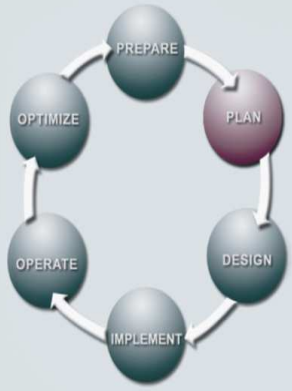
# Security Posture Assessment Services de Cisco

**Identificar, analizar y validar vulnerabilidades de seguridad de red que pueden amenazar a su empresa**

## 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

Para proteger sus aplicaciones y datos empresariales críticos de intrusiones de seguridad, su organización requiere una amplia y profunda seguridad de red. Sin embargo, desarrollar robustas defensas de seguridad requiere una clara comprensión del estado actual de vulnerabilidad de la red, aplicaciones y sistemas. Como parte de la fase de planeación del enfoque Lifecycle Services de Cisco®, los Security Posture Assessment Services de Cisco, diseñados para grandes empresas, brindan una evaluación detallada de vulnerabilidades de los dispositivos de red, servidores, computadoras de escritorio, aplicaciones Web y bases de datos en su red.

Los servicios Security Posture Assessment de Cisco consisten de tres servicios:

- **External Security Posture Assessment Service de Cisco –** Identifica vulnerabilidades que permiten a redes externas y no confiables obtener acceso a redes y sistemas internos y confiables y recomienda soluciones para realizar mejoras.
- **Internal Security Posture Assessment Service de Cisco** – Identifica los pasos que usted debe tomar para frustrar ataques intencionales o errores involuntarios de usuarios y sistemas internos y confiables.
- **Wireless Security Posture Assessment Service de Cisco** – Identifica los riesgos y puntos de exposición de su infraestructura inalámbrica y recomienda soluciones para resolverlos.

Juntos, estos servicios brindan protección proactiva a su infraestructura tecnológica al identificar vulnerabilidades en la red, las aplicaciones Web y el perímetro de Internet, y priorizar acciones correctivas para proteger la confiabilidad, integridad y disponibilidad de los activos e información de su organización.

Dado que las tecnologías, procesos de negocios y amenazas de red siempre están cambiando, la postura de seguridad de su organización nunca permanece estática. Muchas organizaciones realizan valoraciones de posturas de seguridad para evaluar el estado evolutivo de la seguridad de red de su empresa. Las valoraciones continuas pueden ayudarle a mantener una visión actualizada de su actual postura de seguridad de red.

Con los servicios Security Posture Assessment de Cisco, su organización puede:

- Reducir el riesgo de acceso intencional o accidental a sus activos e información tecnológica
- Identificar vulnerabilidades de seguridad en su infraestructura de red
- Desarrollar una lista priorizada de pasos requeridos para arreglar vulnerabilidades identificadas
- Mejorar el cumplimiento de regulaciones federales y estatales que requieren valoraciones de seguridad

- Reducir el tiempo y los recursos utilizados para tratar de mantenerse al tanto de nuevas y emergentes vulnerabilidades
- Validar las políticas y prácticas actuales de seguridad contra las mejores prácticas de la industria y verificar áreas que requieren presupuesto o personal de seguridad
- Recibir una valoración de seguridad independiente y realizada por terceros para fortalecer las políticas de seguridad y esfuerzos de cumplimiento de normas de su organización

## EXTERNAL SECURITY POSTURE ASSESSMENT SERVICE DE CISCO

**Identificando vulnerabilidades en redes y servicios conectados a Internet**

El External Security Posture Assessment de Cisco identifica el riesgo de seguridad asociado con los sistemas y servicios conectados a Internet que posee su organización al identificar vulnerabilidades que pudieran permitir a redes externas y no confiables obtener acceso a redes, aplicaciones y sistemas internos y confiables.

Los expertos de Cisco Systems® empiezan por conducir un escaneo remoto de vulnerabilidades de la presencia en Internet de su organización utilizando herramientas especializadas y automatizadas con capacidades que van más allá de las herramientas comerciales estándar. Después de confirmar el registro de los dispositivos de Internet, los expertos Cisco realizan un escaneo para buscar servicios visibles externamente. Dado que la mayoría de los servicios tienen vulnerabilidades inherentes y bien conocidas, los ingenieros de Cisco determinan si dichos servicios son un riesgo al confirmar manualmente vulnerabilidades que pueden conducir a brechas de seguridad. El servicio simula actividades típicas de atacantes maliciosos de una manera segura y controlada en un intento por comprometer los dispositivos de perímetro y los controles de seguridad de Internet, proveyendo el análisis profundo que se necesita para identificar y validar vulnerabilidades (Ver Tabla 1).

