

# Prácticas líder de Cisco: Operaciones de la Administración del Cisco IOS

## Contenido

[Abstracto](#)

[Introducción](#)

[Información general](#)

[Objetivos](#)

[Audiencia](#)

[prerrequisitos](#)

[Crear una estrategia de las operaciones de la Administración del Cisco IOS](#)

[Identificación de los productos a entregar](#)

[Identificación de las medidas del dispositivo fundamental](#)

[Definición de los papeles y de las responsabilidades](#)

[Identificando los campos de especialización requeridos](#)

[Identificación de los contribuidores dominantes](#)

[Identificación de las responsabilidades](#)

[Recursos de presupuesto](#)

[Después de un proceso de las operaciones de la Administración del Cisco IOS de la mejor práctica](#)

[‘Control de versión de software’](#)

[Administración de fallas’](#)

[Administración de problemas](#)

[Estandarización de la configuración](#)

[Administración de la disponibilidad](#)

[Lista de verificación de las operaciones de la Administración del Cisco IOS](#)

[Información Relacionada](#)

[Servicios de Cisco y soporte](#)

## **Abstracto**

Las prácticas líder de Cisco son un conjunto de los documentos codificados que proporcionan la dirección relevante y confiable en las operaciones de redes para los Productos Cisco y las soluciones. Las prácticas líder son desarrolladas y soportadas por los ingenieros premiados del TAC de Cisco y del Advanced Services que usted puede utilizar para ayudar a crear su propio conjunto de las prácticas líder de emular. Los clientes de Cisco han aplicado estas prácticas líder en su entorno de red de ganar el rendimiento de la red y la Disponibilidad.

Se recomienda altamente para complementar estas prácticas líder con los servicios de Cisco y sus Partners. Para más información sobre cómo optimizar su rendimiento de la red y Disponibilidad, entrar en contacto por favor su Representante representante de ventas de los

servicios sobre el sitio web del Advanced Services de Cisco y descubrir más sobre el soporte de la optimización de red - soporte de ingeniería enfocado, la disponibilidad de la red del soporte de la mejora (NAIS), la evaluación del proceso de administración del software (SMPA), y la implementación NAIS-SMPA.

## Introducción

### Información general

Los procesos operativos alrededor de la administración del software pueden ayudar a reducir la complejidad de la red, los problemas de soporte reactivo de la disminución y a mejorar el tiempo de solución de problemas. Este documento proporciona una estrategia, las recomendaciones de la herramienta, y las prácticas recomendadas para la Administración total del software del <sup>®</sup> del Cisco IOS (Cisco IOS).

[Crear una estrategia de las operaciones de la Administración del Cisco IOS](#) y [los siguientes las secciones de proceso de las operaciones de la mejor práctica de una Administración del Cisco IOS](#) en este documento discuten la metodología recomendada para la introducción y enumeran las mejores herramientas que se utilizarán para la fase de las operaciones. La fase de las operaciones incluye los procesos de la práctica recomendada para el siguiente:

Proceso	Descripción
Control de versión de software	El seguimiento, validar, y la mejora del estado coherente del software dentro del software identificado "sigue".
Administración de fallas	Dinámico monitoreando y actuando sobre la prioridad más alta SNMP y los mensajes de Syslog generados por el Cisco IOS.
Administración de problemas	De manera rápida y eficiente recogiendo la información del problema crítico para los asuntos relacionados del software para ayudar a prevenir los eventos futuros.
Estandarización de la configuración	"Estandarizando" las configuraciones para reducir el potencial para que código no comprobado sea ejercitado en la producción y para estandarizar el Network Protocol y el comportamiento de la característica.
Administración de la disponibilidad	Mejorando la Disponibilidad basada en la métrica, los objetivos de mejora, y los proyectos de la mejora

Este documento asume que usted ha implementado los procesos siguientes de la práctica recomendada para las hojas de operación (planning), el diseño y la implementación del Cisco IOS:

- Áreas de software manejables identificadas (agrupamientos de versiones de software) en su entorno basado en la plataforma, el módulo, la característica, el protocolo, y los requisitos de topología.
- Versiones de Cisco IOS seleccionadas, certificadas, y comunicadas por los agrupamientos de versiones de software.
- Implementó constantemente las versiones de Cisco IOS estándar en cada uno de los agrupamientos de versiones de software.

