# Red de Autodefensa de Cisco: sistemas estratégicos para la seguridad de la información

**"La solución de Cisco proporciona una seguridad fiable y eficaz. Los clientes conseguirán una mayor protección de las aplicaciones críticas de su empresa con menor intervención del personal TI".**
**- Joel Conover, Current Analysis**

Las organizaciones que miran al futuro reinventan, cada día, la forma en que llevan a cabo sus negocios mediante la adopción de modelos basados en Internet. ¿Los resultados? Ventajas competitivas, nuevas fuentes de ingresos y procesos empresariales optimizados.

Sin embargo, las conexiones a Internet sin una seguridad apropiada pueden poner en peligro las ganancias en productividad que hacen más rentables a las empresas de hoy en día. En el pasado, las amenazas a la seguridad desde fuentes externas se movían a un ritmo lento ante el cual era sencillo defenderse. En el actual entorno interconectado, cualquier amenaza llega a todo el mundo en cuestión de minutos y los sistemas de seguridad deben reaccionar instantáneamente.

Cada vez, en mayor medida, los ataques a la seguridad se dirigen a las aplicaciones empresariales que se basan en el uso de exploradores Internet. Estas complejas aplicaciones dinámicas no siempre disponen de firmas antivirus o parches periódicos de actualización; debido a esto, una brecha en la seguridad puede exponer los activos, provocar situaciones de responsabilidad legal, dañar gravemente la confianza y afectar de forma negativa a la rentabilidad.

Para enfrentarse a este problema, los administradores utilizan actualmente soluciones tácticas, con un enfoque de la seguridad basado en reacciones puntuales. Estas soluciones puntuales introducen mayor complejidad e inconsistencia en el entorno. Esto da como resultado:

- Una seguridad frágil. La complejidad e inconsistencia crean vacíos de riesgo.
- Baja visibilidad de extremo a extremo. Impide obtener la visión necesaria para una administración operativa eficaz y el control de políticas de seguridad.
- Erosión de la postura de seguridad. Las organizaciones no tienen capacidad de mantener la seguridad y mucho menos de mejorarla.
- Mayor coste total de propiedad. Las soluciones puntuales requieren una compleja integración y necesitan más atención en su implementación, mantenimiento y administración a lo largo del tiempo.
- Falta de agilidad. La complejidad obstaculiza la capacidad de la organización para coordinar las políticas orientadas a objetivos empresariales en constante evolución.

En algunos sectores como los servicios médicos y financieros, los gobiernos están regulando la privacidad de los datos. Las soluciones puntuales pueden proteger la privacidad de los datos en los extremos de una red, pero estas soluciones no proporcionan el conocimiento en profundidad y la visibilidad de todas las áreas de la red. La visibilidad de la seguridad de extremo a extremo ofrece a los administradores TI la información que necesitan para implementar las prácticas recomendadas en toda la red y garantizar el cumplimiento de las normas que exigen los gobiernos.

En el entorno actual, resulta esencial alinear los procesos de la tecnología de la información (TI) con los objetivos empresariales. La red toca todas las partes de la infraestructura de una empresa; esta es la razón por la cual una solución de red integrada y global se encuentra en una posición excepcional para ayudar a las empresas en el logro de sus objetivos.

## LA VISIÓN DE CISCO

Cisco Systems® da a los administradores de seguridad la capacidad de implementar, de forma segura, aplicaciones y procesos vitales para las empresas en redes integradas, a fin de que puedan incrementar su productividad y obtener una ventaja competitiva. Estas redes son resistentes, integradas y adaptables. La confianza que se genera al conocer que los procesos y la información empresarial de una organización son plenamente seguros es un factor esencial para el crecimiento dinámico y el aumento de la productividad.

Otros fabricantes de seguridad pueden ofrecer soluciones puntuales que establecen un nivel básico de seguridad en las redes IP. Estas soluciones requieren, con frecuencia, grandes esfuerzos de integración que consumen tiempo, son caros y muy complejos.

Cisco® proporciona los sistemas y servicios integrados de seguridad que necesitan las redes de misiones críticas de una organización. Cisco añade también inteligencia de seguridad a la infraestructura de red, ya que entiende que la seguridad no es algo accesorio, si no una pieza fundamental en los procesos empresariales y, en definitiva, en el éxito de una organización.

