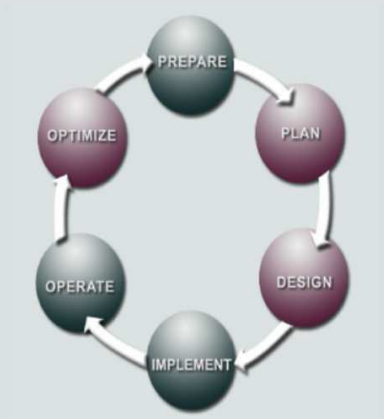
Security Unified Communications Services de Cisco

Servicios de planeación y diseño para ayudar a asegurar la integridad, privacidad y disponibilidad de Unified Communications de Cisco

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

Muchas organizaciones han descubierto que las Comunicaciones IP – la convergencia de datos, voz y vídeo en una sola red – pueden mejorar la productividad y movilidad de los empleados, al tiempo que reducen dramáticamente los costos de comunicación. Pero la clave para alcanzar estas ventajas es la certeza de que las comunicaciones IP son seguras y están protegidas contra interrupciones.

Numerosas amenazas, desde fallas en dispositivos hasta ataques maliciosos, pueden afectar la integridad, privacidad y disponibilidad de Comunicaciones IP. Para incrementar la protección, Cisco Systems® recomienda un enfoque en el que múltiples capas de seguridad estén integradas a través de aplicaciones y sistemas de Unified Communications de Cisco.

Como parte de las fases de planeación, diseño y optimización del enfoque Lifecycle Services de Cisco®, Cisco Systems ofrece servicios de Security Unified Communications diseñados para grandes empresas. A través de éstos, los consultores de Cisco emplean una metodología consistente y comprobada en el análisis de sistemas Unified Communications de Cisco y ofrecen recomendaciones para una protección exhaustiva a nivel sistema.

A través de los servicios Security Unified Communications de Cisco, ingenieros de Cisco expertos en unified communicaciones y seguridad evalúan la política de seguridad en comunicaciones de su organización, la seguridad de su sistema Unified Communications de Cisco y la seguridad subyacente integrada en su red. Los consultores identifican vulnerabilidades y desviaciones de su política de seguridad corporativa y las mejores prácticas de la industria y le proporcionan recomendaciones detalladas para fortalecer la seguridad de Unified Communications de Cisco y evitar demoras en la implementación y poca calidad de servicio.

Los servicios Security Unified Communications de Cisco incluyen los siguientes componentes de servicio:

- Unified Communications Security Policy and Procedure Review de Cisco
- Unified Communications System Security Design Review de Cisco
- Unified Communications Network Security Design Review de Cisco
- Unified Communications Vulnerability Test de Cisco

BENEFICIOS

Con los servicios Security Unified Communications de Cisco, su organización puede:

- **Mitigar amenazas de seguridad de Unified Communications de Cisco** – Identificar

vulnerabilidades y desviaciones de seguridad de su política corporativa de seguridad y mejores prácticas de industria

- **Mejorar la integridad, privacidad y disponibilidad de Unified Communications de Cisco** – Recomendar mejoras a su infraestructura y sistemas de comunicación para habilitar seguridad integrada y de múltiples capas
- **Incrementar la productividad de su administración de red y personal de Tecnología** – Habilitar a su organización para imponer políticas y procedimientos de seguridad de Unified Communications de Cisco consistentes y eficientes
- **Reducir el costo total de propiedad (TCO, por sus siglas en inglés) de Unified Communications de Cisco** – Mejorar los procedimientos operativos de su sistema de comunicaciones IP a través del despliegue consistente de controles de seguridad, tales como procedimientos de revisión de mejoras, configuraciones de sistemas y endurecimiento de servidores
- **Reduzca el TCO de su red** – Extienda las capacidades de seguridad existentes para la red de datos a los servicios de comunicación y permita que su organización esté mejor preparada para futuras iniciativas de despliegue de Unified Communications de Cisco

UNIFIED COMMUNICATIONS SECURITY POLICY AND PROCEDURE REVIEW DE CISCO

Analizar las políticas y procedimientos operativos ayuda a mejorar la seguridad de Unified Communications de Cisco

A través del Unified Communications Security Policy and Procedure Review de Cisco, los consultores de Cisco realizan una revisión a profundidad de las políticas de seguridad y procedimientos operativos de Unified Communications de Cisco de su organización. (Ver Tabla 1.)