## Objetivos

Esta sección le ayuda a manejar y a mantener las versiones de Cisco IOS estandarizadas dentro de las pistas definidas. Usted aprenderá cómo:

- Desarrolle un proceso del control de versión de software para asegurar el estado coherente de la versión de software dentro de los agrupamientos de versiones de software identificados.
- El monitor, notifica, y resuelve los procesos basados en los mensajes de administración y las alertas (SNMP/syslog) de la falla del dispositivo para ayudar dinámico a resolver los problemas potenciales del software y del incidente.
- Colección eficiente de información del problema crítico para que software ayude a reducir el tiempo de solución de problemas por problemas relacionados con el software.
- Estandarice las configuraciones del dispositivo para ayudar a asegurar el protocolo, la característica, el acceso, y el estado coherente de la Seguridad para el entorno.

## Audiencia

Este documento es apropiado para los individuos y los administradores con una orientación técnica que son responsables de la operación diaria de la red. El documento describe cómo establecer los procesos operativos para ayudarle a reducir la complejidad de la red, los problemas de soporte reactivo de la disminución y a mejorar el tiempo de solución de problemas por la coherencia de la red constructiva y mejorando las capacidades para la administración de fallas proactiva.

## prerrequisitos

Ésos implicados en las operaciones de la Administración del Cisco IOS deben tener un conocimiento sólido del diseño de la infraestructura de red, y administración, determinado con el equipo de Cisco, y deben tener acceso a los detalles de la topología de red objetivo, de la configuración del dispositivo, del perfil de la actividad, del uso de la aplicación, y de la directiva de la utilización de recursos. El acceso, y la experiencia con, a las herramientas de la información disponibles en el [Cisco Connection Online](#) (CCO), también se requiere. Si usted [no se ha registrado](#) ya [con el CCO](#), sugerimos que usted haga tan para el acceso a las herramientas descritas en este documento.

## Crear una estrategia de las operaciones de la Administración del Cisco IOS

Muchas estrategias de calidad y herramientas existen para ayudar a manejar los entornos del Cisco IOS. Este capítulo se centra en tres estrategias dominantes para manejo de las

operaciones del Cisco IOS en entornos más de gran disponibilidad, e incluye una matriz de las herramientas operativas dominantes que son específicamente útiles para manejo de los problemas del Cisco IOS y del Cisco IOS.

La primera estrategia dominante es mantener el entorno tan simple como sea posible, evitando la variación la configuración y las versiones deL Cisco IOS tanto cuanto sea posible. La certificación del Cisco IOS se ha discutido ya, no obstante la coherencia de la configuración es otra área clave. El grupo arquitectura/ingeniería debe encargarse de la creación de los estándares de configuración. La implementación y el grupo de operaciones entonces tienen la responsabilidad de configurar los estándares y de mantener los estándares con el control de versión deL Cisco IOS y los estándares/control de la configuración del Cisco IOS.

La segunda estrategia dominante es la capacidad de identificar y de resolver rápidamente a las fallas de la red. El grupo de operaciones debe identificar generalmente los problemas de red antes de los usuarios los señala, y los problemas deben ser resueltos lo más rápidamente posible sin la afectación adicional o el cambio del entorno. Dos prácticas recomendadas dominantes en esta área son administración de problemas y administración de fallas (ambos se discuten más adelante en este documento).

**Note:** El Cisco IOS herramienta Stack Decoder se puede utilizar para ayudar rápidamente a diagnosticar las caídas del Cisco IOS Software.

La tercera estrategia dominante es “mejora constantemente”. El proceso primario es mejorar una Disponibilidad calidad-basada del programa de mejora. Realizando la análisis de la causa raíz en todos los problemas, incluyendo los problemas IOS-relacionados de Cisco, una organización puede mejorar la cobertura de la prueba, mejorar los tiempos de solución de problemas, y mejorar los procesos que eliminarán o reducirán el impacto de la caída del sistema. La organización también puede analizar los problemas comunes y crear procesos para resolverlos más rápidamente.