## CREACIÓN DE LA RED DE AUTODEFENSA

La Red de Autodefensa de Cisco es un conjunto de sistemas estratégicos para la seguridad que utiliza la red para identificar, impedir y adaptarse a las amenazas que provienen de fuentes internas y externas. Una red de autodefensa simplifica el entorno de seguridad a través de una estrecha integración, una completa seguridad, una mayor visibilidad de extremo a extremo y un mejor coste total de propiedad. Todos los componentes de la red (la plataforma de red segura, los servicios y tecnologías avanzadas, la administración operativa y el control de políticas de seguridad) juegan un papel en la seguridad del entorno de red.

La integración, colaboración y capacidad de adaptación son capacidades básicas de la Red de Autodefensa de Cisco. Con una amplitud y una profundidad excepcionales en ofertas y experiencia de seguridad, sólo Cisco puede ofrecer este método de sistemas basado en red.

- **Integración** de la seguridad a través de toda la infraestructura existente; incorporada, no añadida. Cada elemento de la red actúa como un punto de defensa.
- **Colaboración**, en toda la red, entre los componentes de seguridad y de red. La seguridad se convierte en un sistema que involucra la cooperación entre los extremos y los elementos de red con capacidad de seguridad, y la aplicación de las políticas de seguridad.
- **Capacidad de adaptación** de la red a la evolución inteligente y a las nuevas amenazas. Por ejemplo, métodos de comportamiento que reconocen automáticamente nuevos tipos de amenazas a medida que aparecen, colaboración entre los servicios de seguridad y la inteligencia de red para respuestas dinámicas, y una gran capacidad de reconocimiento para gestionar las amenazas en varias capas de la red.

## COMPONENTES ESENCIALES DE LA SEGURIDAD DE RED

La Red de Autodefensa de Cisco se compone de cinco partes fundamentales para una eficaz seguridad de red.

La plataforma de red segura es la base de toda la Red de Autodefensa de Cisco. En esta plataforma puede implementar tecnologías y servicios avanzados de seguridad, cuándo y dónde sean necesarios, para resolver los requerimientos de control y contención de amenazas, comunicaciones confidenciales y transacciones seguras. Al abarcar la red de extremo a extremo, la administración operativa y el control de políticas de seguridad conforman la estructura de una administración eficaz de la seguridad, el control y la capacidad de respuesta.


## Plataforma de red segura

La plataforma de red segura es una base sólida, segura y flexible desde la que se puede construir una Red de autodefensa. Con Cisco, la seguridad se considera una característica de red integral y fundamental. Las capacidades que, de modo tradicional, se obtenían sólo como niveles de una solución puntual, ahora son funciones fundamentales de la infraestructura de red. Con la seguridad integrada en el propio tejido de la red, la plataforma de red segura proporciona una base elegante y flexible sobre la cual se pueden añadir fácilmente las tecnologías y servicios de seguridad más avanzados. De esta forma, una plataforma de red segura que se basa en tecnología Cisco permite que su red evolucione de modo orgánico (en fases de actualización planificadas y predecibles) y estratégico, utilizando aquello de lo que dispone para implementar seguridad cuándo y dónde sea necesario. Este método protege la inversión, simplifica el entorno y, en definitiva, reduce el coste total de propiedad, así como el de la seguridad.

Muchas soluciones puntuales de seguridad tradicionales, como firewalls, sistemas de control de acceso, protección de antivirus en red, sistemas de detección y prevención de intrusiones (IPS), seguridad IP (IPSec), redes privadas virtuales (VPN) y VPN SSL (Secure Sockets Layer), se encuentran integradas ahora en plataformas de red seguras creadas con tecnología Cisco.