**Tabla 1.** Actividades, metodología y entregables del External Security Posture Assessment de Cisco

| Actividades | Metodología y entregables |
|---|---|
| • Identificar y confirmar la presencia de sistemas y servicios visibles en Internet al:<br>– Identificar el número de sistemas y dispositivos activos, incluyendo anfitriones detrás de dispositivos de filtraje tales como firewalls<br>– Escanear puertos de Protocolo de Control de Transmisiones (TCP, por sus siglas en inglés) y de Protocolo de Datagramas de Usuario (UDP, por sus siglas en inglés) para determinar si algún servicio es visible externamente<br>– Investigar y confirmar potenciales sistemas, servicios, dispositivo y aplicaciones objetivo<br>• Emular las actividades típicas de hackers a través de medios no destructivos, para confirmar la presencia de vulnerabilidades y el nivel de acceso no autorizado<br>• Proveer un análisis detallado de los ataques simulados para identificar vulnerabilidades críticas y comparar los resultados de la valoración con las mejores prácticas y políticas recomendadas por la industria, así como los requerimientos operativos de la organización<br>• Priorizar los riesgos descubiertos y proveer acciones recomendadas para mejorar el estado de seguridad de su red y cumplir con los objetivos de seguridad organizacionales | **Metodología**<br>• Recabar y revisar documentación de su red<br>• Identificar sistemas y servicios objetivo visibles desde Internet<br>• Conducir pruebas automatizadas de vulnerabilidad en los objetivos<br>• Analizar datos de vulnerabilidad y validar la presencia de vulnerabilidades<br>• Proveer análisis y recomendaciones de vulnerabilidades<br>• Proveer una presentación ejecutiva en sus instalaciones sobre los hallazgos y recomendaciones<br>**Entregables**<br>El Reporte de Valoración Externa de la Postura de Seguridad (External Security Posture Assessment Report). Este entregable típicamente:<br>• Prioriza las vulnerabilidades descubiertas e identifica los hallazgos más críticos<br>• Provee análisis y estadísticas de vulnerabilidades para sistemas y servicios individuales<br>• Ofrece acciones recomendadas para mejorar el estado de seguridad de la red para cumplir con sus objetivos de seguridad |

## Beneficios

Con el External Security Posture Assessment de Cisco, su organización puede:

- Identificar proactivamente vulnerabilidades de seguridad en Internet que presentan un riesgo a sus redes, sistemas e información
- Ejecutar recomendaciones priorizadas para proteger dispositivos, sistemas y aplicaciones de acceso no autorizado
- Simular efectivamente a un atacante externo para confirmar los riesgos presentados por hackers o usuarios maliciosos de Internet
- Probar salvaguardas actuales de seguridad en Internet para ayudar a asegurar que la actividad maliciosa no logre penetrar o interrumpir el servicio
- Mejorar el estado general de seguridad de su red al proveer acciones recomendadas para mitigar las vulnerabilidades identificadas

## INTERNAL SECURITY POSTURE ASSESSMENT SERVICE DE CISCO

**Revelando las debilidades de seguridad en redes, aplicaciones y procesos internos**

Aun cuando es cada vez más frecuente que ocurran incidentes externos de seguridad de la red, su organización no puede darse el lujo de pasar por alto la amenaza que surge de fuentes internas y confiables. Ya sea que un evento sea causado por conducta maliciosa intencional o un simple error, las amenazas internas pueden ser aun más perjudiciales y más caras que una brecha externa de seguridad.

El Internal Security Posture Assessment de Cisco es una simulación controlada de ataques para estimar la exposición de sistemas, aplicaciones y dispositivos de red dentro de la red interna y confiable. Durante la realización de la valoración, los ingenieros de Cisco toman un profunda postura para obtener acceso no autorizado a sus recursos internos (ver Tabla 2). Este enfoque incluye tanto identificación automatizada de vulnerabilidades como explotación secundaria a través de la simulación de un ataque de un intruso real de una manera segura y controlada para confirmar manualmente vulnerabilidades. Esta explotación secundaria puede incluir el tomar como blanco relaciones de confianza entre anfitriones, revelando debilidades de las contraseñas y obteniendo acceso administrativo a sus sistemas, proveyendo un enfoque estructurado para identificar vulnerabilidades que de otra manera hubieran pasado inadvertidas.

Los expertos de Cisco entonces pueden proveer un reporte que describa las fortalezas y debilidades encontradas en los escenarios de prueba, con recomendaciones para mejoras. Al identificar los pasos requeridos para frustrar ataques intencionales o errores involuntarios de personas internas confiables, el Internal Security Posture Assessment de Cisco le ayuda a asegurar mejor sus valiosos activos de información.

