Dispositivos de seguridad Cisco Email Security Appliance

Durante los últimos 20 años, el correo electrónico ha dejado de ser una herramienta que utilizaban principalmente los técnicos y los investigadores para convertirse en la red troncal de las comunicaciones corporativas. Cada día se intercambian más de 100 000 millones de mensajes de correo electrónico corporativos. A medida que crece el uso del correo electrónico, la seguridad cobra mayor importancia. Efectivamente, las campañas de spam masivo han dejado de ser el único foco de preocupación. En la actualidad, el spam y el malware son simplemente piezas de un complejo panorama que incluye tanto amenazas que entran como riesgos que salen.

Las soluciones de Cisco® Email Security ofrecen protección para el correo electrónico de alta disponibilidad frente a las amenazas dinámicas y en constante evolución que afectan a las organizaciones hoy en día. Con sus soluciones basadas en appliances virtuales, en la nube e híbridas, Cisco Email Security ha sido reconocido por analistas independientes como un producto líder que ofrece:

- **Protección más rápida e integral para el correo electrónico** que, a menudo, va horas o días por delante de la competencia.
- **Acceso a una de las redes más grandes de inteligencia de amenazas con Cisco Talos**, que se basa en análisis de seguridad colectiva en tiempo real.
- **Protección de mensajes salientes,** mediante funciones integradas como la prevención de la pérdida de datos (DLP), el cifrado del correo electrónico y la integración opcional con la solución DLP para empresas de RSA.
- **Coste total de propiedad bajo,** gracias a ventajas como son su tamaño reducido, una sencilla implementación y la administración automatizada, que permiten ahorrar a largo plazo.

Descripción general del producto

La solución integral de Cisco ofrece una implementación sencilla y rápida, con poco mantenimiento, baja latencia y costes operativos reducidos. Nuestra tecnología diseñada para “configurar y olvidarse” libera al personal una vez que se activa la configuración automática de políticas. A continuación, el sistema envía automáticamente actualizaciones de seguridad a la solución de inteligencia de amenazas basada en la nube de Cisco. Los datos de inteligencia de amenazas se actualizan en los dispositivos de seguridad Cisco Email Security Appliance (ESA) cada tres o cinco minutos, lo cual le ofrece una capacidad de respuesta frente a amenazas actualizada y líder en el sector que va horas o días por delante de la competencia. La flexibilidad en términos de opciones de implementación y la perfecta integración con su infraestructura de seguridad existente convierten a Cisco Email Security en una opción excelente para sus necesidades empresariales.

Appliance virtual

El Cisco Email Security Virtual Appliance (ESAV) reduce considerablemente el coste de implementación de la seguridad para el correo electrónico, especialmente en redes muy distribuidas. El dispositivo permite al administrador de red crear instancias donde y cuando se necesiten utilizando la infraestructura de red existente. El Cisco ESAV es una versión de software del Cisco ESA y funciona junto con un VMware ESXi Hypervisor, y con servidores Cisco Unified Computing Systems™ (Cisco UCS®). Por la compra de cualquiera de los paquetes de software de Cisco Email Security, recibirá una licencia ilimitada para Cisco ESAV.

Con Cisco ESAV, puede responder al instante al aumento del tráfico con una planificación de la capacidad simplificada. No es necesario comprar y recibir los appliances por correo: puede aprovechar las nuevas oportunidades de negocio sin añadir complejidad al Data Center ni tener que contratar a personal adicional.

Características y ventajas

Cisco Email Security protege sus sistemas de correo electrónico más importantes con soluciones híbridas, virtuales, en la nube o basadas en appliances. Cisco Email Security ha sido reconocida por analistas independientes como la mejor fuente de soluciones de seguridad para el correo electrónico. En la Tabla 1 se resumen las principales características y ventajas de las soluciones de Cisco Email Security.