## Control y contención de amenazas

La solución de control y contención de amenazas de Cisco se compone de tecnologías avanzadas e innovadoras que van más allá de la simple defensa contra las amenazas: las controlan y contienen de forma dinámica y en colaboración. Las empresas no pueden permitirse los periodos de inactividad y las pérdidas en la productividad del negocio que se derivan de las brechas de seguridad. La solución de control y contención de amenazas no sólo protege los extremos vulnerables, si no también múltiples puntos de la infraestructura de red. En el actual entorno de seguridad, las amenazas desconocidas son tan dañinas como las conocidas. Las avanzadas tecnologías de Cisco supervisan y analizan, de modo continuo y dinámico, la actividad de la red, buscando comportamientos anómalos y potenciales amenazas desconocidas. Si se detecta una actividad sospechosa, las tecnologías de Cisco aplican automáticamente las políticas de seguridad, envían alarmas al personal responsable y proponen soluciones para los posibles problemas.

Las ventajas de la solución de control y contención de amenazas de Cisco incluyen:

- Protección dinámica contra amenazas conocidas y desconocidas
- Contención dinámica y mitigación distribuida de infecciones y ataques
- Administración de parches y actualizaciones para forzar la conformidad con la política de seguridad en el extremo de la red
- Menores costes operativos

Algunos ejemplos de tecnologías avanzadas que se utilizan para conseguir estas ventajas son la protección de extremos (estaciones de trabajo y servidores) basada en comportamientos, la mitigación distribuida de ataques de denegación de servicio (DdoS), la detección de intrusiones, la aplicación de las políticas de seguridad y las respuestas dinámicas.

## Comunicaciones confidenciales

La solución de comunicaciones confidenciales de Cisco permite que su organización obtenga las ventajas empresariales del uso de las comunicaciones inalámbricas, comunicación de voz, vídeo y datos, y a la vez pueda garantizar la privacidad e integridad de las comunicaciones críticas para la empresa a través de estos medios. La solución consiste en productos, tecnologías y servicios de red integrados, adaptables y que trabajan en colaboración, orientados a proteger las comunicaciones y ampliar, de forma económica, el alcance de la red para una fuerza de trabajo con alta movilidad. La solución incluye capacidades VPN avanzadas y soluciones completas para las comunicaciones inalámbricas y de voz seguras.

Las ventajas de la solución de comunicaciones confidenciales de Cisco incluyen:

- Mejoras en la productividad
- Mayor flexibilidad para usuarios remotos
- Privacidad y confidencialidad de las comunicaciones críticas de la empresa
- Ampliación del alcance de la red de bajo coste

Las avanzadas capacidades de Cisco incluyen una característica que elimina la información confidencial de la memoria y los discos duros (por ejemplo, en un quiosco Internet) cuando los usuarios finalizan las sesiones VPN SSL. Las soluciones de seguridad para conexiones inalámbricas y de voz incluyen servicios de autenticación de usuarios y productos y tecnologías de cifrado así como mecanismos de acceso seguro a las herramientas de administración, lucha contra el fraude, etc.

## Transacciones seguras

La agilidad de las organizaciones depende de transacciones entre una aplicación y otra en las empresas, y de transacciones desde y hacia los clientes.  En muchos casos, la información transaccional reside en aplicaciones muy vulnerables o que se han desarrollado de forma interna. Los hackers pueden aprovechar esos "agujeros" de seguridad en el código personalizado de estas aplicaciones vulnerables y robar, interceptar, cambiar o destruir datos vitales de las aplicaciones. La solución de transacciones seguras de Cisco ayuda a garantizar la seguridad y la disponibilidad de las aplicaciones vulnerables, y la privacidad de la información de alta sensibilidad que reside en ellas. La solución inspecciona y protege las transacciones de las aplicaciones mediante la inspección de Capa 4-7, el cifrado, la aplicación de políticas y el control de aplicaciones. Además, la solución de transacciones seguras garantiza que su sistema de seguridad cumpla con las normativas que exigen los gobiernos.

Las ventajas de la solución de transacciones seguras de Cisco incluyen:

- Legitimidad de transacciones de las aplicaciones
- Transacciones seguras entre aplicaciones
- Alta disponibilidad de las aplicaciones
- Privacidad del cliente
- Protección de los activos empresariales ante la exposición al exterior
- Reducción del riesgo de litigio

La solución de transacciones seguras de Cisco es un servicio de seguridad de la capa de aplicaciones que se extiende a toda la plataforma de red segura e implementa seguridad a nivel del protocolo de aplicación y a nivel de carga útil en los paquetes (payload), a fin de conseguir un control mayor y más exhaustivo.

