Administrar infraestructura tecnológica de red

Breve descripción:

Este componente busca facilitar la apropiación de los conocimientos para gestionar la infraestructura tecnológica de red según modelos de referencia y procedimientos técnicos, implementando sistemas de monitoreo según estándares, políticas y recursos de la organización.

Octubre 2023

Tabla de contenido

Introducción

La gestión y mantenimiento de una red es un proceso que requiere conocimiento técnico, metodológico y conceptual; en este componente se abordarán temas sobre estándares, políticas, análisis de riesgos y fallas, entre otros, que implican la contextualización de lo aprendido. El siguiente video presenta de manera genérica e introductoria en qué consiste la administración de una infraestructura tecnológica de red.

Video 1. Administrar infraestructura tecnológica de red

Enlace de reproducción del video

Síntesis del video: Administrar infraestructura tecnológica de red
La administración de una infraestructura tecnológica requiere de la planeación de las plataformas, del monitoreo constante del funcionamiento de la red para

prevenir posibles fallas o errores. De esta forma, se garantiza la estabilidad de la conexión y la seguridad de la red, la cual puede definirse como las prácticas y políticas que se adoptan con el fin de prevenir y supervisar el uso indebido, el acceso no autorizado, la modificación o denegación de la red informática y el acceso a sus recursos.

Todo lo anterior forman parte esencial de la gestión de una infraestructura tecnológica de red, la cual se implementa según los procedimientos técnicos y recursos de la organización.

1. Análisis y planeación

Si no existe una política de seguridad, la disponibilidad de la red puede verse comprometida. Por ello, se debe iniciar por evaluar los riesgos que tenga la red y pensar en crear un equipo de respuesta; luego, se realizará la implementación de la administración de la seguridad y supervisión de la red para detectar violaciones de seguridad; finalmente, con la revisión o supervisión, se deben realizar las modificaciones a que haya lugar y adaptarla a las exigencias de los posibles ataques que se puedan presentar.

Durante el análisis y planeación de las políticas de seguridad se enmarcan tres fases globales que son: preparación, prevención y restauración.

1.1. Preparación

Según el informe oficial de mejores prácticas para políticas de seguridad de la red de Cisco (2005), para implementar una política de seguridad previamente se debe hacer lo siguiente:

- Crear las declaraciones de política de uso.
- Realizar un análisis de riesgo.
- Establecer una estructura de equipo de seguridad.

Declaración de políticas de uso

Documento donde se detallan los roles y responsabilidades de usuarios referente a la seguridad. A continuación se describe el proceso de esta práctica.

Se inicia con una política general que incluye todo el sistema de red y datos al interior de la empresa o institución; suministra a los usuarios los elementos básicos de la política de seguridad, su propósito, las guías de consulta para mejores prácticas de seguridad y la definición de las responsabilidades en cuanto a la seguridad.

Luego, se crea una declaración de uso aceptable que provea a las personas las nociones básicas de información útil y disponible de la misma. Debe explicar, claramente, cualquier acto específico que se haya identificado como ataques a la seguridad y las acciones punitivas que serán tomados si se detecta un ataque a la seguridad (Cisco, 2005).

Por último, se establece la declaración de uso admisible del administrador que ayude a explicar los procedimientos para la administración de cuentas de usuario, aplicación de políticas y revisión de privilegios. La empresa debe presentar claramente las políticas específicas relativas a las contraseñas de usuario o al manejo posterior de datos adquiridos por dichos usuarios (Cisco, 2005)

Análisis de riesgo

En Cisco (2005), se menciona que el análisis de riesgos debe identificar los riesgos en la red, junto con los recursos de red, los datos, y sus partes, asignar una calificación de amenaza para cada parte, y aplicar un nivel adecuado de seguridad, lo cual permitirá mantener un equilibrio viable entre la seguridad y el acceso necesario a la red.

Para ello, se tiene en cuenta la asignación de los niveles de riesgo por recurso de red, los cuales pueden ser: bajo, medio y alto. Luego, con esta información se realizará una matriz de seguridad. A continuación se amplía cada uno de los niveles de riesgo.

- **Bajo riesgo.** Datos que de verse comprometidos (datos observados por el personal no autorizado, datos corruptos o datos perdidos), no se interrumpiría el servicio ni causaría problemas económicos y legales. En este caso la información, el dispositivo o los datos se pueden recuperar fácilmente y no permite el acceso adicional de otros sistemas.
- **Riesgo medio**. Los datos que sí estuvieron comprometidos (los datos vistos por el personal no autorizado, los datos corrompidos o los datos perdidos) causarían una interrupción leve en el servicio, problemas legales y económicos de menor importancia, o proporcionan el acceso adicional a otros sistemas. El dispositivo o los datos requieren un esfuerzo leve para restaurarse o el proceso de restauración perturba el sistema.
- **Riesgo alto**. Datos que de verse comprometidos (datos observados por el personal no autorizado, datos corruptos o datos perdidos), pueden causar interrupción extrema en el servicio y originarían problemas económicos o legales importantes, o amenazaría la integridad o la seguridad de una persona. El proceso de restauración requiere demasiado esfuerzo y ocasiona perturbaciones en el sistema.

Tan pronto se haya asignado el nivel de riesgo, es importante identificar los tipos de usuarios del sistema, entre los más comunes y que se pueden diferenciar son:

- **Usuarios internos**: usuario administrador responsable de los recursos de red, usuario privilegiado con mayor acceso o usuario con acceso general.
- **Usuarios externos**: usuarios con acceso a algunos recursos, otros usuarios externos o clientes.

Luego, al identificar tanto el nivel de riesgo como el tipo de acceso necesario de cada sistema de red, es importante construir la matriz de seguridad, la cual proporciona una referencia rápida para cada sistema y es el punto de partida para otras medidas de seguridad, como crear la estrategia adecuada para restringir el acceso a los recursos de red.

Tabla 1. Matriz de seguridad

Sistema	Descripción	Nivel de riesgo	Tipos de usuario
"Switches" ATM	Dispositivo del núcleo de red	Alto	Administrador para configurar el dispositivo (solo equipo de soporte técnico); los demás para usar como transporte.
"Routers" de la red	Dispositivo de distribución de red	Alto	Administrador para configurar el dispositivo (solo equipo de soporte técnico); los demás para usar como transporte.
"Firewall"	Dispositivo de red de acceso	Alto	Administrador para configurar el dispositivo (solo equipo de soporte técnico); los demás para usar como transporte.
Bases de datos Oracle	Aplicación de red	Alto o moderado	Administrador para administrar el sistema; usuarios con privilegios para actualización de datos; usuarios generales para acceso de datos; los demás para acceso a datos parciales.
"Switches" en "rack".	Dispositivo de red de acceso	Medio	Administrador para configurar el dispositivo (solo equipo de soporte técnico); los demás para usar como transporte.

Sistema	Descripción	Nivel de riesgo	Tipos de usuario
ISDN o servidores de marcación rápida.	Dispositivo de red de acceso	Medio	Administrador para configurar el dispositivo (solo equipo de soporte técnico); usuarios con privilegios para acceso especial.
Servidor interno de correo electrónico.	Aplicación de red	Medio	Administrador para configuración; los demás usuarios para uso interno.
DN y servidores DHCP.	Aplicaciones de red	Medio	Administradores para configuración; usuarios con privilegios y generales para uso de los servidores.
Servidor externo de correo electrónico.	Aplicación de red	Bajo	Administrador para configuración; los demás para transporte de correo entre Internet y el servidor de correo interno.