Tabla 1. Actividades, metodología y entregable del Unified Communications Security Policy and Procedure Review de Cisco

Actividades	Metodología y entregable
• Revisar la documentación de políticas de seguridad para Unified Communications de Cisco, tales como controles de acceso, chequeo de virus, reportes y recuperación de incidentes, monitoreo de seguridad e integridad de datos • Analizar los procedimientos operativos de Unified Communications de Cisco para protección de virus, administración de incidentes, respaldar/restaurar la red, monitoreo de seguridad y procedimientos de revisión de aplicaciones • Revisar Unified Communications de Cisco y los procedimientos de control de acceso de red, incluyendo administración de privilegios, autentificación de usuario, protección de contraseñas y acceso remoto • Analizar procedimientos organizacionales para administrar seguridad de red, incluyendo roles y responsabilidades, toma de decisiones multifuncionales y administración de cambios	**Metodología** • Realizar un encuentro antes de la evaluación para recabar información e iniciar la revisión • Recabar información en sitio • Programar pruebas de vulnerabilidad en sitio • Proporcionar una presentación en sitio del análisis y los hallazgos preliminares de brechas de seguridad de Unified Communications de Cisco • Presentar el análisis y hallazgos finales de brechas de seguridad de Unified Communications de Cisco **Entregable** El Reporte de Políticas y Procedimientos de Seguridad de Unified Communications de Cisco. Este entregable incluye típicamente: • Un resumen ejecutivo de los principales hallazgos • Recomendaciones detalladas para fortalecer la tecnología, política y procedimiento de seguridad de Unified Communications de Cisco

CISCO UNIFIED COMMUNICATIONS SYSTEM SECURITY DESIGN REVIEW

Ayudando a asegurar que los servicios de Unified Communications de Cisco estén basados en un sólido diseño de seguridad del sistema

A través del Unified Communications System Security Design Review de Cisco, ingenieros de seguridad de voz de Cisco revisan y analizan sistemas críticos de Unified Communications de Cisco, tales como CallManager de Cisco, teléfonos IP de Cisco y software Unity® de Cisco. El equipo de Cisco identifica vulnerabilidades y le brinda recomendaciones para mejorar la protección contra acceso no autorizado, *spoofing* de identidad (envío de correo alegando que es de una fuente confiable), *toll fraud* (capacidad de tomar ventaja de las vulnerabilidades de VoIP para robarle capacidad a la red) y amenazas a las capas de aplicaciones. (Ver Tabla 2.)

Tabla 2. Actividades, metodología y entregable de Unified Communications System Security Design de Cisco

Actividades	Metodología y Entregable
• Proporcionar descubrimiento de anfitrión y sistema operativo de sistemas Unified Communications de Cisco e identificar y verificar servicios de red desplegados • Verificar que la seguridad esté funcionando para todas las funciones de voz desplegadas • Revisar la seguridad del servidor de aplicaciones de Unified Communications de Cisco para ayudar a asegurar que las mejores prácticas de servidores y configuración estén implementadas • Verificar que el software antivirus recomendado esté instalado y desempeñar una revisión de configuración de antivirus • Verificar que la detección de intrusión de anfitrión esté afinada y configurada correctamente en los servidores de telefonía IP, CallManager de Cisco y el sistema Unity de Cisco • Proporcionar recomendaciones para endurecimiento del sistema operativo y teléfonos, autentificación de usuario, detección de intrusiones y acceso remoto, conforme sea necesario	**Metodología** • Realizar una reunión antes de la evaluación para recabar información e iniciar la revisión • Recabar información en sitio • Programar pruebas de vulnerabilidad en sitio • Proporcionar una presentación en sitio del análisis y los hallazgos preliminares de brechas de seguridad de Unified Communications de Cisco • Presentar el análisis y hallazgos finales de brechas de seguridad de Unified Communications de Cisco **Entregable** La Especificación de Diseño de Seguridad de Unified Communications de Cisco, el cual proporciona recomendaciones detalladas para mejorar la seguridad del sistema para aplicaciones de Unified Communications de Cisco

CISCO UNIFIED COMMUNICATIONS NETWORK SECURITY DESIGN REVIEW

Ayudando a asegurar que la infraestructura de seguridad de red proteja a los sistemas y aplicaciones de Unified Communications de Cisco

A través del curso de este servicio, los ingenieros de red de Cisco llevan a cabo una revisión del diseño de seguridad de la red para identificar las vulnerabilidades y desviaciones de su política corporativa y de las mejores prácticas de la industria que pueden comprometer la seguridad de Unified Communications de Cisco (Ver Tabla 3.)