Tabla 1. Características y ventajas

Característica	Ventaja
Inteligencia sobre amenazas globales	Obtenga protección rápida e integral para correo electrónico, respaldada por una de las redes más grandes de detección de amenazas del mundo. Cisco Email Security proporciona una visibilidad amplia y una enorme presencia a nivel global que incluye: • 100 TB de inteligencia de seguridad diaria • 1,6 millones de dispositivos de seguridad implementados: firewalls, sensores del sistema de prevención de intrusiones (IPS) de Cisco y dispositivos web y de correo electrónico • 150 millones de terminales • 13 000 millones de solicitudes web al día • 35% del tráfico de correo electrónico empresarial mundial Cisco Talos proporciona una vista de la actividad global del tráfico las 24 horas del día. Analiza anomalías, descubre nuevas amenazas y supervisa las tendencias del tráfico. Cisco Talos contribuye a prevenir los ataques de hora cero generando continuamente nuevas reglas que envían actualizaciones a los ESA de Cisco. Estas actualizaciones se realizan cada tres o cinco minutos, proporcionando una defensa contra las amenazas líder en el sector.
Bloqueo de spam	El spam es un problema complejo que exige una sofisticada solución. Con Cisco es muy fácil. Para evitar que el spam llegue a los buzones de entrada, una defensa multicapa combina una capa externa de filtrado basada en la reputación del remitente y una capa interna de filtrado que realiza un análisis en profundidad del mensaje. Con el filtrado de reputación, más del 80% del spam se bloquea antes incluso de que llegue a la red. Las mejoras recientes incluyen análisis contextual y automatización mejorada, así como la autoclasificación, con el fin de proporcionar una potente defensa frente a las campañas de Snowshoe. Los clientes que manejan grandes volúmenes de correo electrónico en breves períodos de tiempo podrán aplicar filtros basados en el remitente o el asunto, que bloquearán los mensajes asociados o los pondrán en cuarentena.

Característica	Ventaja
Protección frente a malware avanzado	Los Cisco ESA ahora incluyen protección frente a malware avanzado (AMP), una solución de defensa frente al malware que aprovecha la amplia red de inteligencia de seguridad en la nube que proporciona Sourcefire (que ahora forma parte de Cisco). Proporciona protección a lo largo de todo el ciclo de ataque: antes, durante y después del mismo. También ofrece puntuación y bloqueo según la reputación, sandboxing de archivos y retrospección de archivos para realizar un análisis continuo de las amenazas, incluso después de que hayan cruzado el gateway del correo electrónico. Los usuarios pueden bloquear más ataques, llevar a cabo un seguimiento de los archivos sospechosos, mitigar el alcance de un brote y remediarlo rápidamente. AMP está disponible para todos los clientes de Cisco ESA como función con una licencia adicional.
Control de mensajes salientes	Los ESA de Cisco controlan los mensajes salientes a través de DLP, el cifrado del correo electrónico y la integración opcional con RSA Enterprise Manager. Este control ayuda a garantizar que los mensajes más importantes cumplan con los estándares del sector y estén protegidos durante el tránsito. Además, el análisis antivirus y antispam de los mensajes salientes, junto con la limitación de la velocidad de datos salientes, se pueden utilizar para evitar que los equipos o las cuentas que se encuentren en riesgo en su empresa se incluyan en las listas negras de correo electrónico. Novedad: El ESA ahora soporta la firma y el cifrado Secure/Multipurpose Internet Mail Extensions (S/MIME), además del protocolo Transport Layer Security (TLS).
Excelente rendimiento	Los ESA de Cisco bloquean rápidamente los nuevos virus del correo electrónico entrante. Las colas de entrega de dominio evitan que los correos electrónicos que no se pueden entregar provoquen un atasco para las entregas críticas a otros dominios.