Establecer una estructura de equipo de seguridad

Se debe crear un equipo de seguridad funcional, liderado por un administrador de seguridad, en el que participen cada una de las áreas operativas de la empresa. Los representantes en el equipo deben conocer la política de seguridad y los aspectos técnicos del diseño y de la implementación de seguridad y se requiere, entonces, capacitación adicional para los miembros del equipo. La siguiente figura presenta una estructura del equipo de seguridad de acuerdo a su función.

Figura 1. Estructura del equipo de seguridad

Descripción de la figura: Estructura del equipo de seguridad
La estructura del equipo de seguridad está confirmado en tres niveles. **Operativo:** • Seguridad ligadas a los recursos humanos • Seguridad física y ambiental • Desarrollo y mantenimiento de sistemas • Gestión de comunicaciones y operaciones • Gestión de la continuidad del negocio **Estratégico**: • Gestión de activos • Control de accesos

- Cumplimiento

Táctico:

- Política de seguridad
- Aspectos organizativos de la seguridad de la información.

Sumado a esto, el equipo de seguridad posee tres áreas de responsabilidad: elaboración de políticas, práctica y respuesta.

- **Elaboración de políticas**: está centrada en establecer y revisar las políticas de seguridad para la compañía, es necesario revisar brevemente el análisis de riesgos y la política de seguridad anualmente.
- **Práctica**: es la etapa en la que el equipo de seguridad realiza el análisis de riesgos, aprueba las solicitudes de cambio de seguridad, revisa las alertas de seguridad de los proveedores y la lista de correo CERT ("Critical Emergency Response Team"). También debe convertir los requisitos de la política de seguridad en implementaciones técnicas específicas con lenguaje sencillo.
- **Respuesta:** mientras que la supervisión de red identifica las violaciones de seguridad, es al equipo de seguridad quien le corresponde realizar la solución de problemas y la corrección de dichas violaciones. Cada uno de los miembros del equipo de seguridad debe conocer detalladamente las funciones de seguridad proporcionadas por el equipo en su área operativa.

Una vez definidas las responsabilidades de equipo, se deben establecer las funciones individuales y responsabilidades de cada uno de los miembros del equipo de seguridad.

1.2. Prevención

La prevención se puede dividir en dos partes: cambios en la seguridad y vigilar la seguridad de red.

Cambios en la seguridad

Están definidos como los cambios al equipo de red que impliquen un posible impacto en la seguridad general de la red. La política de seguridad debe identificar requisitos de configuración de seguridad específicos, en términos no técnicos. Es decir, en lugar de definir un requisito como “Ninguna conexión al FTP de las fuentes externas se permitirá a través del “firewall””, se debe definir el requisito como “Las conexiones externas no deben extraer archivos de la red interna” (Cisco, 2005).

El equipo debe definir un conjunto único de requisitos para la organización, entre los cuales está el de revisar la lista de requisitos de lenguaje sencillo para identificar la configuración de red o los problemas de diseño específicos que cumplan los requisitos. Una vez creados estos cambios en las configuraciones de la red requerida para implementar la política de seguridad, se pueden aplicar a cualquier cambio de configuración posterior.

El equipo de seguridad debe revisar los siguientes cambios y cumplir con las siguientes guías de consulta.

Cambios de prevención

- Cambios la configuración “firewall”.
- Cambio en las listas de control de acceso (ACL).
- Cambios en la configuración del “Simple Network Management Protocol” (SNMP).

- Cambio o actualización en el “software” que sea diferente al del listado de nivel de revisión de “software” aprobado.

Guías de consulta

- Cambiar habitualmente las contraseñas de los dispositivos de red.
- Restringir el acceso a los dispositivos de red a una lista aprobada de personas.
- Asegurar que los niveles de revisión del “software” actual del equipo de red y de los entornos de servidor cumplan con los requisitos de configuración de seguridad.

Además de lo mencionado anteriormente, sería importante incluir a un representante del equipo de seguridad en la junta de aprobación de administración de cambios, para que supervise los cambios que revisa la junta. El representante del equipo de seguridad tiene la potestad para negar cualquier cambio que se considere cambio de seguridad hasta que haya sido aprobado por el equipo de seguridad.

Vigilar la seguridad de red

“La supervisión de seguridad es similar a la supervisión de red, a menos que se centre en la detección de los cambios en la red que indican una violación de seguridad” (Cisco, 2005). Con la supervisión de la seguridad se puede determinar cuál es la violación y, al realizar el análisis de riesgo, es posible identificar el nivel de supervisión necesario en términos de la amenaza para el sistema; de otra parte, al aprobar los cambios de seguridad se identifican las amenazas concretas para la red y todos estos parámetros permiten desarrollar con claridad lo que se necesita supervisar y con qué frecuencia.

En la matriz del análisis de riesgos, el “firewall” se considera un dispositivo de red de riesgo elevado, esto indica que debe supervisar en tiempo real. La sección aprobación de los cambios de seguridad específica que debe supervisar cualquier cambio al “firewall”. Esto significa que el agente de la consulta SNMP debe supervisar intentos fallidos de ingreso al sistema, tráfico inusual, cambios al “firewall”, acceso concedido al “firewall”, y configuración de conexiones a través del “firewall” (Cisco, 2005).

Con el ejemplo anterior, se asegura la posibilidad de crear una política de monitorización para cada área identificada en el análisis de riesgos. Es recomendable supervisar, cada semana, el equipo de bajo riesgo; a diario, el equipo de riesgo moderado; y cada hora, el equipo de riesgo elevado. Si por cualquier eventualidad se requiere una detección más rápida, se debe supervisar en intervalos más cortos de tiempo.

Como última recomendación, la política de seguridad debe poder notificar al equipo de seguridad sobre las violaciones de seguridad. Normalmente, el “software” de supervisión de red es quien, en primera instancia, detecta la violación con acciones de notificación al centro de operaciones y al equipo de seguridad, y si se necesita hacer uso de un localizador.

1.3. Respuestas

Para abordar la temática de respuesta se puede enmarcar en tres aspectos: violaciones de seguridad, restauración y revisión.

Violaciones de seguridad

Al detectar una violación se hace necesario tomar decisiones de forma muy rápida que permitan proteger el equipo de red, determinar el fragmento de intrusión, recuperar las operaciones normales del sistema y la respuesta a una intrusión sea más viable. El primer paso a realizar después de detectada una intrusión es notificar al equipo de seguridad. Por lo tanto, debe existir un procedimiento adecuado en la política de seguridad que aplique la respuesta adecuada y que, además, esté disponible las 24 horas del día, los siete días de la semana.

El nivel de autoridad dado al equipo de seguridad debe estar definido de tal manera que se pueda realizar los cambios, indicando el orden de los mismos, estas acciones correctivas son:

- Aislar, desconectar y apagar los sistemas que han sido violados o la fuente de la violación.
- Establecer contacto con el portador o el ISP en un intento de localizar el ataque.
- Implementar cambios para prevenir accesos adicionales a la violación.
- Notificar al personal del área legal administrativa interna.
- Restaurar los sistemas según la lista de prioridades.
- Tener comunicación directa con la policía, y otros organismos gubernamentales.
- Utilizar dispositivos de grabación para obtener pruebas.

