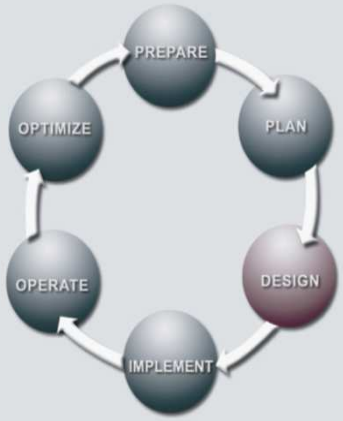
Security Design Services de Cisco

Creando soluciones de seguridad integrada para incrementar la seguridad, disponibilidad y desempeño

METODOLOGIA DEL CICLO DE VIDA DE LOS SERVICIOS



La metodología exclusiva del Ciclo de Vida de los Servicios de Cisco define las actividades necesarias en cada fase del ciclo de vida de la red para ayudar a asegurar la excelencia de los servicios. A través de esta metodología, que une las fuerzas de Cisco, nuestros partners especializados en redes y nuestros clientes, es posible obtener mejores resultados.

Fases del Ciclo de la Red

- **Preparación -** Desarrollo de plan de negocios para justificar la inversión tecnológica
- **Planeación -** Evaluación del estado actual de la red para soportar la solución propuesta
- **Diseño -** Creación de un diseño detallado para manejar requerimientos técnicos y de negocios
- **Implementación -** Despliegue de la nueva tecnología
- **Operación -** Mantenimiento de la salud de la red en el día a día de las operaciones
- **Optimización -** Alcance de la excelencia operacional a través de mejoras permanentes

VISIÓN GENERAL DEL SERVICIO

Conforme el número y la complejidad de las amenazas de seguridad a la red crecen, proteger la red corporativa se vuelve cada vez más importante. Aun cuando su organización comprenda las amenazas a las cuales debe responder, adaptar la arquitectura de seguridad de la red para resolverlas puede ser difícil. Un diseño defectuoso puede reducir la efectividad de nuevas soluciones de seguridad, retrasar el despliegue e incrementar los costos de integración.

Los Security Design Services de Cisco, diseñados para grandes empresas, ahora son parte de la fase de diseño del enfoque de Lifecycle Services de Cisco®. Los consultores de Cisco Systems® pueden trabajar con su organización para desarrollar un sólido diseño de seguridad. La metodología de diseño de Cisco considera todos los aspectos de su seguridad de red y su integración con la infraestructura central de la red. Utilizando un enfoque profundo y de tipo arquitectónico basado en estándares de la industria, los expertos en seguridad de Cisco pueden ayudar a desarrollar una defensa de múltiples capas contra ataques dirigidos por hackers o ataques indiscriminados de virus o gusanos (worms).

Al tomar un enfoque tipo arquitectónico, la infraestructura de seguridad diseñada por Cisco está creada para durar y puede evolucionar con el paso del tiempo para soportar el despliegue de nuevas aplicaciones de negocios. Además, al especificar un conjunto común de soluciones, políticas y prácticas de seguridad que pueden replicarse a todo lo largo y ancho de su organización, Cisco puede ayudarle a reducir los costos operativos de su red al ahorrarle tiempo y dinero en administración de seguridad de red, reduciendo el costo total de propiedad de su red.

Los servicios de Security Design de Cisco comprenden los dos siguientes componentes:

- **Security Design Review** – Revisa su diseño actual de seguridad de red para identificar las vulnerabilidades de arquitectura, diseño e implementación y proveer recomendaciones para construir, mejorar o recrear la ingeniería de su diseño de seguridad de red
- **Security Design Development** – Ayuda a desarrollar la estrategia, plan y diseño detallado para integrar soluciones de seguridad nuevas o mejoradas a su infraestructura de red

SECURITY DESIGN REVIEW

Alineando el diseño de seguridad de red con los objetivos empresariales y de seguridad

Los expertos de seguridad de red de Cisco conducen una revisión colaborativa de la estrategia de negocios de su organización y los objetivos, requerimientos y estándares de seguridad relacionados con la misma. Los ingenieros de Cisco entonces proveen un profundo análisis del diseño de seguridad de red para determinar su efectividad para cumplir con sus estrategias

de negocios y TI. Basado en un análisis de la información de red recabada, los ingenieros de Cisco proveen una revisión detallada de las vulnerabilidades de su red (Tabla 1), para ayudar a asegurar que el diseño de seguridad cumpla con las comprobadas mejores prácticas de diseño de seguridad de red de la industria.