DLP	Puede utilizar una o más políticas predefinidas (hay más de 100 entre las que elegir) para evitar que los datos confidenciales salgan de la red. Si lo prefiere, puede utilizar partes de estas políticas predefinidas para crear sus propias políticas personalizadas. El motor de DLP de correo electrónico de RSA incorporado utiliza estructuras de datos preajustadas junto con sus propios puntos de datos opcionales, como palabras, frases, diccionarios y expresiones regulares, para crear rápidamente políticas precisas con un nivel mínimo de falsos positivos. El motor DLP puntúa las infracciones por gravedad, por lo que puede aplicar diferentes niveles de remediación según sus necesidades.
Bajo coste	Su formato reducido, la configuración sencilla y la gestión automatizada de actualizaciones se traducen en un ahorro durante la vida de la solución Cisco Email Security. La solución de Cisco tiene uno de los costes totales de propiedad más bajos del mercado.
Implementación flexible	Todas las soluciones de Cisco Email Security comparten un enfoque sencillo en términos de implementación. El asistente de configuración del sistema puede gestionar incluso entornos complejos y, en cuestión de minutos, conseguirá que su sistema se encuentre protegido y listo para funcionar, lo que permitirá que sea más seguro y más rápido. La licencia se basa en el número de usuarios, no en el número de dispositivos, por lo que puede aplicarla por usuario en lugar de por dispositivo y ofrecer protección los datos entrantes y salientes del correo electrónico sin coste adicional. Esta función le permite analizar mensajes salientes con los motores antivirus y antispam para responder así a las necesidades de su empresa. Cisco ESAV ofrece las mismas funciones que Cisco ESA, con la comodidad añadida y el ahorro de costes del modelo de implementación virtual. Cisco ESAV ofrece aprovisionamiento con autoservicio inmediato. Con una licencia de Cisco ESAV, puede implementar gateways virtuales de seguridad para el correo electrónico en la red sin conexiones a Internet. La licencia de Cisco ESAV incluye licencias de software integradas. Puede aplicar licencias en cualquier momento a un nuevo archivo de imagen virtual de Cisco ESAV almacenado a nivel local. Si es necesario, los archivos de imagen virtual limpios se pueden clonar, lo que ofrece la posibilidad de implementar varios gateways de seguridad para el correo electrónico de manera inmediata. Puede ejecutar soluciones de Cisco Email Security de hardware y virtuales en la misma implementación. De este modo, las pequeñas sucursales o las ubicaciones remotas pueden contar con la misma protección que la sede central sin necesidad de instalar y mantener el hardware en las distintas ubicaciones. Puede gestionar fácilmente las implementaciones personalizadas con el appliance de gestión de seguridad de contenido (SMA) de Cisco o el appliance virtual de gestión de seguridad de contenido (SMAV) de Cisco.
Soluciones que se adecuan a sus clientes	La solución basada en la nube es un servicio completo y fiable que incluye software, potencia informática y soporte. La interfaz de usuario gestionada conjuntamente es idéntica a la de Cisco ESA y ESAV. Por lo tanto, consigue una protección excepcional con poca carga administrativa y sin hardware in situ que supervisar y gestionar. La solución híbrida ofrece control avanzado de los mensajes confidenciales salientes in situ y, al mismo tiempo, le permite beneficiarse de las ventajas económicas de la nube. Los appliances de hardware y virtuales in situ están listos para conectarse. Puede elegir el modelo que mejor se adapte a su entorno para proteger los mensajes entrantes y salientes en el gateway.