Es importante detallar cualquier cambio que se haya realizado sin la aprobación administrativa en la política de seguridad, de tal forma que se pueda determinar el

grado en que se vio comprometido el sistema por el ataque a la seguridad, y procesar también las violaciones externas.

A continuación, se relacionan algunos aspectos a tener en cuenta para determinar el grado de violación.

- Registrar el evento al obtener los rastros del espía de la red, los archivos del registro, los usuarios activos, y las conexiones de red.
- Inhabilitar las cuentas, desconectar de la red y de internet para limitar cualquier compromiso adicional.
- Realizar una copia de seguridad del sistema implicado, ayudando a analizar, detalladamente, el daño y el método de ataque.
- Buscar qué otros sistemas o cuentas fueron comprometidos en el ataque.
- Conservar y revisar, constantemente, los archivos de registro de dispositivos de seguridad y de supervisión de red pues son de gran ayuda al proporcionar pistas sobre el método de ataque.

Restauración

Restaurar el funcionamiento normal de la red es el objetivo final de la respuesta a una violación de seguridad; en la política de seguridad se debe definir cómo realizar y conservar las copias de seguridad disponibles, detallar para cada sistema las condiciones de seguridad que requiere la restauración de estas copias y si se necesita aprobación previa, se debe incluir el proceso para obtener la aprobación.

Revisión

El proceso de revisión es el esfuerzo final para crear y mantener una política de seguridad. Hay tres aspectos que se deben revisar:

- **Política**. Debe ser dinámica y adaptativa a un entorno evolutivo. Para mantener la red actualizada es importante revisar la política existente contra las mejores prácticas conocidas. Controlar el sitio web permitirá saber si hay consejos útiles, prácticas, mejoras de la seguridad y alertas que se puedan incorporar a la política de seguridad.
- **Postura.** Los datos que sí estuvieron comprometidos (los También se debe comparar la postura de la red con la postura de seguridad deseada, pues en cualquier momento, un ente externo especialista en seguridad puede intentar penetrar en la red y probar la postura de la red y la respuesta de seguridad de la organización. Es recomendable para las redes de alta disponibilidad, realizar esta prueba cada año.
- **Práctica**. Se especifica como una prueba o ejercicio del equipo de soporte técnico, con esto se podría asegurar que poseen los conocimientos necesarios durante una violación de seguridad. No es requisito notificar este ejercicio por parte de la administración y se puede realizar en conjunto con la prueba de postura de la red. Aquí se identifican los tiempos en los procedimientos y la capacidad del personal para tomar acciones correctivas.

2. Gestión y monitoreo

Estos dos conceptos a tratar son totalmente diferentes y se definirán a continuación.

La **gestión** se refiere al control de los recursos en la red para evitar fallas en su funcionamiento y degradación de los servicios que presta, mientras que el **monitoreo** abarca el proceso continuo de recolección y análisis de datos que permitan anticipar inconvenientes en la red.

En general, un sistema de gestión y monitoreo de redes permite controlar los recursos "software" y "hardware" en la red por medio del monitoreo constante a dichos recursos. También permite observar la red completa como una arquitectura única asignando a cada punto las direcciones y etiquetas, con propiedades concretas para cada componente y enlace del sistema conocido.

Los elementos básicos de un sistema de gestión y monitoreo de redes se presentan a continuación:

- **Gestor o estación de gestión**. Llamado también NMS ("Network Monitoring System" - Sistema de Monitoreo de Red) actúa como como interfaz entre el sistema de gestión de red y el administrador de red posee una base de datos de información para gestión de red sacada de las bases de datos de todas las entidades a gestionar en la red. Ejecutan aplicaciones que supervisan, permanentemente, todos los dispositivos.
- **Agente**. Poseen bases de datos local de información de administración. Es un elemento activo encargado de responder a las solicitudes de acción iniciadas en la estación de gestión y de manera asíncrona, proporciona

información importante y no solicitada a la estación de gestión. Se trata de un módulo del "software" de gestión de red implantado en los dispositivos a gestionar. Los recursos de red a ser gestionados aparecen como objetos que hacen parte de la MIB ("Management Information Base" – Base de Información de Gestión).

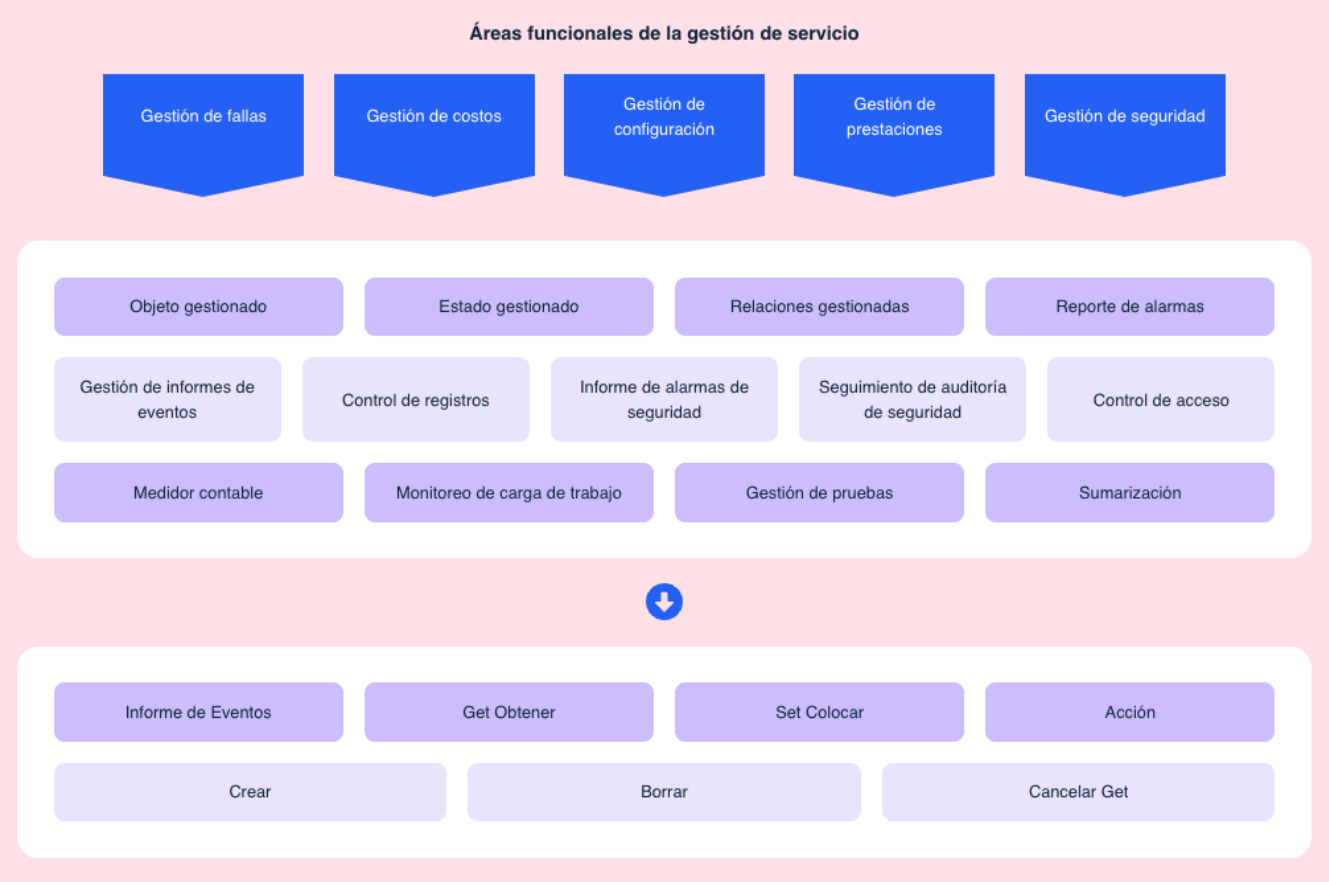
- **Dispositivos administrativos**. Recogen y almacenan información de control y monitoreo.