**Tabla 2.** Actividades, metodología y entregables del Internal Security Posture Assessment de Cisco

| Actividades | Metodología y entregables |
|---|---|
| Identificar la presencia de vulnerabilidades en la red interna al:<br>• Realizar un barrido de paquetes buscadores en la red para identificar dispositivos, sistemas operativos y aplicaciones<br>• Escanear puertos TCP y UDP críticos y bien conocidos en anfitriones identificados<br>• Confirmar la existencia de vulnerabilidades identificadas<br>Utilizar artificios en las vulnerabilidades del sistema, aplicaciones y dispositivos de red al simular un ataque controlado a la red y:<br>• Desempeñar una serie de artificios secundarios en relaciones de confianza entre anfitriones<br>• Explotar problemas causados por usuarios tales como la utilización de la misma contraseña en Windows, Novell y UNIX<br>• Explotar la información recopilada de sistemas, aplicaciones y dispositivos penetrados<br>• Intentar penetrar archivos de contraseñas y obtener acceso como administrador (Windows), raíz (UNIX) o supervisor (Novell) | **Metodología**<br>• Recabar y revisar su documentación de red<br>• Identificar y confirmar todas las vulnerabilidades<br>• Conducir pruebas primarias y secundarias de vulnerabilidad<br>• Analizar datos de vulnerabilidad y validar la presencia de vulnerabilidades<br>• Proveer análisis y recomendaciones de vulnerabilidad<br>• Proveer una presentación ejecutiva en sus oficinas de los hallazgos y recomendaciones<br>**Entregables**<br>El reporte Interno de la Valoración de la Postura de Seguridad (The Internal Security Posture Assessment Report). Típicamente, este reporte:<br>• Prioriza las vulnerabilidades descubiertas e identifica los hallazgos más críticos<br>• Provee análisis y estadísticas de vulnerabilidad para sistemas y servicios individuales |

| | |
|---|---|
| Analizar los datos de la prueba para identificar vulnerabilidades críticas y comparar los resultados de la valoración con las prácticas de seguridad recomendadas en sus políticas organizacionales de seguridad | • Provee acciones recomendadas para mejorar el estado de seguridad de la red para cumplir los objetivos de seguridad de su organización |

### Beneficios

Con el Internal Security Posture Assessment de Cisco, su organización puede:

- Adquirir una valoración costo-efectiva e imparcial de sus riesgos internos de seguridad de información
- Identificar amenazas críticas a la seguridad que representan un riesgo para sus dispositivos, sistemas y aplicaciones dentro de su "confiable" red corporativa
- Simular efectivamente a un atacante interno para cuantificar los riesgos presentados por un empleado o contratista disgustado
- Validar políticas y prácticas internas de seguridad contra las mejores prácticas de la industria
- Mejorar el estado general de seguridad de su red al realizar las acciones recomendadas para mitigar las vulnerabilidades

## WIRELESS SECURITY POSTURE ASSESSMENT SERVICE DE CISCO

**Cuantificando riesgos de seguridad y vulnerabilidades en redes inalámbricas**

La tecnología y los servicios inalámbricos deben integrarse completamente al marco de trabajo de seguridad de su organización y brindar el mismo nivel de privacidad y protección que una infraestructura cableada. El Wireless Security Posture Assessment de Cisco evalúa su arquitectura y configuraciones inalámbricas para identificar puntos de exposición, localizar puntos de acceso no autorizados y recomendar soluciones para fortalecer el estado de seguridad de su infraestructura inalámbrica.

Los expertos Cisco empiezan por inspeccionar sus instalaciones para descubrir y crear un mapa de todos los puntos de acceso disponibles (Ver Tabla 3). Al comparar los puntos de acceso encontrados, así como la información recopilada durante la visita a la localidad contra la lista de dispositivos autorizados, los ingenieros de Cisco pueden identificar posibles dispositivos "delincuentes". Los ingenieros de Cisco entonces comparan su arquitectura y configuración de red inalámbrica con las mejores prácticas de la industria, documentando vulnerabilidades y amenazas conocidas.

Moviéndose fuera de las instalaciones de su organización, la valoración también utiliza sofisticadas antenas inalámbricas para buscar tráfico de LANs inalámbricas (WLANs) que se esté filtrando desde los edificios. De ser necesario, los ingenieros Cisco se mueven hacia áreas controladas del edificio para continuar buscando tráfico WLAN. Después de descubrir dicho tráfico, los ingenieros determinan el método de encripción y autentificación utilizado e intentan obtener acceso al segmento de la LAN.