Tabla 3. Actividades, metodología y entregable de la Unified Communications Network Security Design Review de Cisco

Actividades	Metodología y entregable
• Llevar a cabo una revisión del diseño de seguridad de su infraestructura de red que soporta sistemas y aplicaciones de Unified Communications de Cisco • Analizar la arquitectura de seguridad de la red Unified Communications de Cisco para identificar vulnerabilidades del diseño • Revisar la configuración de capas de acceso de voz para chequear que todas las funciones y mejores prácticas de seguridad estén implementadas • Llevar a cabo un análisis detallado de seguridad de los dispositivos de infraestructura y componentes de red de Unified Communications de Cisco, incluyendo: – Gateways de voz – Dispositivos de acceso remoto – Sistemas de detección de intrusiones – Seguridad al borde – Firewalls – Routers y switches – Sistemas de administración de seguridad • Proporcionar recomendaciones de diseño para topología de red, colocación de dispositivos y mejoras de conectividad, incluyendo documentación de recomendaciones de protocolo, política y funciones • Desarrollar configuraciones muestra para firewalls, sistemas de detección de intrusiones, puntos de control de admisión a la red, protección al borde, routers, switches, gateways de voz, VPNs y servers de control de acceso	**Metodología** • Realizar una reunión antes de la evaluación para recabar información e iniciar la revisión • Recabar información en sitio • Programar pruebas de vulnerabilidad en sitio • Proporcionar una presentación en sitio del análisis y los hallazgos preliminares de brechas de seguridad de Unified Communications de Cisco • Presentar el análisis y hallazgos finales de brechas de seguridad del Unified Communications de Cisco **Entregable** La Especificación de Diseño de Seguridad de Red Unified Communications de Cisco, la cual detalla mejoras recomendadas para el diseño general de seguridad, la configuración de funciones y la integración de dispositivos para sistemas y aplicaciones Unified Communications de Cisco

CISCO UNIFIED COMMUNICATIONS VULNERABILITY TEST

Identificar debilidades de seguridad en la infraestructura Unified Communications de Cisco

Utilizando herramientas de evaluación avanzadas y especializadas, los ingenieros de seguridad de Cisco buscan y explotan vulnerabilidades dentro de la infraestructura Unified Communications de Cisco para identificar exposiciones de seguridad (Ver Tabla 4). Esta prueba de vulnerabilidad permite a su organización evaluar su habilidad para detectar y responder a amenazas a los sistemas Unified Communications de Cisco y a validar políticas y procedimientos de seguridad de voz.

Tabla 4. Actividades, metodología y entregable del Unified Communications Vulnerability Test de Cisco

Actividades	Metodología y entregable
• Llevar a cabo un escaneo automatizado de los sistemas Unified Communications de Cisco para descubrir y probar servicios • Simular un ataque controlado a la red para determinar potenciales vulnerabilidades del sistema, aplicación y dispositivos de red • Realizar técnicas manuales para explotar y confirmar vulnerabilidades identificadas • Realizar ardides secundarios, incluyendo explotación de relaciones de confianza entre anfitriones y vulnerabilidades de contraseñas • Llevar a cabo revisiones de configuraciones de dispositivos Unified Communications de Cisco para identificar riesgos de seguridad • Revisar prácticas de administración de dispositivos incluyendo verificación de contraseñas de dispositivos de infraestructura Unified Communications de Cisco • Analizar y presentar resultados de pruebas y proporcionar recomendaciones sobre mejoras a la arquitectura, política y configuración para ayudar a prevenir futuras explotaciones	**Metodología** • Realizar una reunión antes de la evaluación para recabar información e iniciar la revisión • Recabar información en sitio • Programar pruebas de vulnerabilidad en sitio • Proporcionar una presentación en sitio del análisis y los hallazgos preliminares de brechas de seguridad de Unified Communications de Cisco • Presentar el análisis y hallazgos finales de brechas de seguridad del Unified Communications de Cisco **Entregable** El Reporte de Vulnerabilidades de Unified Communications de Cisco, el cual identifica vulnerabilidades y proporciona un plan de soluciones recomendadas

POR QUÉ CISCO

Unified Communications de Cisco pueden abrir un mundo de movilidad, productividad y beneficios de costos para su organización – pero sólo si sus sistemas y aplicaciones Unified Communications de Cisco son privadas y seguras. Los servicios Security Unified Communications de Cisco proporcionan recomendaciones detalladas de planeación, evaluación y diseño que su empresa necesita para mantener la integridad, privacidad y disponibilidad de Unified Communications de Cisco.

DISPONIBILIDAD Y PARA ORDENAR

Los servicios Security Unified Communications de Cisco están disponibles a través de Cisco y los partners de Cisco alrededor del mundo. La información varía por región.

PARA OBTENER MÁS INFORMACIÓN

Para obtener más información acerca de los servicios Security Unified Communications de Cisco o el enfoque Lifecycle Services de Cisco, contacte 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.

C78-33499-00 02/06