Después de evaluar el diseño existente para detectar vulnerabilidades, los ingenieros de Cisco identifican y priorizan los requerimientos de seguridad para soluciones de red, incluyendo detección de intrusiones, acceso remoto, protección del borde, mitigación de amenazas, control de perímetro y VPNs. Cisco puede recomendar mejoras a su diseño de red incluyendo topología de red, colocación de dispositivos y conectividad. Tomando en cuenta todos los aspectos de su seguridad de red – incluyendo escalabilidad, desempeño y capacidad de administración, Cisco puede recomendar mejoras en protocolos, políticas y funciones para componentes individuales de seguridad.

Tabla 1. Actividades, metodología y entregables del Security Design Review

Actividades	Metodología y entregable
• Revisar sus metas, objetivos y requerimientos de seguridad de red • Revisar su arquitectura y diseño de seguridad de red existente • Identificar y analizar las vulnerabilidades de arquitectura y diseño • Proveer un análisis detallado de los componentes de seguridad de red, incluyendo: – Dispositivos de perímetro – Dispositivos de control de admisión a la red – Dispositivos de mitigación de amenazas – Dispositivos de acceso remoto – Sistemas de detección de intrusiones – Firewalls – Protección de puntos en el borde – Routers y switches – Conexiones de Extranet – Sistemas de administración de seguridad • Recomendar mejoras a la topología, componentes, funciones y características • Desarrollar configuraciones muestra para firewalls, dispositivos NAC, dispositivos de mitigación de amenazas, sistemas de detección de intrusiones, protección del borde, routers, switches, VPNs, servidores de control de acceso, dispositivos inalámbricos y herramientas de administración de seguridad • Especificar requerimientos de hardware y software incluyendo herramientas de administración de seguridad de red • Proveer recomendaciones para administración y mantenimiento continuo de la solución de seguridad	**Metodología** • Conducir un taller de diseño para recabar información e iniciar la revisión del diseño • Analizar el diseño actual de seguridad de red contra la estrategia y requerimientos organizacionales • Proveer un análisis preliminar y final de brechas basado en las mejores prácticas de la industria • Entregar un análisis del impacto de nuevos requerimientos de seguridad en la infraestructura de red • Recomendar mejoras al diseño de infraestructura de seguridad **Entregable** • Un documento de Revisión de Diseño de Seguridad que identifica las vulnerabilidades existentes en la red; recomienda mejoras al diseño, componentes y funciones generales de seguridad; y provee diagramas de red y configuraciones muestra

SECURITY DESIGN DEVELOPMENT

Aplicando una estrategia y un diseño sensatos para el despliegue de nuevas soluciones de seguridad

El Security Design Development puede ayudar a su organización a desarrollar una estrategia, plan y diseño para integrar nuevas soluciones de seguridad en su infraestructura central de red. Con este servicio, los expertos de Cisco pueden ayudar a su organización a desarrollar un diseño de seguridad de red hecho a la medida que brinde una defensa de múltiples capas contra amenazas de seguridad, que acorte los tiempos de implementación y que suavice la migración asociada con el despliegue de nuevas soluciones de seguridad.

Su organización puede evitar errores o retrasos potencialmente costosos al aprovechar la pericia de Cisco en un amplio conjunto de tecnologías de seguridad de red incluyendo control de admisión a la red, dispositivos de mitigación de amenazas, detección de intrusiones, firewalls, acceso remoto y VPNs (Ver Tabla 2). Al ayudar a prevenir costosos rediseños para soportar a una nueva solución, el servicio reduce el costo total de propiedad de su red y permite a su organización prepararse mejor para las futuras iniciativas de integración y despliegue.

Con este servicio, los consultores y arquitectos de Cisco conducen una revisión de los objetivos de seguridad de su organización y brindan un profundo análisis de los requerimientos técnicos, de procedimiento y recursos para un despliegue de seguridad hecho a la medida. Después de de entender las metas y requerimientos de seguridad de su empresa, los expertos en seguridad de Cisco ayudan a desarrollar un diseño para la solución de seguridad incluyendo diagramas detallados de la red y configuraciones muestra que permitan la integración en su ambiente de red.