## Identificación de los productos a entregar

Los productos a entregar del proceso de la operación de la Administración del Cisco IOS Software incluyen:

- Procesos y herramientas del control de versión de software
- Supervisión y procesos de la administración de fallas
- Procesos de administración de problema
- Normas de configuración del dispositivo y procesos de la auditoría
- Disponibilidad de la red de la metodología, información y procesos del estudio

## Identificación de las medidas del dispositivo fundamental

La métrica se debe definir como parte del plan de operaciones y utilizar para determinar si las herramientas y los procesos están produciendo los resultados deseados. Los siguientes son algunos ejemplos de las métricas útiles de la Administración del Cisco IOS Software:

- Disponibilidad de la red (debido a los problemas de software)
- % de la conformidad de la versión deL Cisco IOS al estándar (en a por la base de la pista)
- % del estado coherente de la configuración del dispositivo (basado en los estándares)
- Métrica de la administración de problemas (MTTR, # boletos, # códigos del cierre)

## Definición de los papeles y de las responsabilidades

Identifique, califique, y ensamble un grupo multidisciplinar de administradores y/o de leads de la arquitectura de red, de la ingeniería de la red, y de los grupos de operaciones de la puesta en práctica para ayudar a asegurar las hojas de operación (planning), el diseño, la implementación, y las fases acertadas de las operaciones de sus proyectos de la actualización de IOS.

### Identificando los campos de especialización requeridos

Ensamble un grupo multidisciplinar de administradores y/o de leads de la Administración de redes, de la ingeniería de la red, de la implementación y de los grupos de operaciones para ayudar con la fase de las operaciones de su proyecto de la Administración del Cisco IOS.

### Identificación de los contribuidores dominantes

- Administrador de la red: Los administradores nombran, departamento, información de contacto Nombre del backup principal, departamento, información de contacto Nombre del backup secundario, departamento, información de contacto si procede
- Arquitecto de la red: Los arquitectos nombran, departamento, información de contacto Nombre del backup principal, departamento, información de contacto Nombre del backup secundario, departamento, información de contacto si procede
- Ingeniero de red: Los ingenieros nombran, departamento, información de contacto Nombre del backup principal, departamento, información de contacto Nombre del backup secundario, departamento, información de contacto si procede
- Ingenieros de las operaciones de la red (NOC): Los ingenieros nombran, departamento, información de contacto Nombre del backup principal, departamento, información de contacto Nombre del backup secundario, departamento, información de contacto si procede

### Identificación de las responsabilidades

- El administrador de la red es responsable de: Mantener el Plan del proyecto Asignación/reasignar los recursos Manejo del control de cambios Manejo del progreso Manejo de la información de presupuesto
- El arquitecto de la red es responsable de: Analizar los estándares de red y las advertencias de la versión Mantener la matriz de la actualización del software Mantener la matriz de la administración del candidato Mantener la matriz de los requisitos de memoria
- Los ingenieros de la red (NOC) son responsables de: Implementando y asegurando la conformidad a los estándares de red Identificación de los problemas del software y de las causas raíz Acción correctiva de recomendación Monitorear la red

### Recursos de presupuesto

Los requerimientos de recurso se deben determinar en la etapa de las operaciones para soportar la estrategia de administración del software para la organización. Esto incluirá los personales requeridos mide el tiempo y los gastos en inversión de capital necesarios para soportar la estrategia del software.

En muchos casos, un retorno en la inversión (ROI) o el plan presupuestario para las prácticas de

administración del software se puede generar sobre la base del costo de tiempo de inactividad y de los requerimientos de disponibilidad. Si la organización puede determinar el tiempo de inactividad debido a los problemas del software, después una mayoría de este coste puede ser compensada vía las prácticas recomendadas identificadas de la administración del software. Si el coste no puede ser compensado totalmente, después la organización debe considerar una más estrategia de administración del software básico que ayude a mejorar la productividad previniendo el retrabajo adicional como resultado de los problemas del software.

## [Después de un proceso de las operaciones de la Administración del Cisco IOS de la mejor práctica](#)

Las mejores prácticas para seguir un proceso de las operaciones de la Administración del Cisco IOS incluyen:

<b>Mejor práctica</b>	<b>Detalle</b>
<a href="#">‘Control de versión de software’</a>	Implementando solamente las versiones de software estandarizadas y monitoreando la red para validar o para cambiar posiblemente el software debido a la conformidad de la NON-versión.
<a href="#">Administración de fallas’</a>	El SNMP y la colección del mensaje de Syslog, la supervisión y el análisis son procesos de administración de fallas recomendados para resolver más problemas de red específicos del Cisco IOS que sean difíciles o imposibles identificar cualquier otra manera.
<a href="#">Administración de problemas</a>	Procesos de administración de problema detallados que definen la Identificación del problema, la recopilación de información, y un trayecto de solución bien-analizado. Estos datos se utilizan para determinar la causa raíz.
<a href="#">Estandarización de la configuración</a>	Las normas de configuración representan la práctica de crear y de mantener los dispositivos y los servicios similares “globales” estándar de los parámetros de la configuración a través dando por resultado la coherencia de configuración global a nivel empresarial.
<a href="#">Administración de la disponibilidad</a>	Mejora de la calidad usando la disponibilidad de la red como la mejora de la calidad métrica.