El protocolo SNMP ("Simple Network Management Protocol"- Protocolo de gestión de red simple) es el encargado de comunicar la estación de gestión y el agente; dicho protocolo cuenta con las siguientes capacidades clave:

- ***"Get":*** obtener valores específicos del agente por parte de la estación de gestión.
- ***"Set":*** se establecen valores específicos en el agente desde la estación de gestión.
- ***"Notify":*** notificación de eventos significativos desde el agente hacia la estación.

A continuación se presentan las áreas funcionales de la gestión de servicio.

Figura 2. Áreas funcionales de la gestión de servicio



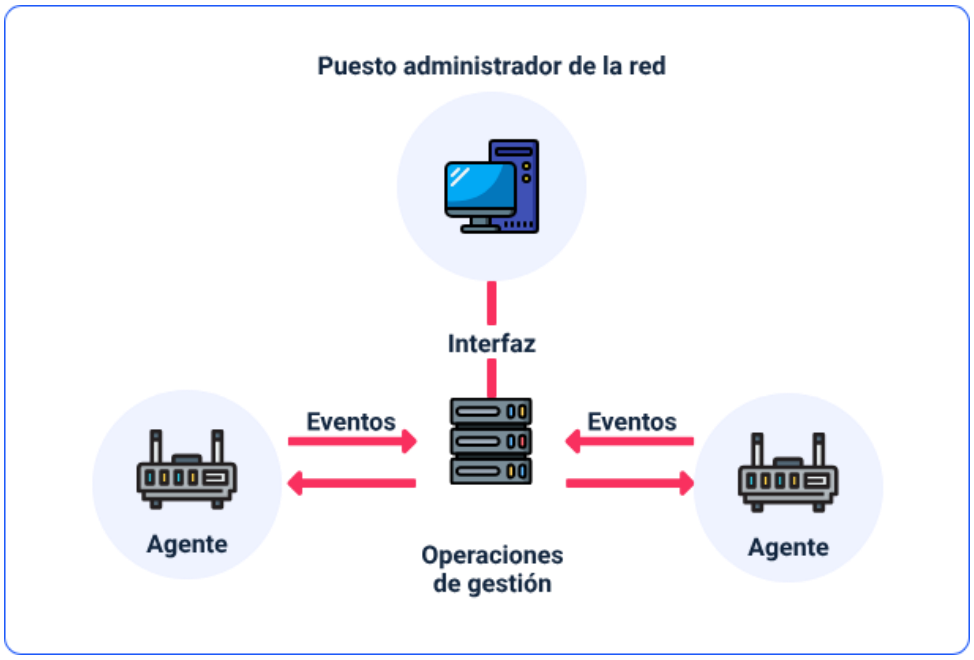
Descripción de la figura: Áreas funcionales de la gestión de servicio
Las áreas funcionales de la gestión de servicio son: gestión de fallas, gestión de costos, gestión de configuración, gestión de prestaciones y gestión de seguridad. Estas a su vez desarrollan trece estándares: objeto gestionado, estado gestionado, relaciones gestionadas, reporte de alarmas, gestión de informe eventos, control de registros, informe de alarmas de seguridad, seguimiento de auditoría de seguridad, control de acceso, medidor contable, monitoreo de carga de trabajo, gestión de pruebas y sumarización.

Finalmente, dichos estándares definen las funciones de gestión de los servicios:

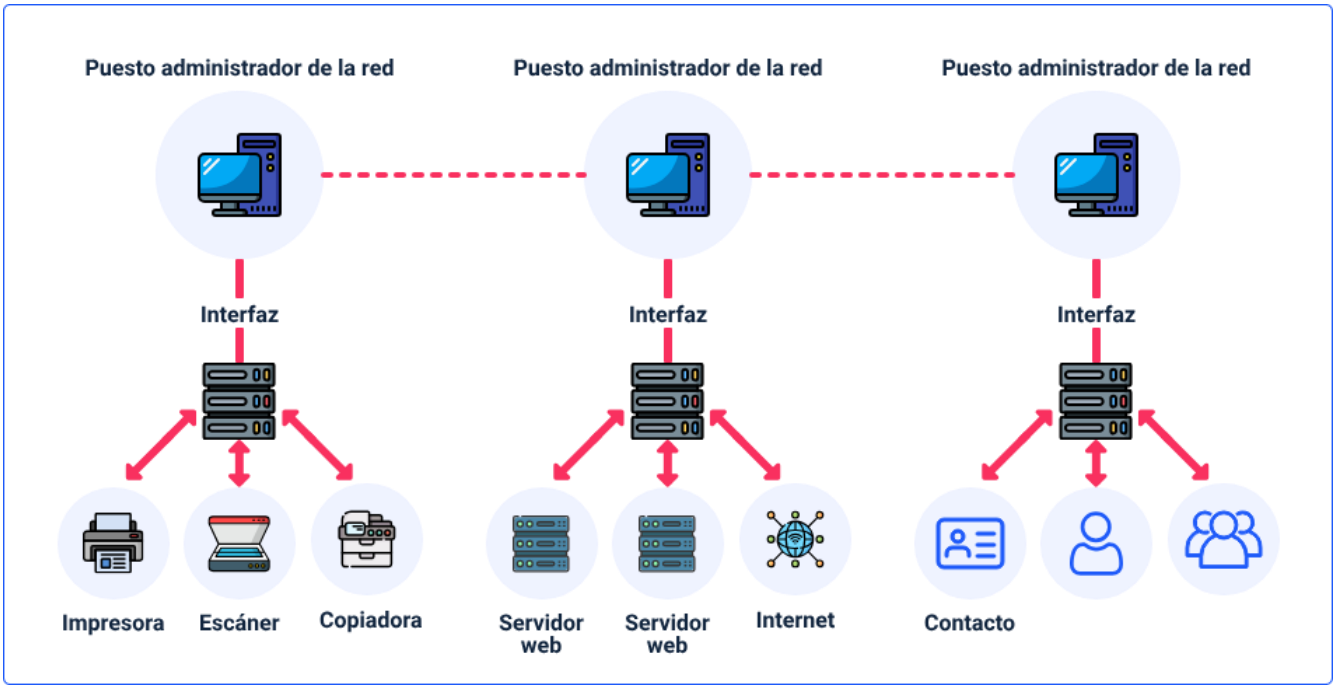
Informe de eventos, “get” obtener, “set” colocar, acción, crear, borrar y cancelar “get”.

Para el monitoreo de la red existen dos esquemas para gestionarla, esto de acuerdo con su tamaño, que se pueden nombrar como: centralizado y descentralizado.

Centralizado. Existe solo una estación de gestión para el control de los recursos de la red, es utilizado especialmente en las redes de Área Local LAN (“Local Area Network”).



Descentralizado. Existen varias estaciones de gestión de alto nivel denominadas servidores de gestión, cada cual puede gestionar directamente una parte de los agentes. Se utiliza especialmente para las redes de Área Amplia WAN (“Wide Area Network”).