## Administración operativa y control de políticas

La solución de administración operativa y control de políticas de Cisco es un conjunto estructurado de herramientas de administración de seguridad integrada, adaptable y en colaboración. Los administradores de hoy en día se enfrentan a un difícil reto. Son responsables de la aplicación de las políticas de seguridad en entornos empresariales muy complejos y que cambian constantemente. No sólo son responsables de la protección de los activos empresariales, si no que muchos

también tienen la responsabilidad de mantener la conformidad con las políticas de seguridad de la empresa y con las regulaciones del gobierno con relación a la privacidad. Las herramientas de administración operativa de Cisco ayudan a los administradores de seguridad en sus tareas rutinarias; en tanto que las herramientas de control de políticas les permiten mantener la conformidad requerida.

Las ventajas de la solución de administración operativa y control de políticas de seguridad de Cisco incluyen:

- Mayor velocidad y precisión en la implementación de seguridad
- Visibilidad de extremo a extremo del control de la seguridad
- Respuesta rápida a las amenazas
- Administración adecuada de los flujos de trabajo
- Ayuda con los informes de conformidad

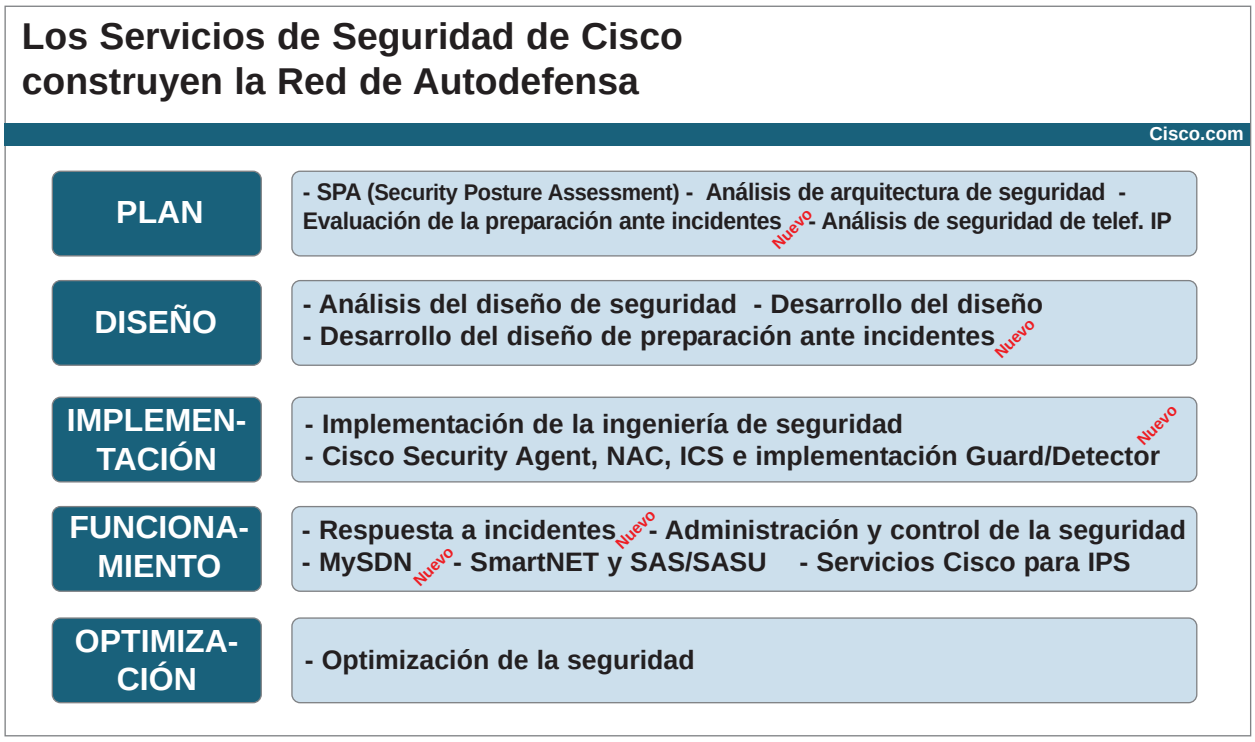
La eficaz tecnología de control, análisis y respuesta de Cisco simplifica la administración de seguridad y proporciona visibilidad de extremo a extremo sobre la información que se utiliza para la generación de informes de conformidad y el proceso de auditoría.