### [‘Control de versión de software’](#)

El control de versión de software es el proceso de implementación de sólo versiones de software estandarizadas y de supervisión de la red, con el fin de validar o, posiblemente, cambiar software

debido a que la versión no es la adecuada. El control de versión de software es generalmente realizado usando un proceso de certificación y un control de los estándares. Muchas organizaciones publican los estándares de versión en un servidor Web central. Además, entrenan a un personal de la implementación para revisar qué versión se está ejecutando y poner al día la versión si no es cumple con las normas. Algunas organizaciones tienen un proceso de la puerta de la calidad donde la validación secundaria se completa con las auditorías para asegurarse de que el estándar está seguido durante la implementación.

Durante la operación de la red, no es también infrecuente ver las versiones de software no estándar en la red, especialmente si la red es grande con un personal grande de las operaciones. Esto puede ser debido a uno del siguiente:

- Más nuevo personal inexperimentado
- Comandos boot mis configurados
- Implementaciones no verificadas

Se recomienda para validar periódicamente los estándares de versión de software usando las herramientas tales como Resource Manager Essentials CiscoWorks2000 (RME) que pueda clasificar todos los dispositivos por la versión deL Cisco IOS. Cuando se identifica una versión no estándar, debe ser señalada por medio de una bandera inmediatamente y un ticket de problemas o cambiar el boleto se inicie para traer la versión al estándar identificado.

## Herramientas disponibles

El Administrador de inventarios RME CiscoWorks2000 simplifica grandemente la Administración de la versión deL Cisco IOS de los routers Cisco y del Switches a través de las herramientas de informe basadas en web que los dispositivos del informe y de la clase basaron en la versión de software, la plataforma del dispositivo, y el Nombre del dispositivo.

## Administración de fallas'

La administración de fallas es el proceso de recoger, de monitorear y de analizar el SNMP y los mensajes de Syslog para resolver más problemas de red específicos del Cisco IOS que sean difíciles o imposibles identificar cualquier otra manera.

## Colección del SNMP trap

La colección y la notificación del SNMP trap es un proceso básico en administración de fallas usada para identificar los eventos de software o del soporte físico y/o causa un crash sin la Consulta SNMP por encima o el retardo contraído de los intervalos de sondeo. Los mensajes trampa se generan directamente del dispositivo de red a un sistema de administración de red que proporcione los Servicios de notificación. La colección y la notificación de estos desvíos es esenciales para la resolución rápida de muchos eventos de red incluyendo los eventos no de usuario-afectación tales como la pérdida de Dispositivos principales o de links en un entorno redundante.

Para recoger y monitorear estos desvíos, los desvíos se deben configurar correctamente en el dispositivo así como los sistemas de administración de red. Los sistemas de administración de red deben alertar al grupo de operaciones de la red cuando se ha recibido un desvío. La notificación puede entonces ocurrir bajo la forma de paginación, email o pantallas del evento en un entorno NOC.

Sin importar cómo se presentan los datos, éstos critican los casos, o las excepciones, se deben

analizar y revisar en una base normal (diario preferiblemente) por las operaciones de la red y/o el equipo de soporte de red. Las causas de todas las excepciones encontradas deben ser investigadas. Algunas excepciones registradas pueden no ser bastante críticas aumentar inmediatamente una alarma en el Network Operations Center. El estudio, la investigación y la resolución dinámicos de las excepciones de menor importancia pueden ayudar a los grupos de soporte de la red a reducir o a prevenir las interrupciones de la red.

## **Colección del mensaje de Syslog**

Los mensajes de Syslog son enviados por el dispositivo a un servidor de recolección. Estos mensajes pueden ser errores de hardware o de software o pueden ser informativos (por ejemplo cuando alguien ha estado en configurado terminal en un dispositivo).