2.1. Gestión de fallas

Mantener la conectividad, las aplicaciones y los servicios de una red funcionando a un nivel óptimo es algo imprescindible en la gestión de redes. La gestión de fallas de red ayuda a identificar, evitar y resolver los problemas que pueden dificultar el rendimiento de una red de transmisión digital.

Los gastos que pueden acarrear una mala gestión de la red pueden llegar a ser importantes, además de conllevar pérdida de tiempo y rendimiento.

La gestión de fallas de la red se hace necesaria, pues mantener y garantizar la continuidad y el funcionamiento de la red se ha vuelto crucial. Una buena gestión de los fallos ofrece vertientes muy positivas, pues permite mantener un rendimiento de red óptimo garantizando la disponibilidad, la minimización de los tiempos de inactividad y la detección temprana de los fallos.

Se pueden definir las fallas o eventos de una red como aquellos sucesos que interfieren en el correcto funcionamiento de la red, y por consiguiente disminuyen significativamente su rendimiento. Los ejemplos de fallos más comunes incluyen fallos en el "hardware", en el cableado, interferencia inalámbrica, así como un cambio en el estado del puerto, saturación de ancho de banda o, lo que es peor, la pérdida de conectividad.

El proceso de gestión de fallas puede verse modificado en cuestión de la plataforma utilizada para ello, pero comúnmente se siguen los siguientes pasos:

Detectar la localización del fallo. La continua monitorización de la red permite detectar anomalías en el rendimiento de la red o la interrupción del funcionamiento de esta, para ello normalmente se aplica la gestión de fallas activa y/o pasiva de red.

Por un lado, la gestión de fallas activa realiza continuas consultas a diferentes elementos de la red en busca de los dispositivos de la red y de su estado. Es decir, la gestión activa está solicitando, constantemente, información para detectar cualquier fallo. Por otro lado, la gestión de fallas pasiva monitorea los entornos de la red para detectar eventos que suceden y que ellos mismos muestran que se ha producido una falla, sin necesidad de recurrir a las continuas consultas que vimos en la gestión activa.

En definitiva, la gestión activa pregunta por las fallas a los diferentes elementos de una red. Por el contrario, la gestión pasiva se limita a escuchar, es decir, detectar eventos que indican claramente que se ha producido un fallo.

Análisis y aislamiento. Identificar el tipo de evento o falla sucedido en la red que ha producido un impacto y conocer su causa raíz son procesos de los más importantes. Una vez comprendido el problema, el fallo se ha de aislar de la red con el fin de que la

red continúe en funcionamiento con normalidad, garantizando de este modo la continuidad en el servicio.

Informar. Una de las partes muy importantes es la notificación del fallo. Puesto que permite avisar de los problemas a los técnicos de asistencia técnica, a los administradores mediante correo electrónico o SMS, y de forma visual a los administradores de NOC.

Resolver. Se evalúa el origen del problema, y en su caso se subsana o se reemplaza. Es importante contar con un buen NMS ("Network Management System") que permita resolver los problemas de forma sencilla y ágil, de forma automática e incluso poder aplicar el mantenimiento preventivo.

Plataformas de administración de redes

Una plataforma para gestionar la red se puede considerar como una aplicación "software" con funcionalidades básicas de gestión para los dispositivos que la conforman.

La plataforma debe suministrar funciones básicas entre las cuales se tienen:

- Interfaz gráfica de usuario (GUI).
- Mapa de red.
- Sistema gestor de base de datos (DBMS).
- Método estándar de consulta de dispositivos (protocolo).
- Menús configurables del sistema.
- Registro de eventos ("Event Log").

Igualmente, debe mostrar estas características adicionales:

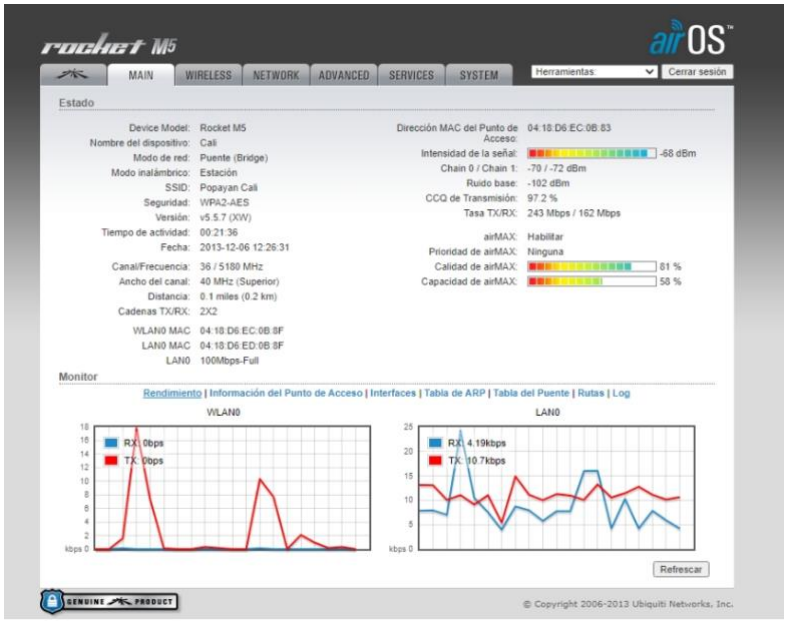
- Herramienta para gráficos.
- Seguridad del sistema.

En la actualidad existen diferentes plataformas de gestión de redes y estas depende de cada uno de los fabricantes de los componentes o dispositivos de red; de acuerdo con lo anterior, se pueden nombrar las siguientes:

- Air OS Redes inalámbricas Ubiquiti.
- CiscoView por medio web WWW fabricante Cisco.
- Netview for AIX (Tivoli) proveedor IBM.
- OpenView de HP.
- Spectrum de Cabletron.
- SunNet Manager (Solstice), fabricante Sun.

A continuación, se puede visualizar la interfaz gráfica principal donde se visualiza el rendimiento para un radioenlace con equipos Rocket M5 de Ubiquiti, visualizando desde la estación o receptor.

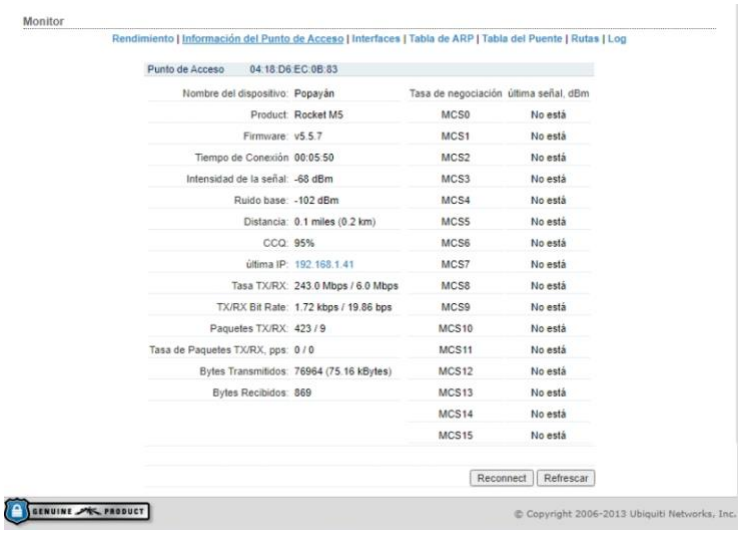
Figura 3. Interfaz gráfica Rocket M5



Nota. Tomado de Ubitiqui Networks, Inc. (2006-2013)

De otro lado, se puede observar también para este caso los datos del punto de acceso a la red o transmisor con todas las características del mismo.