## SOLUCIONES DE SEGURIDAD INTEGRADA DE CISCO: UN CONJUNTO DE OFERTAS DE SEGURIDAD DE RED

Los galardonados productos y servicios de seguridad, distribución y soporte técnico de Cisco ofrecen las soluciones de seguridad que su empresa necesita.

### Servicio y soporte técnico de Cisco

Cisco ofrece los siguientes servicios de seguridad de red:




El modelo de Cisco para el servicio y soporte técnico se basa en el reconocimiento de la potencialidad de Internet para acelerar la resolución de los problemas de red, así como para permitir al cliente un acceso rápido a información crucial, la formación de su personal y un trabajo dinámico para la mejora del rendimiento global de la red.

Cisco.com es la base de un conjunto de aplicaciones de red interactivas que proporcionan acceso inmediato y abierto a la información, los recursos y sistemas de Cisco. A través de Cisco.com, los clientes y partners directos tienen acceso a numerosas aplicaciones, incluyendo aplicaciones Cisco ITS (Internet Technical Support), que ofrecen soluciones online de soporte técnico.

Para conseguir el máximo tiempo de actividad de la red, la asistencia técnica está disponible de forma continua por parte de los ingenieros del Cisco TAC (Technical Assistance Center) Para obtener más información, visite: http://www.cisco.com/tac.

## Servicios Avanzados de Cisco para la seguridad de red

Los consultores de los Servicios Avanzados de Cisco tienen certificaciones CCIE® y CISSP de nivel experto, y también la experiencia en planificación, diseño, implementación y optimización de grandes infraestructuras de seguridad de red para empresas líderes y organizaciones gubernamentales.

**Planificación y evaluación.** Cisco puede proporcionar una evaluación completa de la postura de seguridad de su organización, incluyendo un análisis de la arquitectura global de seguridad de la red y la preparación antes posibles incidencias. Esta evaluación del sistema de seguridad se lleva a cabo por expertos con una amplia experiencia práctica y genera una imagen del estado de la seguridad de la red, mediante una exhaustiva evaluación de los dispositivos, servidores, equipos y bases de datos de su red. Los expertos de Cisco analizan la seguridad de su red con relación a las prácticas recomendadas del sector, e identifican vulnerabilidades que pueden ser una amenaza para su organización. Basándose en este análisis en profundidad, Cisco ofrece recomendaciones sobre cómo mejorar la postura de seguridad global y establece prioridades en las acciones a seguir. Network Security Architecture Review es una evaluación general de la arquitectura de seguridad de su red, que identifica las acciones correctoras que le permitan obtener la conformidad con la norma ISO 17799, las prácticas recomendadas del sector y las políticas de seguridad internas de la empresa.

Diseñado para ayudar a las organizaciones a estar preparadas para la detección, la información y la respuesta frente a incidentes de seguridad, los Servicios Avanzados de Cisco ofrecen un conjunto de servicios de preparación y respuesta, incluyendo una evaluación del estado de la organización ante los incidentes (Incident Readiness Assessment), que analiza las prácticas recomendadas de una organización, las herramientas y procedimientos operativos, y la infraestructura de seguridad de red para identificar acciones que mejoren la preparación general ante los incidentes. Los Servicios Avanzados de Cisco también pueden evaluar la preparación de su red para admitir las nuevas soluciones de la Red de Autodefensa de Cisco, como el control de admisión de red (NAC), Cisco Security Agent y el software y dispositivos de Cisco IPS.