La supervisión del Syslog requiere el soporte o los scripts de la herramienta de sistema de administración de red (NMS) ayudar a analizar y a señalar sobre los datos Syslog. Esto incluye la capacidad para clasificar los mensajes de Syslog por la fecha o período de tiempo, dispositivo, tipo de mensaje de Syslog o frecuencia del mensaje. En redes más grandes, las herramientas o los scripts se pueden implementar para analizar los datos Syslog y para enviar las alertas o las notificaciones a los sistemas de administración de eventos o las operaciones y personal de ingeniería. Si las alertas para una amplia variedad de datos Syslog no se utilizan, la organización debe revisar un diario más prioritario de los datos Syslog por lo menos y crear los tickets de problemas por problemas potenciales. Para dinámico detectar los problemas de red que no se pueden considerar con la supervisión normal, revisión periódica y análisis de los datos Syslog históricos se deben realizar para detectar las situaciones que pueden no indicar un problema inmediato, pero puede proporcionar una indicación de un problema antes de que se convierta en afectación del servicio.

## **Herramientas disponibles**

Algunas de las herramientas más populares del receptor de trampa SNMP incluyen el siguiente:

- HP OpenView Network Node Manager de Hewlett Packard en [openview.hp.com](http://openview.hp.com)
- Integridad del espectro de Aprisma en [www.aprisma.com](http://www.aprisma.com)
- Netview de IBM Tivoli en [www.tivoli.com](http://www.tivoli.com)

La herramienta más popular del Syslog para la Administración del Cisco IOS es CiscoWorks2000 administrador de RME Syslog. Otras herramientas disponibles incluyen el SL4NT, un programa del shareware de [www.netal.com](http://www.netal.com) que deja cisco.com y el soldado I de OpenSystems en [www.opensystems.com](http://www.opensystems.com)

## **Administración de problemas**

La administración de problemas, un aspecto de la administración de fallas, es la disciplina manejo de los problemas a partir de la época del acontecimiento a través de identificación, del troubleshooting, de resolución y de cierre.

Muchos clientes experimentan el tiempo de inactividad debido adicional a una falta de procesos en administración de problemas. El tiempo muerto adicional puede ocurrir cuando los administradores de la red intentan resolver el problema que usa rápidamente una combinación de comandos o de cambios de configuración de servicio-afectación bastante que pasando el tiempo en la Identificación del problema, la recopilación de información, y un trayecto de solución bien-analizado. La conducta observada en esta área incluye recargar los dispositivos o borrar las tablas de IP Routing antes de investigar un problema y su causa raíz. Esto ocurre en algunos



casos debido a los objetivos de la solución de problemas del soporte de primer nivel. El objetivo de todas las cuestiones relacionadas con software debería ser recolectar rápidamente la información necesaria para el análisis de las causas raíz antes de restaurar la conectividad o el servicio.

Un proceso de administración de problema se recomienda, y debe incluir cierto grado de descripciones de problemas predeterminadas y de colecciones apropiadas del comando " show " antes de extender el problema a un segundo nivel de soporte. El soporte de primer nivel debe nunca incluir las rutas del claro o los dispositivos el recargar. Idealmente, la organización del soporte de primer nivel debe recoger rápidamente la información y después extender el problema al soporte del segundo nivel. Pasando un poco más tiempo que identifica y que describe el problema en el soporte del nivel uno, una detección de la causa raíz es mucho más probable, así permitiendo una solución alternativa, una Identificación de laboratorio, y una información del bug. El soporte del segundo nivel se debe versificar bien en los tipos de información que Cisco puede necesitar para diagnosticar un problema o para clasificar un informe de bug, incluyendo:

- Vacíos de memoria
- Salida de información de ruteo
- Salida del comando show del dispositivo

## Estandarización de la configuración

Las normas de configuración del dispositivo globales representan la práctica de mantener los dispositivos y los servicios similares "globales" estándar de los parámetros de la configuración a través dando por resultado la coherencia de configuración global a nivel empresarial. Los comandos global configuration son los comandos que se aplican al dispositivo entero y no a los puertos individuales, a los protocolos o a las interfaces, y generalmente acceso del dispositivo del impacto, comportamiento general del dispositivo y seguridad del dispositivo. En el Cisco IOS, esto incluye los siguientes comandos:

- Servicio
- IP
- VTY
- Puerto de la consola
- Registro
- AAA/TACACS+
- SNMP
- Banner

También importante en las normas de configuración del dispositivo globales es una convención para nombres apropiada del dispositivo que permite que los administradores identifiquen el dispositivo, el tipo de dispositivo y la ubicación del dispositivo basados en el nombre DNS del dispositivo. La coherencia de configuración global es importante para la compatibilidad total y la confiabilidad de un entorno de red porque ayuda a reducir la complejidad de la red y a aumentar la compatibilidad de red. Muchas veces se experimenta una dificultad de soporte sin la estandarización de configuración debido a un comportamiento incorrecto o incoherente del dispositivo, al acceso SNMP y a la seguridad general del dispositivo.

Mantener las normas de configuración del dispositivo globales es lograda normalmente por un grupo interno de la ingeniería o de operaciones que cree y mantenga los Parámetros de configuración global para los dispositivos de red similares. Es también una práctica adecuada proporcionar una copia del archivo de configuración global en los directorios TFTP para poderlos

descargar inicialmente a todos nuevamente los dispositivos del aprovisionado. También útil es un archivo accesible de la red que proporciona el archivo de configuración estándar con una explicación de cada parámetro de la configuración. Algunas organizaciones configuran todos los dispositivos similares en una forma periódica para ayudar a asegurar la coherencia de configuración global, o periódicamente los dispositivos del estudio para los estándares correctos de la configuración global.

Los estándares de la interfaz o de la configuración del protocolo representan la práctica de los estándares que mantienen para la interfaz y la configuración del protocolo, que mejora la disponibilidad de la red reduciendo la complejidad de la red, proporcionando al dispositivo y al comportamiento del protocolo previstos y mejorando la compatibilidad de red. La inconsistencia de la interfaz o de la configuración del protocolo puede dar lugar al comportamiento del dispositivo inesperado, a las cuestiones del Traffic Routing, a los problemas de conectividad crecientes y al tiempo creciente del soporte reactivo.

Los estándares de la configuración de la interfaz pueden incluir:

- CDP (protocolo cisco discovery)
- Descriptores de la interfaz
- Configuración de guardado en memoria caché
- Otros estándares del específico del protocolo

Las normas de configuración específicas del protocolo pueden incluir:

- Configuración de IP Routing
- Configuración de DLSw
- Configuración de la lista de acceso
- Configuración de ATM
- Configuración de Frame Relay
- Configuración del árbol de expansión
- Asignación VLAN y configuración
- VTP (protocolo virtual trunking)
- HSRP (Hot Standby Routing Protocol)
- Otros dependiendo de qué se configura dentro de la red

Un ejemplo de los estándares IP puede incluir el tamaño de subred, el espacio de IP Address usado, el Routing Protocol usado y la configuración del Routing Protocol.

Mantener los estándares del protocolo y de la configuración de la interfaz es normalmente la responsabilidad de los grupos de la ingeniería y de la implementación de la red. El grupo de ingeniería debe ser responsable de identificar, de probar, de validar y de documentar los estándares. El grupo de la implementación es entonces responsable de usar los documentos de ingeniería o las plantillas de configuración para provision los nuevos servicios. El grupo de ingeniería debería crear documentación sobre todos los aspectos de estándares requeridos para asegurar consistencia. Las plantillas de configuración se deben también crear para ayudar a aplicar las normas de configuración. Los grupos de operaciones deberían capacitarse con respecto a las normas y deben ser capaces de identificar problemas de configuración no estándar. La coherencia de la configuración se ve de gran asistencia en la prueba, la validación, y la fase de la certificación. Sin las plantillas de configuración estandarizadas, es casi imposible probar, validar, o certificar adecuadamente una versión deL Cisco IOS para moderado una Red grande.

## [Administración de la disponibilidad](#)

La Administración de la disponibilidad es el proceso de la mejora de la calidad usando la disponibilidad de la red como la mejora de la calidad métrica. Muchas organizaciones ahora están midiendo el tipo de la Disponibilidad y de la caída del sistema. Los tipos de la caída del sistema pueden incluir el siguiente:

- Hardware
- Software
- Link/portador
- Poder/entorno
- Diseño
- Error de usuario/proceso

Identificando las caídas del sistema y realizando la análisis de la causa raíz inmediatamente después de la recuperación, la organización puede identificar los métodos para mejorar la Disponibilidad. Casi todas las redes que han alcanzado la Alta disponibilidad tienen algún tipo de proceso de la mejora de la calidad.