Figura 4. Resumen información del punto de acceso



Nota. Tomado de Ubitiqui Networks, Inc. (2006-2013)

A continuación, se muestra en un video los menús de gestión y administración en el sistema Air OS de un radioenlace específico entre dos puntos, realizado con equipos Rocket M5 de Ubiquiti Networks.

Video 2. Gestión AIROS Ubiquiti

Enlace de reproducción del video

Síntesis del video: Gestión AIROS Ubiquiti
Videotutorial en el que se explica como acceder al monitor de gestión y administración de un radio enlace específico con un equipo Rocket M5 de Ubiquiti Networks para conectarse entre la ciudad de Popayán y Cali. Los equipos se encuentran configurados con un punto de acceso o transmisor y una estación o receptor.

Como paso inicial se debe configurar la IP del PC en el que se va a trabajar por el “Panel de control”, luego “Redes e internet” y, finalmente, “Centro de redes y recursos compartidos”. Están allí se va a cambiar la configuración de Ethernet. Se da clic en “Propiedades” y en “versión 4 (TCP/IPv4). Se abre una ventana, y allí, manualmente, se coloca la dirección IP, dentro del mismo rango del equipo. Una vez se escribe, aparece automáticamente la Máscara de subred y se coloca la puerta de enlace con la dirección del equipo al cual se va a enlazar el monitoreo. Con estos pasos ya se puede ingresar a la configuración del monitoreo.

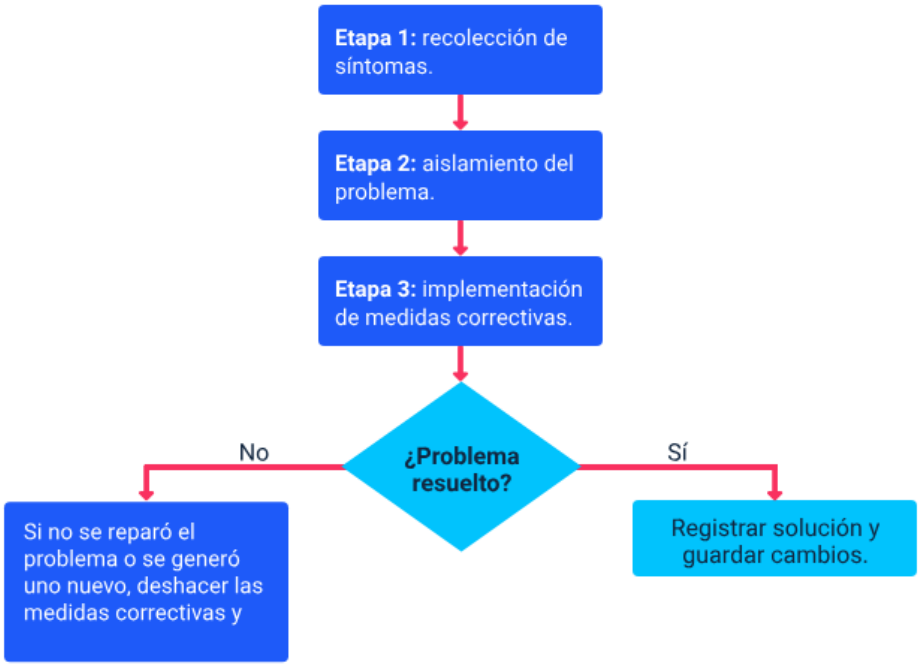
Después, se ingresa con el navegador a la IP del equipo. Estando allí se visualiza todo el monitor, el rendimiento de las redes, el estado del punto de acceso, interfaces, la tabla de ARP, la tabla Puente, las rutas y las novedades del radio enlace.

Infraestructura de resolución de problemas

La resolución de problemas es el proceso de identificar, hallar y corregir problemas. Los individuos con experiencia suelen seguir su instinto para resolver los problemas; no obstante, existen técnicas estructuradas que se pueden usar para determinar la causa más probable y la solución correspondiente.

El siguiente diagrama muestra los procedimientos generales para la resolución de problemas incluyendo las etapas básicas.

Figura 5. Resolución de problemas



Descripción de la figura: Resolución de problemas
Inicia con la recolección de síntomas, luego se asila el problema y finalmente se implementan las medidas correctivas. Si no se resuelve el problema o se generó uno nuevo, hay que deshacer las medidas correctivas y comenzar nuevamente. Por el contrario, si el problema se resuelve, se registra la solución y se guardan los cambios.

Al resolver problemas debe completarse la documentación correspondiente y esta documentación debe incluir toda la información posible sobre lo siguiente:

- El problema encontrado.

- Los pasos dados para determinar la causa del problema.
- Los pasos para corregir el problema y asegurarse de que no vuelva a ocurrir.

Cuando se informe un problema, se debe verificar y determinar el alcance; una vez confirmado el problema, el primer paso para resolverlo es recopilar información.

Recopilación de información: recopilar información directamente de los afectados es un buen punto de partida. En las preguntas se pueden incluir los siguientes temas: experiencias del usuario final, síntomas observados, mensajes de error e información sobre cambios recientes de configuración en dispositivos o aplicaciones.

Hay varias técnicas para resolver problemas, entre ellas:

- **Descendente**: inicia con la capa de aplicación y sigue hacia abajo. Analiza el problema desde el punto de vista del usuario y de la aplicación.
- **Ascendente**: empieza con la capa física y sigue hacia arriba. La capa física tiene que ver con el “hardware” y las conexiones de cables.
- **Divide y vencerás:** suele comenzar en una de las capas del medio para luego seguir hacia arriba o hacia abajo.

Sumado a lo anterior, también se deben tener en cuenta estos aspectos.

¿En qué consiste la técnica "ensayo y error"?

Se basa en el conocimiento individual para determinar la causa más probable del problema. El encargado de resolver problemas supone cuál puede ser la solución más probable según su experiencia previa y sus conocimientos de la estructura de la red. Tras implementar la solución, si no funciona, emplea esta información a fin de

determinar la segunda causa más probable; este proceso se repite hasta aislar y solucionar el problema.

¿En qué consiste el llamado problema físico?

A continuación, se amplía sobre esta temática y algunos comandos que se usan para la resolución de problemas:

Video 3. ¿En qué consiste el llamado problema físico?

Enlace de reproducción del video

Síntesis del video: ¿En qué consiste el llamado problema físico?
Los problemas físicos, principalmente, tiene que ver con los aspectos de “hardware” de las computadoras, los dispositivos de “networking” y con los cables

que los interconectan. No tienen en cuenta la configuración lógica de esta "software" de los dispositivos.