Especificaciones del producto

La Tabla 2 incluye las especificaciones de rendimiento de Cisco ESA, la Tabla 3 contiene las especificaciones de hardware de Cisco ESA, la Tabla 4 resume las especificaciones de Cisco ESAV y la Tabla 5 muestra las especificaciones del appliance de gestión de seguridad de contenido (SMA) de Cisco.

Tabla 2. Especificaciones de rendimiento de Cisco ESA

Implementación	Modelo	Espacio en disco	Duplicación de RAID	Memoria	CPU
Grandes empresas	ESA C680 de Cisco	1,8 TB (600 x 3)	Sí (RAID 10)	32 GB	2 x 6 (2 procesadores de 6 núcleos)
Medianas empresas	ESA C380 de Cisco	1,2 TB (600 x 2)	Sí (RAID 1)	16 GB	1 x 6 (1 procesador de 6 núcleos)
Pequeñas y medianas empresas o sucursales	ESA C170 de Cisco	500 GB (250 x 2)	Sí (RAID 1)	4 GB	1 x 2 (1 procesador de dos núcleos)

Nota: Para elegir el tamaño adecuado, consulte el índice máximo de flujo de correo y el tamaño medio de los mensajes con un especialista en seguridad de contenido de Cisco.

Tabla 3. Especificaciones de hardware de Cisco ESA

Modelo	Cisco ESA C680	Cisco ESA C380	Cisco ESA C170
Unidades en rack (RU)	2 RU	2 RU	1 RU
Dimensiones (Al. x An. x Pr.)	3,5 x 19 x 29 pulg. (8,9 x 48,3 x 73,7 cm)	3,5 x 19 x 29 pulg. (8,9 x 48,3 x 73,7 cm)	1,67 pulg. x 16,9 pulg. x 15,5 pulg. (4,24 x 42,9 x 39,4 cm)
Opción de alimentación de CC	Sí	Sí	No
Ciclo de alimentación remota	Sí	Sí	No
Fuente de alimentación redundante	Sí	Sí	No
Disco duro intercambiable sin reiniciar el sistema	Sí	Sí	Sí
Interfaces Ethernet	Tarjetas de interfaz de red (NIC) de 4 gigabits, RJ-45	NIC de 4 gigabits, RJ-45	NIC de 2 gigabits, RJ-45
Velocidad (Mbps)	10/100/1000, negociación automática	10/100/1000, negociación automática	10/100/1000, negociación automática
Opción de 10 Gigabit Ethernet sobre fibra	Sí (accesoria)	No	No

Tabla 4. Especificaciones del Cisco ESAV

Usuarios de correo electrónico				
Usuarios de correo electrónico	**Modelo**	**Disco**	**Memoria**	**Núcleos**
Solo para evaluaciones	ESAV C000v de Cisco	250 GB (SAS 10K SAS)	4 GB	1 (2,7 Ghz)
Pequeña empresa (hasta 1000)	ESAV C100v de Cisco	250 GB (SAS 10K SAS)	6 GB	2 (2,7 Ghz)
Mediana empresa (hasta 5000)	ESAV C300v de Cisco	1024 GB (SAS 10K SAS)	8 GB	4 (2,7 Ghz)
Grandes empresas o proveedores de servicios	Cisco ESAV C600v	2032 GB (10 000 RPM SAS)	8 GB	8 (2,7 Ghz)
Servidores				
Cisco UCS	Hipervisor VMware ESXi 5.0, 5.1 y 5.5			

Tabla 5. Especificaciones de la plataforma SMA de Cisco serie M

Modelo	Cisco SMA M680	Cisco SMA M380	Cisco SMA M170
Cantidad de usuarios	Más de 10 000	Hasta 10 000	Hasta 1000

Dónde implementarlo

Puede implementar las soluciones Cisco Email Security:

- **En las instalaciones:** Cisco ESA es un gateway de correo electrónico implementado normalmente en una zona desmilitarizada. El tráfico entrante de protocolo simple de transferencia de correo (SMTP) se dirige a la interfaz de datos de Cisco ESA según las especificaciones establecidas por los registros de intercambio de correo. Cisco ESA lo filtra y lo envía de vuelta al servidor de correo de la red. El servidor de correo envía el correo saliente a la interfaz de datos de Cisco ESA, donde se filtra según las políticas del correo electrónico saliente y se entrega a los destinos externos.
- **Virtualmente:** Con Cisco UCS en su sucursal pequeña, puede alojar Cisco ESAV con otros productos de Cisco, como el dispositivo virtual Cisco Web Security Appliance (WSAV). Juntos, ofrecen el mismo grado de protección que sus equivalentes en hardware, pero suponen un ahorro de dinero en recursos de espacio y de alimentación. Puede administrar de manera centralizada esta implementación personalizada con Cisco SMA o SMAV.

Opciones de seguridad en la nube

Cisco Cloud Email Security le proporciona un modelo de implementación flexible de seguridad para el correo electrónico. Le ayuda a reducir costes gracias a la gestión conjunta y al hecho de no contar con ninguna infraestructura de seguridad de correo electrónico in situ.

Cisco Hybrid Email Security le ofrece las ventajas de Cloud Email Security, los controles salientes avanzados del cifrado de mensajes y la prevención de la pérdida de datos in situ. Esta solución híbrida le permite llevar a cabo la transición a una solución en la nube a su propio ritmo.

Cisco Email Security: Licencias de los appliances físicos y virtuales

Con todos los paquetes de software de Cisco Email Security (Cisco Email Security Inbound, Cisco Email Security Outbound o Cisco Email Security Premium) se incluye una licencia de Cisco ESAV. Esta licencia tiene el mismo plazo de validez que el resto de servicios de software del paquete y puede utilizarse para tantas instancias virtuales como sean necesarias, siempre que se mantenga dentro del número de usuarios para los que la haya adquirido. Las licencias de Cisco ESA se incluyen en todos los paquetes de software de Cisco Email Security. Solo tiene que comprar las licencias correspondientes al número de cuentas de correo que vaya a gestionar y, a continuación, deberá adquirir los appliances adecuados para las instalaciones. En el caso de los appliances virtuales, pida simplemente las licencias de software.