**Diseño.** Cisco puede trabajar con Ud. en el diseño de una sólida red de autodefensa. A través de un método arquitectónico detallado, los Servicios avanzados de Cisco pueden ayudarle a desarrollar una defensa multinivel contra los ataques directos de hackers, virus y gusanos. Puede utilizar el servicio de diseño de preparación ante incidentes (Incident Readiness Design Development) para de-sarrollar mejoras técnicas y procedimentales para sus herramientas, procedimientos, tecnología y administración de incidentes. Mediante este servicio, Cisco realiza recomendaciones para la mejora de su diseño de seguridad actual, incluyendo la topología de red, el emplazamiento de dispositivos y las conexiones. Tomando en cuenta todos los aspectos de la seguridad de red (como la capacidad de ampliación, el rendimiento y la administración), Cisco puede recomendar las configuraciones de protocolos, políticas de seguridad y características que mejoren la seguridad frente a las amenazas.

**Implementación.** Una red de autodefensa no sólo debe estar diseñada estratégicamente, si no también implementarse, configurarse e integrarse en la infraestructura de red con la máxima atención. Una vez que se ha definido el diseño de la solución de seguridad, los ingenieros de Cisco pueden dar soporte a su equipo mediante la implementación de tareas que ayuden a desplegar, configurar e integrar una nueva solución, como Cisco NAC, Cisco Security Agent, el software o los dispositivos de Cisco IPS, o Cisco Guard y Detector en su entorno de producción. Los ingenieros de Cisco pueden ofrece la experiencia necesaria para implementar y gestionar la solución de seguridad, reforzar la capacidad de su equipo para cumplir con exigentes fechas límite y, a la vez, minimizar las costosas interrupciones en su infraestructura.

**Funcionamiento y optimización.** Una vez que sus soluciones de seguridad se han diseñado e implementado con éxito, su infraestructura de red debe estar lista para admitir las demandas crecientes de las nuevas amenazas y del cambio en la dinámica de la empresa. Cisco Services for IPS proporciona información oportuna, actualizaciones de los archivos de

firmas y un completo soporte para las soluciones Cisco IPS. MySDN ofrece informes actualizados de inteligencia sobre las amenazas y vulnerabilidades actuales. El servicio Cisco de respuesta ante incidentes (Incident Response) está disponible para que expertos de seguridad de Cisco proporcionen asistencia a su personal durante un ataque a la red. A medida que cambian las condiciones de la red, los ingenieros de Cisco trabajarán con Ud. para llevar a cabo comprobaciones de optimización que ayuden a garantizar que la infraestructura de seguridad de su red cumple con los objetivos de rendimiento previstos.

## Servicios de Externalización de Cisco

### Soluciones de Servicios de Seguridad Gestionada de Cisco

Para que los proveedores de servicios puedan sacar partido de la creciente demanda de servicios de seguridad y servicios VPN gestionados, Cisco ofrece una amplia variedad de ofertas para una introducción del servicio rápida y eficiente. Los servicios VPN gestionados que se basan en IPSec, MPLS (Multiprotocol Label Switching) o ambos, permiten a los proveedores de servicios aumentar los servicios de conexión existentes con opciones de acceso remoto e interconexión entre redes. De esta forma, es posible ofrecer servicios de valor como telefonía IP, comercio electrónico, gestión de la cadena de suministro y distribución de contenido. Los servicios de seguridad gestionados, como los cortafuegos gestionados, la detección de intrusiones gestionadas o la detección y mitigación de ataques DdoS, pueden formar un paquete con otros servicios.

Al ofrecer servicios VPN o de seguridad gestionados, podrá utilizar de forma óptima las capacidades de los routers Cisco y los switches Cisco Catalyst® que usa actualmente para sus conexiones. De esta forma, la inversión actual se maximiza y los costes de implementación se minimizan, ampliando las oportunidades de servicios para obtener nuevos flujos de ingresos.

### El Programa Cisco Powered Network

Los proveedores de servicios que muestran el logotipo Cisco Powered se han ganado este derecho por haber mantenido altos niveles de calidad de red y por la construcción de sus servicios con equipamiento de Cisco; el mismo equipamiento a través del cual viaja prácticamente todo el tráfico de Internet. Los servicios que ofrecen estos proveedores son fiables y seguros.

### Partners de canal de Cisco

El Programa de especialización en seguridad de Cisco (Cisco Security Specialization) reconoce a los partners de canal de Cisco que han desarrollado las habilidades necesarias para vender, diseñar, instalar y mantener las soluciones de seguridad de Cisco de los clientes. A medida que se adoptan rápidamente las soluciones empresariales de Internet, los partners con especialización de seguridad podrán solventar la creciente demanda de implementación de seguridad y servicios de soporte técnico.