Los problemas físicos pueden surgir en redes conectadas por cable o inalámbricas. Uno de los mejores métodos para detectar problemas físicos es utilizar los sentidos (vista, olfato, tacto y oído). A continuación, algunos comandos que se utilizan para la resolución de estos problemas:

- "**Ipconfig**". Se utiliza para ver información sobre la configuración IP actual de un "host".
- "**Ping**". Se utiliza para probar si se puede acceder a un host de destino.
- "**Tracert**". Proporciona información de conectividad de la ruta que un paquete recorre a fin de llegar a destino e información de conectividad de cada "router" (salto) que haya en el camino. También indica cuánto tarda el paquete en ir del origen a cada salto y volver (tiempo de ida y vuelta). "Tracert" puede ayudar a identificar dónde se perdió o se demoró un paquete debido a cuellos de botella o zonas más lentas de la red.
- "**Netstat**". Es una utilidad de red importante que puede usarse para verificar esas conexiones. "Netstat" indica el protocolo que se está usando, la dirección y el número de puertos locales, la dirección y el número de puertos ajenos y el estado de la conexión.
- "**Nslookup**". Permite que el usuario final busque información sobre un nombre DNS en particular en el servidor DNS. Al enviar el comando "**Nslookup**", la información recibida incluye la dirección IP del servidor

DNS que se está utilizando y la dirección IP asociada al nombre DNS especificado. "**Nslookup**" se suele usar como herramienta para la resolución de problemas, a fin de determinar si el servidor DNS resuelve los nombres como corresponde.

Detección de fallas y notificaciones

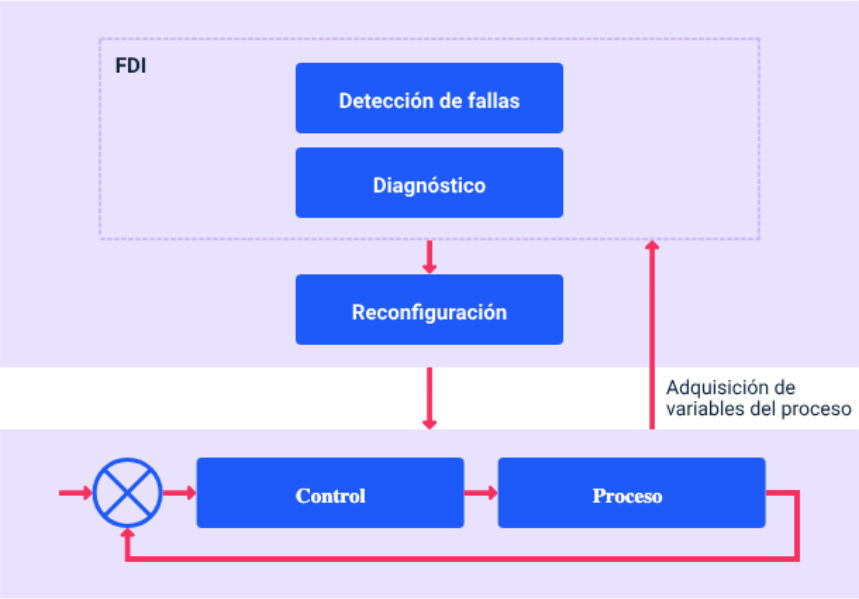
Los procesos actuales, por su complejidad, exigen sistemas de seguridad cada vez más confiables. El mal funcionamiento de los equipos puede provocar pérdidas económicas, peligro para los operarios e inconvenientes para los usuarios, entre otros.

a supervisión de procesos es el conjunto de acciones orientadas a asegurar un correcto funcionamiento, incluso en situaciones de riesgo. Un sistema de supervisión debe cumplir tres etapas fundamentales: la detección de fallas, su diagnóstico y el restablecimiento de las condiciones de operación de acuerdo con las especificaciones.

De acuerdo con Hurtado et al. (2016), una falla es un cambio en el comportamiento de alguno de los componentes de un sistema, de manera que este ya no puede cumplir con la función para la cual fue diseñado. Los sistemas de detección y diagnóstico de fallas se presentan como una solución que permite determinar el estado de operación del proceso, así como identificar la naturaleza de las fallas presentadas, su localización y riesgo.

La figura a continuación muestra un esquema general de un sistema de detección y diagnóstico de fallas.

Figura 6. Sistema de detección y diagnóstico de fallas



En este esquema, las entradas y salidas del bloque proceso-controlador alimentan un sistema de supervisión encargado de detectar la presencia de fallas y diagnosticar su naturaleza. Con esta información es posible corregir los parámetros del controlador de forma manual o automatizada o intervenir en el proceso para corregir los problemas detectados.

Se han propuesto múltiples enfoques para realizar la detección y el diagnóstico de fallas, de los cuales se puede hacer la siguiente clasificación:

Métodos basados en modelos matemáticos del proceso. Son estrategias que hacen uso de un modelo formulado a partir del conocimiento de las dinámicas involucradas en el proceso. Se fundamentan en la obtención de una diferencia entre las salidas del proceso y de un modelo del proceso, de donde se infiere la presencia de una falla. Este enfoque representa un costo computacional muy bajo y únicamente puede

ser aplicado a procesos donde es posible obtener dicho modelo de forma analítica, lo que limita su aplicación en sistemas no lineales. La obtención de los parámetros del proceso también representa una gran dificultad, la cual puede ser abordada por técnicas de identificación de sistemas.

Métodos a partir de modelos obtenidos de datos históricos del proceso. Para sistemas donde es posible recolectar numerosos datos representativos de su operación, tanto en condiciones normales como anormales, es posible construir un modelo mediante técnicas como redes neuronales o modelos difusos del tipo Takagi-Sugeno. Estos enfoques son, generalmente, costosos computacionalmente y requieren de grandes volúmenes de datos representativos, los cuales en algunas ocasiones no están disponibles; resultan muy útiles para obtener modelos de sistemas dinámicos no lineales.

Métodos a partir de datos del proceso. Parten igualmente de grandes volúmenes de datos históricos, pero desde una perspectiva diferente en la que no se busca obtener un modelo del proceso, sino resolver un problema de clasificación. Para este propósito se ha propuesto el uso de clasificadores difusos, análisis de componentes principales, redes neuronales artificiales, máquinas con vectores de soporte, funciones de base radial, entre otras. El principal inconveniente de estas técnicas radica en el costo computacional y en que generalmente operan como un sistema de “caja negra”, incapaz de brindar información adicional sobre la falla.

Monitoreo y notificación proactiva de fallas

El monitoreo de red consiste en realizar periódicamente o en tiempo real mediciones del comportamiento de la red, esto mediante el uso de un software para la

facilidad y precisión de los informes de estado. Un sistema de monitorización de red busca problemas causados por la sobrecarga y/o fallas en los servidores, como también problemas de la infraestructura de red u otros dispositivos.

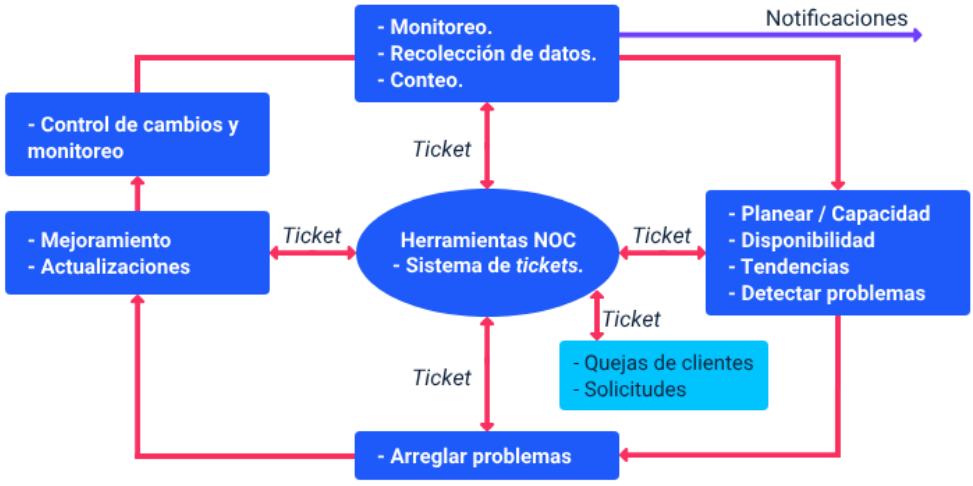
Cuando se monitoriza el servidor, y sus servicios en general, es vital para la infraestructura anticiparse ante cualquier inconveniente. Durante este proceso se verifican también los códigos HTTP enviados del servidor, que suelen ser la forma más rápida de verificar el funcionamiento de estos. Así, pues, se envían notificaciones después del proceso anticipado del monitoreo, para que se puedan resolver las fallas en el sistema.