Tabla 2. Actividades, metodologías y entregable del Security Design Development de Cisco

Actividades	Metodología y entregable
• Analizar las metas, objetivos y requerimientos de la seguridad de su red • Desarrollar una estrategia, plan y diseño para obtener un enfoque que abarque toda la corporación y que esté dirigido hacia la seguridad de red • Evaluar la arquitectura de red existente para identificar vulnerabilidades de arquitectura, diseño e implementación • Analizar el impacto de integrar la nueva solución con la infraestructura existente de TI, las operaciones de software y los procedimientos de administración de seguridad • Evaluar que tan lista está la red para el despliegue de la solución, incluyendo la infraestructura actual de TI, los dispositivos de seguridad, las operaciones de software y los procedimientos de administración de seguridad • Definir los requerimientos arquitectónicos, topológicos y funcionales para la solución • Desarrollar un diseño detallado incluyendo configuraciones muestra para componentes de seguridad de red, incluyendo: – Dispositivos de control de admisión a la red – Dispositivos de mitigación de amenazas – Dispositivos de perímetro – Dispositivos de acceso remoto – Sistemas de detección de intrusiones – Protección de borde – Firewalls – Routers y switches – Conexiones de Extranet – Sistemas de administración de seguridad • Especificar los requerimientos de hardware y software incluyendo herramientas de administración de seguridad de red • Optimizar el diseño de la solución considerando escalabilidad, redundancia y desempeño • Proveer recomendaciones para la administración y el mantenimiento continuo de la solución de seguridad	**Metodología** • Conducir un taller de diseño para recabar información e iniciar el desarrollo del diseño de seguridad • Analizar la infraestructura existente de seguridad de red contra la estrategia y requerimientos organizacionales • Desarrollar la estrategia y la especificación de diseño de la seguridad de red que cumplan con los requerimientos específicos de TI y seguridad **Entregable** • Una Especificación de Diseño de Seguridad que delinee la estrategia y plan general para la nueva solución y que defina la topología, componentes y funciones del diseño de seguridad incluyendo diagramas de red y configuraciones muestra

BENEFICIOS

Con los servicios de Security Design de Cisco, su organización puede:

- Desarrollar un diseño de seguridad de red hecho a la medida que brinde una defensa de múltiples capas contra amenazas a la seguridad
- Mitigar amenazas de seguridad de red al identificar tanto vulnerabilidades de seguridad como desviaciones a la política de seguridad corporativa y las mejores prácticas de la industria
- Mejorar la confiabilidad, facilidad de mantenimiento y desempeño de su diseño de seguridad de red
- Acortar los tiempos de implementación y migración de nuevas soluciones y tecnologías de seguridad
- Mejorar la productividad del personal de seguridad de red al reducir el tiempo invertido en un costoso y tardado rediseño de la red
- Mitigar costosos retrasos y problemas durante el diseño, implementación y despliegue de nuevas soluciones de seguridad

POR QUÉ CISCO

Una seguridad efectiva de red empieza con un diseño de red sensato, un diseño que incorpore los objetivos y estrategia centrales de su negocio, así como los requerimientos técnicos de la seguridad. Como parte del enfoque Lifecycle Services de Cisco, los servicios de Security Design permiten a su organización proteger mejor los activos del negocio y sus servicios, desplegar nuevas soluciones de red de manera más costo-eficiente y evitar costos retrasos e interrupciones durante la integración.

DISPONIBILIDAD Y PARA ORDENAR

Los servicios Security Design de Cisco están disponibles en todo el mundo a través de Cisco y sus partners. La información puede variar por región.

PARA OBTENER MÁS INFORMACIÓN

Para obtener más información acerca de los servicios Security Design de Cisco o el enfoque Lifecycle Services de Cisco, favor de contactar a su representante Cisco.

Oficinas Centrales Corporativas
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Oficinas Centrales en Europa
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Oficinas Centrales en las Américas
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Oficinas Centrales en Asia Pacífico
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 317 7799

Cisco Systems tiene más de 200 oficinas en los siguientes países y regiones. Las direcciones, números telefónicos y de fax están listados en el sitio de Cisco en 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

Impreso en los EEUU C78-336450-00 02/06