**Tabla 3.** Actividades, metodología y entregables del Wireless Security Posture Assessment de Cisco

| Actividades | Metodología y entregables |
|---|---|
| Identificar, validar y confirmar la presencia de vulnerabilidades en la red WLAN. Típicamente, las actividades incluyen:<br>• Examinar las configuraciones de puntos de acceso inalámbrico y compararlas contra las prácticas de seguridad recomendadas<br>• Localizar tráfico WLAN que se esté filtrando desde las instalaciones del cliente al desplegar sofisticadas antenas inalámbricas<br>• Hacer un mapa de la cobertura de señal con tecnología de Sistema Global de Posicionamiento (GPS, por sus siglas en | **Metodología**<br>• Recabar y revisar la documentación de red del cliente<br>• Identificar y confirmar todas las vulnerabilidades<br>• Conducir pruebas primarias y secundarias de vulnerabilidad<br>• Analizar los datos de vulnerabilidad y validar la presencia de vulnerabilidades<br>• Proveer análisis y recomendaciones de vulnerabilidades<br>• Proveer una presentación ejecutiva en sus instalaciones sobre los hallazgos y recomendaciones |

| | |
|---|---|
| inglés) para trazar las áreas donde se detectó el tráfico WLAN<br>• Si no se detecta tráfico WLAN fuera del edificio y, de ser necesario, revisar la visibilidad y fortaleza de la señal en áreas públicas dentro de edificios y en áreas controladas de los mismos<br>• Determinar si la encripción Privacidad Equivalente al Cable (WEP, por sus siglas en inglés) está habilitada o si el tráfico inalámbrico se está transmitiendo sin encripción<br>Confirmar vulnerabilidades en debilidades de seguridad identificadas para determinar más efectivamente el nivel de acceso no autorizado. Típicamente, las actividades incluyen:<br>• Intentos de descifrar el WEP<br>• Intentos de obtener direcciones IP de clientes y evaluar la seguridad de los puntos de acceso<br>Analizar los datos de pruebas para identificar las vulnerabilidades críticas y comparar los resultados de la valoración inalámbrica con las prácticas de seguridad recomendadas y las políticas organizaciones de seguridad | **Entregables**<br>El Reporte de Valoración de la Postura de Seguridad Inalámbrica (The Wireless Security Posture Assessment Report). Este entregable típicamente:<br>• Prioriza las vulnerabilidades descubiertas e identifica los hallazgos más críticos<br>• Provee análisis y estadísticas de vulnerabilidad para sistemas y servicios individuales<br>• Provee acciones recomendadas para mejorar el estado de seguridad de la red para cumplir con los objetivos de seguridad de su organización |

## Beneficios

Con el Wireless Security Posture Assessment de Cisco, su organización puede:

- Identificar riesgos críticos de la seguridad inalámbrica tales como filtración de información, puntos de acceso no autorización y configuración incorrecta de dispositivos WLAN
- Simular efectivamente a un atacante inalámbrico para cuantificar los riesgos presentados por un escáner malicioso que pase fuera de las instalaciones
- Proteger información de la empresa al identificar el potencial de acceso no autorizado e identificar soluciones para reducir las vulnerabilidades
- Priorizar recomendaciones específicas para fortalecer las configuraciones de seguridad de los dispositivos WLAN
- Validar políticas y prácticas de seguridad interna contra las mejores prácticas de la industria para su infraestructura de red inalámbrica
- Fortalecer el estado general de seguridad de su red inalámbrica a través del desarrollo de un plan para priorizar las mejoras recomendadas

Con el Wireless Security Posture Assessment, la gerencia y los administradores de la red están demostrando su compromiso de lograr una mejora de la seguridad general de la infraestructura inalámbrica. Este compromiso continuo para mejorar el estado de la seguridad de la red inalámbrica incrementará la confianza en la seguridad de sus sistemas y datos.

## POR QUÉ CISCO

Los hackers, usuarios maliciosos de Internet y las amenazas internas a su red y activos de negocio nunca se detienen. De la misma manera, la postura de seguridad de su red, sistemas y aplicaciones no puede permanecer estáticas. Paras poder preservar los servicios críticos de negocios, salvaguardar la confianza y lealtad de sus clientes y reducir los costos de potenciales ataques a la red, usted debe evaluar continuamente el cambiante estado de la seguridad de su empresa a través de valoraciones continuas que lo mantengan al tanto de su actual postura de seguridad.

Como parte del enfoque de Lifecycle Services de Cisco, los servicios de Security Posture Assessment de Cisco brindan un importante primer paso al ayudarle a asegurar la protección ubicua de la red. Con una detallada evaluación del estado actual de la seguridad de red, su organización puede tener una visión clara de sus fortalezas y debilidades de seguridad y desarrollar un plan detallado para proteger más efectivamente su negocio.

## DISPONIBILIDAD Y PARA ORDENAR

Los servicios Security Posture Assessment de Cisco están disponibles a través de Cisco y sus partners a nivel mundial. La información varía por región.

## PARA OBTENER MÁS INFORMACIÓN

Para obtener más información acerca de los servicios Security Posture Assessment 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. C78-332592-00 02/06