de la serie Cisco VPN 3000 permite a la vez la terminación de túneles VPN con IPSec y SSL para lograr una mayor flexibilidad y reducción del costo de propiedad.

SOLUCIONES DE CLIENTE VPN

Cliente VPN de Cisco: Permite la conectividad segura para VPNs de acceso remoto, e incluye la compatibilidad con aplicaciones de comercio electrónico, usuarios móviles y trabajo a distancia. Compatible con los sistemas operativos Windows, Linux, Solaris y Macintosh, el Cliente VPN de Cisco ofrece una implementación completa de las normas IPSec, incluidos el Estándar de cifrado de datos (DES) y DES triple (3DES), cifrado AES y la autenticación por medio de certificados digitales, contraseñas de un solo uso y claves previamente compartidas, RADIUS, Dominio NT, Active Directory/Kerberos y autorización LDAP. El Cliente VPN de Cisco es compatible con la mayoría de las plataformas de cabecera de red de Cisco, incluidos los concentradores Cisco VPN 3000, firewalls PIX de Cisco y todos los routers habilitados con VPN de Cisco.

SOLUCIONES DE ADMINISTRACIÓN DE CONTENIDO

Aceleración SSL de Cisco: Cisco ofrece las soluciones más completas y de más alto rendimiento de la industria para dar soporte a redes internas, redes externas y aplicaciones en Internet basadas en SSL. Las soluciones de Cisco optimizan las transacciones mediante SSL para liberar la capacidad del servidor, escalar el rendimiento del sitio, incrementar la confiabilidad de las transacciones seguras y simplificar la administración de certificados de usuario, reduciendo tanto los gastos operativos como de capital.

Administración de acceso a contenidos y filtrado de contenido: Cisco ofrece soluciones para la administración del acceso al contenido en el extremo de la red, lo que permite a empresas e instituciones educativas opciones dirigidas a bloquear contenidos en la Web y filtrar las direcciones URL.

SOLUCIONES DE ADMINISTRACIÓN DE SEGURIDAD

Cisco Security Management Suite: Este conjunto de productos y tecnologías entregan un marco para administrar la red Autodefensiva de Cisco y crear políticas de administración y de regulación. Esta solución ientegrada entrega funciones que simplifican y automatizan las tareas asociadas con las operaciones de administración de la seguridad, incluyendo: configuración, monitoreo, análisis y mitigación. Los primeros productos claves de este conjunto de productos son Cisco Security Manager (versión 3.0) y majoras para Cisco Security MARS (versión 4.2).

CiscoWorks SIMS: recopila y analiza eventos de seguridad de los Sistemas de detección de intrusiones, firewalls, sistemas operativos, aplicaciones y dispositivos antivirus. Esta información de seguridad se correlaciona estadísticamente, se evalúa de acuerdo con normas de seguridad definidas y se presenta a los administradores en tiempo real en función de su prioridad en un formato en el que se pueda trabajar. CiscoWorks SIMS incluye funciones de diversos proveedores para las soluciones de seguridad de red integradas de Cisco.

DETECCIÓN Y MITIGACIÓN DE ANOMALÍAS

Cisco Guards. Los dispositivos de mitigación de ataques distribuidos de negación de servicio de Cisco son parte de la familia de soluciones más poderosa y completa de la industria para detectar y combatir los ataques distribuidos de negación de servicio, DDoS altamente complejos y sofisticados de hoy en día. Al trabajar en conjunto con Detectores de Tráfico Anómalo de Cisco, Cisco Guards detecta la presencia potencial un un ataque DDoS, desvía el tráfico destinado al dispositivo a atacar e identifica y bloquea tráfico malicioso en tiempo real sin afectar el flujo de transacciones de misión crítica legítimos. Como resultado, las operaciones de negocio de las empresas continuan corriendo, aún cuando estén siendo atacadas, asegurando que la información y los recursos corporativos están siempre protegidos.