## [Lista de verificación de las operaciones de la Administración del Cisco IOS](#)

Paso 1: [Defina los requerimientos y objetivos comerciales](#) (el [clientes registrados solamente](#))

Paso 2: [Evalúe el estado actual de prácticas de administración del Cisco IOS Software](#) (el [clientes registrados solamente](#))

Paso 3: [Defina los papeles y las responsabilidades](#) (el [clientes registrados solamente](#))

Paso 4: [Desarrolle un Plan del proyecto de la administración del software](#) (el [clientes registrados solamente](#))

Paso 5: [Desarrolle una matriz de los requisitos de software](#) (el [clientes registrados solamente](#))

## [Información Relacionada](#)

Un apéndice se ha creado para ayudar al cliente en la obtención de la otra información relacionada valiosa del Cisco IOS por ejemplo: Los fundamentales del Cisco IOS, los procesos internos del Cisco IOS Software de Cisco, el análisis de confiabilidad del software, el Programa de calidad de Cisco las metodologías, de la prueba interna internos de Cisco, y una análisis de campo que muestre las prácticas actuales de la industria y al cliente total experimenta con el Cisco IOS Software

- Administración del Cisco IOS: La información adicional en el Cisco IOS Administración y mejores prácticas se puede encontrar en el White Paper del “Cisco IOS Administración para la conexión en red de alta disponibilidad” en el sitio siguiente:  
[http://www.cisco.com/en/US/tech/tk869/tk769/technologies\\_white\\_paper09186a00800a998b.shtml](http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a00800a998b.shtml)
- Para información específica sobre cómo ejecutar las sondas de la red, que comandos CLI de utilizar, cómo analizar e interpretar los datos del tráfico de la red, y cómo establecer las políticas de uso de la aplicación, visita <http://www.cisco.com>. Este sitio proporciona un rango

completo del soporte, del entrenamiento, de la referencia técnica, y de las soluciones asesores.

- El Cisco IOS tiene las convenciones para nombres específicas que se definen aquí: [http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products\\_tech\\_note09186a0080101cda.shtml](http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_tech_note09186a0080101cda.shtml)
- La información sobre la Disponibilidad del Cisco IOS Release se proporciona aquí: [http://www.cisco.com/en/US/products/sw/iosswrel/products\\_ios\\_cisco\\_ios\\_software\\_releases.html](http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_releases.html)
- Las versiones del Cisco IOS se quitan del CCO y pueden eventual ser ordenadas no más. Esté por favor seguro de fijar las Expectativas del cliente por consiguiente.
- Los boletines de productos del Cisco IOS se utilizan para anunciar las versiones del Cisco IOS a los clientes. Contienen la información abreviada sobre el contenido de versión. El control aquí para la Disponibilidad del nuevo Cisco IOS libera [http://www.cisco.com/en/US/products/sw/iosswrel/products\\_ios\\_cisco\\_ios\\_software\\_releases.html](http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_releases.html)
- La Seguridad de las manijas del Product Security Incident Response Team para los Productos Cisco. Cualquier problema relacionado con la seguridad del Cisco IOS se debe referir este equipo. Cisco la publica público es vulnerabilidades de seguridad. <http://tools.cisco.com/security/center/publicationListing>
- Defectos del Cisco IOS: Los defectos serios del Cisco IOS se deben recomendar para el aplazamiento. Cualquier empleado de Cisco puede hacer la recomendación.
- Los problemas del campo en el Cisco IOS se comunican a los clientes con las recomendaciones del Cisco IOS. [http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080b20ee1.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080b20ee1.shtml)
- Características deL Cisco IOS: Los clientes de los permisos de la herramienta Feature Navigator para encontrar las versiones que soportan las características específicas, y vice versa. <http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>
- El consejero en software de Cisco permite a los clientes para encontrar el software support para las características o el software support para el hardware. <http://tools.cisco.com/Support/Fusion/FusionHome.do> (clientes registrados solamente)

## [Servicios de Cisco y soporte](#)

- [Servicios de soporte técnico](#)
- [Servicios específicos a las tecnologías de interconexión de redes y a las soluciones de Cisco](#)