Licencias de suscripción basadas en plazos

Las licencias son suscripciones basadas en plazos de 1, 3 o 5 años.

Licencias de suscripción basadas en cantidad

La cartera de Cisco Email Security ofrece precios por niveles en función del número de cuentas. Los representantes de ventas y de los partners le ayudarán a determinar la implementación adecuada.

Licencias de software de Cisco Email Security

Existen tres paquetes de licencia de software de Cisco Email Security disponibles, además de una opción independiente que se adquiere por separado: Cisco Email Security Inbound, Cisco Email Security Outbound, Cisco Email Security Premium y la protección frente a malware avanzado. Los componentes principales de cada una de las opciones de software se indican en la Figura 6.

Tabla 6. Componentes de software

Paquetes	Descripción
Cisco Email Security Inbound Essentials	El paquete Cisco Email Security Inbound Essentials ofrece protección frente a las amenazas basadas en correo electrónico e incluye la solución antispam, la solución antivirus Sophos, los filtros de brote de virus y el clustering.
Cisco Email Security Outbound Essentials	El paquete Cisco Email Security Outbound Essentials protege frente a la pérdida de datos mediante el cumplimiento de DLP, el cifrado del correo electrónico y el clustering.
Cisco Email Security Premium	El paquete Cisco Email Security Premium combina la protección de datos entrantes y salientes que se incluye en las dos licencias Cisco Email Security Essentials especificadas, por lo que ofrece protección frente a las amenazas procedentes del correo electrónico y la prevención de la pérdida de datos básica.
Opción independiente	**Descripción**
Protección frente a malware avanzado de Cisco	La protección frente a malware avanzado (AMP) de Cisco puede adquirirse por separado junto con cualquier paquete de software de Cisco Email Security. AMP es una solución de protección frente a malware exhaustiva que permite el bloqueo y la detección de malware, así como el análisis continuo y las alertas retrospectivas de este tipo de amenaza. AMP aumenta la detección antimalware y las funciones de bloqueo que ya ofrece Cisco Email Security con la puntuación y bloqueo según la reputación del archivo, el sandboxing de archivos y la retrospección de archivos para conseguir un análisis continuo de las amenazas, incluso después de que hayan cruzado el gateway de correo electrónico.

Contratos de licencia de software

Con cada compra de una licencia de software se proporcionan el acuerdo de licencia del usuario final (EULA) de Cisco y el acuerdo de licencia del usuario final complementario de Cisco Web Security (SEULA).

Soporte de suscripción de software

Todas las licencias de Cisco Email Security incluyen soporte de suscripción de software, que resulta esencial para que las aplicaciones vitales para la empresa estén siempre disponibles, sean sumamente seguras y funcionen a pleno rendimiento. Este soporte le proporciona los servicios que aparecen a continuación durante el plazo de la suscripción de software que haya adquirido.

- Las actualizaciones de software permiten a las aplicaciones ofrecer el mejor rendimiento, con las funciones más modernas.
- El centro Cisco Technical Assistance Center (TAC) proporciona soporte técnico especializado rápidamente.
- Las herramientas online crean y amplían los conocimientos del personal interno y aumentan la agilidad empresarial.
- La formación colaborativa ofrece oportunidades de formación y conocimientos adicionales.

Servicios de Cisco

En la Tabla 7 se resumen los servicios de Cisco disponibles para las soluciones Cisco Email Security.

Tabla 7. Servicios de Cisco para las soluciones Cisco Email Security

Servicio	Descripción
Servicios de la marca Cisco	• El servicio de planificación y diseño de seguridad de Cisco le permite implementar una solución de seguridad robusta de forma rápida y rentable. • El servicio remoto de instalación y configuración de Cisco Email Security reduce los riesgos de seguridad instalando, configurando y comprobando el correcto funcionamiento de su solución. • El servicio de optimización de la seguridad de Cisco presta apoyo a un sistema de seguridad en constante evolución para poder enfrentarse a las nuevas amenazas de seguridad, mediante el diseño, ajustes de rendimiento y cambios en el sistema.
Servicios de colaboración y para partners	• El servicio de evaluación de la seguridad de los dispositivos conectados a la red de los servicios profesionales de colaboración de Cisco ayuda a mantener un entorno de red reforzado, ya que identifica las brechas de seguridad. • El servicio Cisco Smart Care Service consigue que el negocio funcione como la seda gracias al control proactivo que utiliza inteligencia de visibilidad segura que posibilita un buen rendimiento de la red. • Los partners de Cisco también ofrecen una amplia gama de servicios adicionales a través del ciclo de vida de planificación, diseño, implementación y optimización.
Financiación de Cisco	Cisco Capital® puede adaptar soluciones de financiación a las necesidades empresariales de sus clientes. Adquiera la tecnología de Cisco de una manera más rápida y disfrute antes de sus ventajas.