SERVICIOS AVANZADOS PARA SEGURIDAD EN LA RED

Los consultores de Servicios Avanzados de Cisco poseen certificaciones CCIE y CISSP a nivel experto y cuentan con experiencia en la planificación, diseño, implementación y optimización de infraestructuras de seguridad de red en importantes empresas comerciales y organizaciones gubernamentales.

PARA OBTENER MAS **INFORMACION**

Cisco Systems Argentina / Bolivia / Paraguay y Uruguay
Ing. Butty 240 - piso 17 - Capital Federal. (C1001ABF) - Argentina
Argentina:
0810-444-24726
Paraguay / Uruguay / Bolivia
+54-11-41321100 Ext. 0115
www.cisco.com.ar

Cisco Systems Brasil
Centro Empresarial Nações Unidas - CENU
Av. das Nações Unidas, 12901 - 26º e 18º andares
Torre Oeste São Paulo - SP - Cep: 04578-000
0800 702 4726
www.cisco.com/br

Cisco Systems Chile
Edificio World Trade Center, Torre Costanera
Av. Nva. Tajamar 555
Santiago - Chile.
800 52 2000
www.cisco.com/cl

Cisco Systems Colombia
Carrera 7 No. 71-21. Torre A. Piso 17
Bogotá, Colombia.
018009154303 Ext. 7182506
www.cisco.com/co

Cisco Systems Costa Rica
Centro Corporativo Plaza Roble
Edificio Los Balcones, Primer Nivel
San José, Costa Rica
0800-012-0118 ext. 2653
www.cisco.com/cr

Cisco Systems Ecuador
18776852773 Ext. 7182506

Cisco Systems Panamá
Edificio World Trade Center
Piso 17, Of 1701 Area Comercial, Marbella
Panamá
001-800-507-1286 Ext. 7182653
www.cisco.com/pa

Cisco Systems México
Paseo de Tamarindos 400A, Piso 30
Bosques de las Lomas, México.
001-800-667-0832
Mexico North Ext. 7186297
Mexico DF Ext 7186234
Mexico West Ext 7186235
Mexico South Ext 7182642
www.cisco.com/mx

Cisco Systems Perú
Av. Victor Andrés Belaunde 147, Vía Principal 123
Edificio Real Uno, piso 13
San Isidro, Perú.
+511 215-5117
www.cisco.com/pe

Cisco Systems Puerto Rico
Westernbank Plaza
268 Ave Munoz Rivera, Suite 2300
San Juan, PR 00918
Puerto Rico.
787 620 1888
Bermuda
1-877-841-6599 Ext 6214
Rep. Dominicana
1-888-156-1464 Ext 6214
www.cisco.com/pr

Cisco Systems Venezuela
Av. La Estancia, Centro Banaven,
Torre C, piso 7. Chuao.
0-800-100-4767 ext. 7182506/ 7182649
www.cisco.com/ve

US Toll free
1-800-667-0832
Phone USA: 1-800-493-9697

Cisco Systems cuenta con más de 200 oficinas en distintos paises y regiones. Direcciones, teléfonos y números de fax pueden ser encontrados en el siguiente site: **www.cisco.com/go/offices**

Alemania · Arabia Saudita · Argentina · Australia · Austria · Bélgica · Brasil · Bulgaria · Canadá · Chile · China PRC · Colombia · Corea · Costa Rica · Croacia · Dinamarca · Dubai, UAE · Escocia · Eslovaquia · Eslovenia · España · Estados Unidos · Filipinas · Finlandia · Francia · Grecia · Hong Kong SAR · Hungría · India · Indonesia · Irlanda · Israel · Italia · Japón · Luxemburgo · Malasia · México · Nueva Zelanda · Noruega · Países Bajos · Perú · Polonia · Portugal · Puerto Rico · Reino Unido · República Checa · Rumania · Rusia · Singapur · Sudáfrica · Suecia · Suiza · Tailandia · Taiwán · Turquía · Ucrania · Venezuela · Vietnam · Zimbabwe

N2/KW/LW5530 01/04