## Servicios de Formación de Cisco

### Certificaciones de Seguridad de Cisco

A través de los mejores cursos de formación y exámenes del sector, las certificaciones de seguridad de Cisco confirman las habilidades y las competencias de los profesionales de la seguridad. La certificación Cisco CCSP™ para profesionales de seguridad y las tres certificaciones de seguridad relacionadas-Cisco VPN Specialist, Cisco Firewall Specialist, y Cisco IDS Specialist (para sistemas de detección de intrusiones [IDSs])-responden a las demandas del sector y proporcionan una ruta de certificación profesional en el mercado de la seguridad TI. La certificación CCSP garantiza que su personal tiene la capacidad de implementar con pleno éxito soluciones de seguridad de extremo a extremo.

### Partners autorizados de formación orientada a la seguridad de Cisco

Muchos partners autorizados de formación de Cisco en todo el mundo se centran en la formación de seguridad y ofrecen cursos, laboratorios remotos, materiales de autoaprendizaje y otros recursos sobre las tecnologías de seguridad más recientes. Aquí se pueden incluir dispositivos avanzados de seguridad Cisco PIX®, sistemas de detección de intrusiones

de Cisco, implementaciones de diseño Cisco SAFE y la administración de seguridad de red de Cisco. Se puede encontrar una herramienta para localizar cursos, información, fechas de exámenes y una lista detallada de los partners orientados a la seguridad en:
http://www.cisco.com/go/training.

### Ecosistema de Seguridad de Cisco

Los productos, tecnologías y servicios de la cartera de Cisco son elementos fundamentales del éxito de una solución de seguridad de red. Un método global para la seguridad de red debe tener en cuenta también otras áreas, como la creación de un "ecosistema de seguridad" que haga un uso óptimo de las ventajas que ofrece la línea de productos de Cisco. Este ecosistema incluye varios elementos importantes, como productos de terceros con capacidad de interoperatividad, servicios de implementación, atención al cliente y ofertas de servicio compatibles.

El programa de partners de desarrollo tecnológico de Cisco es un programa de evaluación y marketing conjunto que comprueba la interoperatividad de soluciones complementarias de seguridad de terceros con los productos de Cisco. El programa convierte productos independientes en soluciones de seguridad más eficaces, y ofrece implementaciones probadas y fiables para los clientes de Cisco.

## RESUMEN

Actualmente, la seguridad es una arquitectura de base para todas las tecnologías de comunicaciones de Cisco. Ya sea en la instalación de routers, la seguridad de la infraestructura de conmutación, la implementación de avanzadas tecnologías como voz, vídeo o conexiones inalámbricas que mejoran la productividad, o la protección de los datos almacenados en toda la organización, la seguridad es un componente fundamental de cada pieza de la red. La Red de Autodefensa de Cisco -un conjunto estructurado de sistemas estratégicos integrados, adaptables y en colaboración- ayuda a que organizaciones de todos los tamaños puedan pasar de complejas soluciones puntuales a una seguridad dinámica y simplificada de extremo a extremo. La Red de Autodefensa de Cisco hace posible que las organizaciones puedan implementar prácticas empresariales seguras; reduzcan el riesgo y la complejidad; mantengan bajo control el coste total de propiedad; y protejan, optimicen y amplíen sus negocios.

Para obtener más información sobre la Red de Autodefensa y los sistemas estratégicos de Cisco con relación a la seguridad de la información, visite:
http://www.cisco.com/go/sdn
http://www.cisco.com/go/securityconsulting


**Sede central**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
EE.UU.
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

**Sede en Europa**
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
Países Bajos
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

**Sede en América**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
EE.UU.
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

**Sede en Asia Pacifico**
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799


**Cisco Systems tiene más de 200 oficinas en los siguientes países y regiones. Las direcciones, números de teléfono y de fax se pueden encontrar en el sitio Web Cisco.com en www.cisco.com/go/offices.**

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




C02-332256-00 02/06