Servicios de soporte de Cisco SMARTnet

Para obtener el máximo valor de su inversión en tecnología, puede adquirir el Servicio Cisco SMARTnet® para que pueda utilizarlo con los ESA de Cisco. El servicio Cisco SMARTnet le ayuda a resolver rápidamente los problemas de la red mediante el contacto directo y en cualquier momento con los expertos de Cisco, una serie de herramientas de autoasistencia y la sustitución rápida del hardware. Para obtener más información, visite http://www.cisco.com/go/smartnet.

Cómo evaluar los ESA de Cisco

La mejor forma de entender las ventajas de las plataformas ESA de Cisco series C y X es participar en el programa Try Before You Buy. Para recibir un appliance de evaluación completamente funcional y probarlo en su red sin coste alguno durante 45 días, visite http://www.cisco.com/go/esa.

Cómo evaluar los servicios de Cisco Cloud Email Security Services

La solución basada en la nube es un servicio fiable y completo que ofrece un modelo de implementación flexible de la seguridad para el correo electrónico. Reduce los costes personales gracias a la gestión conjunta y al hecho de no necesitarse ninguna infraestructura de seguridad de correo electrónico in situ. Su equipo de cuentas de Cisco o su distribuidor pueden ayudarle a instalar una evaluación gratuita válida durante 45 días.

Cómo evaluar los ESAV de Cisco

1. Visite http://www.cisco.com/go/esa.
2. En “Support” (Asistencia) en el lado derecho, haga clic en “Software Downloads, Release and General Information” (Descargas de software, versiones e información general). Haga clic en “Download Software” (Descargar software) y, a continuación, haga clic en el enlace de cualquier modelo para ver las imágenes de las máquinas virtuales disponibles para su descarga. También verá una licencia de evaluación XML descargable. Tendrá que descargar una de las imágenes y la licencia de evaluación XML.
3. Descargue la siguiente documentación desde Cisco.com:
   a. Guía de instalación del appliance virtual de Cisco Security
   b. Documentación para Cisco IronPort® Manufacturing - AsyncOS 9.0
4. Siga las instrucciones de la guía de instalación del appliance virtual de Cisco Security para empezar. Tenga en cuenta que las evaluaciones de los appliances virtuales de seguridad de contenido de Cisco no están cubiertas por el Servicio Cisco SMARTnet y, por lo tanto, no se obtendrá soporte.

Información sobre la garantía

Encontrará más información en la página de Garantías de los productos de Cisco.com.

¿Por qué Cisco?

La seguridad es más importante que nunca para su red. Dado que las amenazas y los riesgos persisten, junto con los problemas relativos a la confidencialidad y el control, la seguridad es necesaria para proporcionar continuidad empresarial, proteger información valiosa y mantener la reputación de la marca. Las soluciones de seguridad integrada de Cisco, incluidas en el fabric de la red, le ofrecen mayor visibilidad y control para proteger su empresa sin interrupciones. Nuestro liderazgo en el mercado, la protección frente a amenazas avanzadas (antes, durante y después de un ataque), los productos innovadores y nuestra dilatada trayectoria nos convierten en el proveedor adecuado para satisfacer sus necesidades de seguridad.

Para obtener más información

Para obtener más información, visite http://www.cisco.com/go/ucs

Sede central en América
Cisco Systems, Inc.
San José, CA

Sede central en Asia-Pacífico
Cisco Systems (EE. UU.) Pte, Ltd.
Singapur

Sede central en Europa
Cisco Systems International BV Amsterdam,
Países Bajos

Cisco tiene más de 200 oficinas en todo el mundo. Las direcciones, números de teléfono y fax se encuentran en la Web de Cisco en **www.cisco.com/go/offices**.

Impreso en EE. UU. C78-729751-05 12/14