La notificación proactiva de fallas consiste en generar notificaciones cuando los valores supervisados se acercan a los umbrales de fallas conocidos y no esperar a que el sistema avise que ya falló o, lo que es peor, descubrir por los clientes que la aplicación o el servicio se encuentran inactivos. Con este enfoque, se puede identificar y resolver problemas antes de que sean graves o comiencen a afectar a los usuarios. Con la 2014 "DevOps Research and Assessment" - DORA (Investigación y evaluación de DevOps de 2014 – DORA, (PDF), se demostró que la supervisión proactiva es un predictor importante del rendimiento de la entrega de "software". Según la investigación de DORA, los equipos que usan notificaciones proactivas pueden diagnosticar y resolver problemas con rapidez. Cuando las fallas se informan mediante una fuente externa al equipo de operaciones, como el centro de operaciones de red (NOC) o, peor aún, por parte de los clientes y no mediante la supervisión interna, el rendimiento se ve afectado (Google Cloud, 2020).

2.2. Administración de configuración

Proceso en el cual se preparan los dispositivos y es en la configuración donde se determina el comportamiento de los datos en la red. La administración enmarca las siguientes funciones: inicializar, desconectar o desactivar de forma ordenada la red o parte de ella, mantenimiento y adición de componentes, reconfigurar, definir o cambiar parámetros de configuración, denominar elementos de la red, conocer qué dispositivos tiene la red y configurar “hardware” y “software” de dichos dispositivos.

Figura 7. Administración de configuración



Descripción de la figura: Administración de configuración
Los sistemas de “tickets” permiten: • Arreglar y detectar problemas • Atender las quejas y solicitudes de clientes.

- Monitorear, realizar conteo y recolección de datos.
- Controlar los cambios y actualizaciones

Para la administración de configuración se tienen las tareas siguientes:

- Actualizar el "software".
- Controlar versiones de "software".
- Definir información de configuración de recursos.
- Establecer los usuarios que pueden utilizar recursos específicos.
- Inicializar y finalizar los servicios de red.
- Comprobar la información de configuración en el momento de un ataque, para asegurar que continúa en estado correcto.
- Modificar propiedades de recursos e informar al usuario de los cambios.
- Realizar el arranque y parada de componentes específicos de forma remota.

Estándares de configuración

En la administración existen herramientas básicas como: monitorear la red para verificar elementos activos, con qué características obtener la información, de qué modo están conectados entre sí los diferentes elementos, esta información se mantiene para ayudar a otras funciones de administración.

Administración de archivos de configuración

Se establece la configuración de los dispositivos activos cambiando la configuración por defecto con la nueva configuración, teniendo esto como la

configuración original del dispositivo. Es importante guardar la configuración antes de reiniciar el equipo debido a que se puede perder la configuración en caso contrario.

2.3. Gestión de inventario

Para la empresa y el administrador de la red es muy valioso conocer el inventario de dispositivos activos de TI o de red que componen la red. Es importante realizar este proceso acompañado de un "software" de gestión de inventarios, para conocer de primera mano las altas y bajas de la infraestructura.

Los siguientes se consideran "software" para gestión de inventario de redes:

- Network Inventory Advisor.
- Spicework.
- Lansweeper.
- Total Network Inventory.
- Open Audit.
- EMCO Network Inventory.

2.4. Gestión de "software"

Al igual que la administración del "hardware", es importante conocer el "software" que se tiene instalado en la empresa y gestionar las licencias de estos para evitar infracciones legales por "software" no licenciado; esta acción ayuda a disminuir el porcentaje de probabilidad de ataques informáticos, robo y/o pérdida de información.

3. Gestión del rendimiento

El activo más importante de la infraestructura de tecnologías de la información de toda organización es la red y en gran medida dependen de internet y sus aplicaciones. Es muy importante monitorear y mejorar el rendimiento de la red para que los usuarios finales no se vean afectados por los inconvenientes que haya en esta, y mantener en óptimo funcionamiento los sistemas, garantizando también que se mantengan los acuerdos de nivel de servicio (SLA) y que se presten de forma oportuna soluciones empresariales críticas.

Las redes están expuestas a muchos errores que afectan su rendimiento, es necesario entonces supervisar de forma proactiva para detectar problemas y evitar contratiempos, garantizando así un buen funcionamiento de las aplicaciones críticas. El monitoreo proactivo involucra diagnosticar y solucionar problemas de red antes de que sean notorios para el usuario final y eliminar las amenazas.

A continuación se exponen algunos aspectos en la gestión del rendimiento.

- **Acuerdo de nivel de servicio**. Es un contrato pactado entre el proveedor de servicios y los clientes internos o externos donde se mencionan los servicios adquiridos y/o prestados por el proveedor, además define los estándares que el proveedor va a implementar en sus servicios.
- **Gestión de la seguridad**. La seguridad en los elementos "hardware" o físicos existentes y en los elementos "software" existentes en la red, son dos puntos clave que se deben tratar o emplear, debido a que el mundo está repleto de sistemas, y cada día se implementan muchos más, dejando a la sociedad más expuesta a ataques, pérdidas de información, violación

de sus datos financieros, suplantación de datos para fines no legales, entre infinidad de opciones de inseguridad informática.

- **Autenticación**. Es el proceso que se encarga de validar la existencia de un usuario dentro de un sistema, se puede llevar a cabo mediante la implementación de usuario y contraseña; este usuario puede ser el número de documento del usuario, "mail, "nickname" (o nombre de usuario).

  Otro mecanismo de autenticación puede ser biométrico, por huella dactilar, lector del iris, detección del rostro entre otros, este tipo de autenticación está siendo utilizado por los grandes fabricantes de dispositivos móviles, quienes a menudo se preocupan por la seguridad de los sistemas y también por la velocidad de respuesta de estos mecanismos.
- **Autorización**. Es el proceso que se lleva a cabo después de la autenticación en un sistema informático, la autorización es la encargada de permitir o prohibir el acceso de los usuarios a diferentes módulos.

En la gestión de la seguridad, de acuerdo con Alonso et al. (2014), se deben tener en cuenta dos categorías: tipos de ataques y tipos de defensas.

Al igual que en el cuerpo humano, los sistemas sufren ataques (enfermedades) y el sistema (cuerpo) debe estar listo ante uno o muchos, es lógico mencionar que no se puede evitar dicho ataque al 100% mediante medidas (medicamentos) pero sí sufrir el menor porcentaje de daño posible o lograr un punto tolerable en el sistema, entre los ataques más comunes y las defensas están:

Ataques más comunes

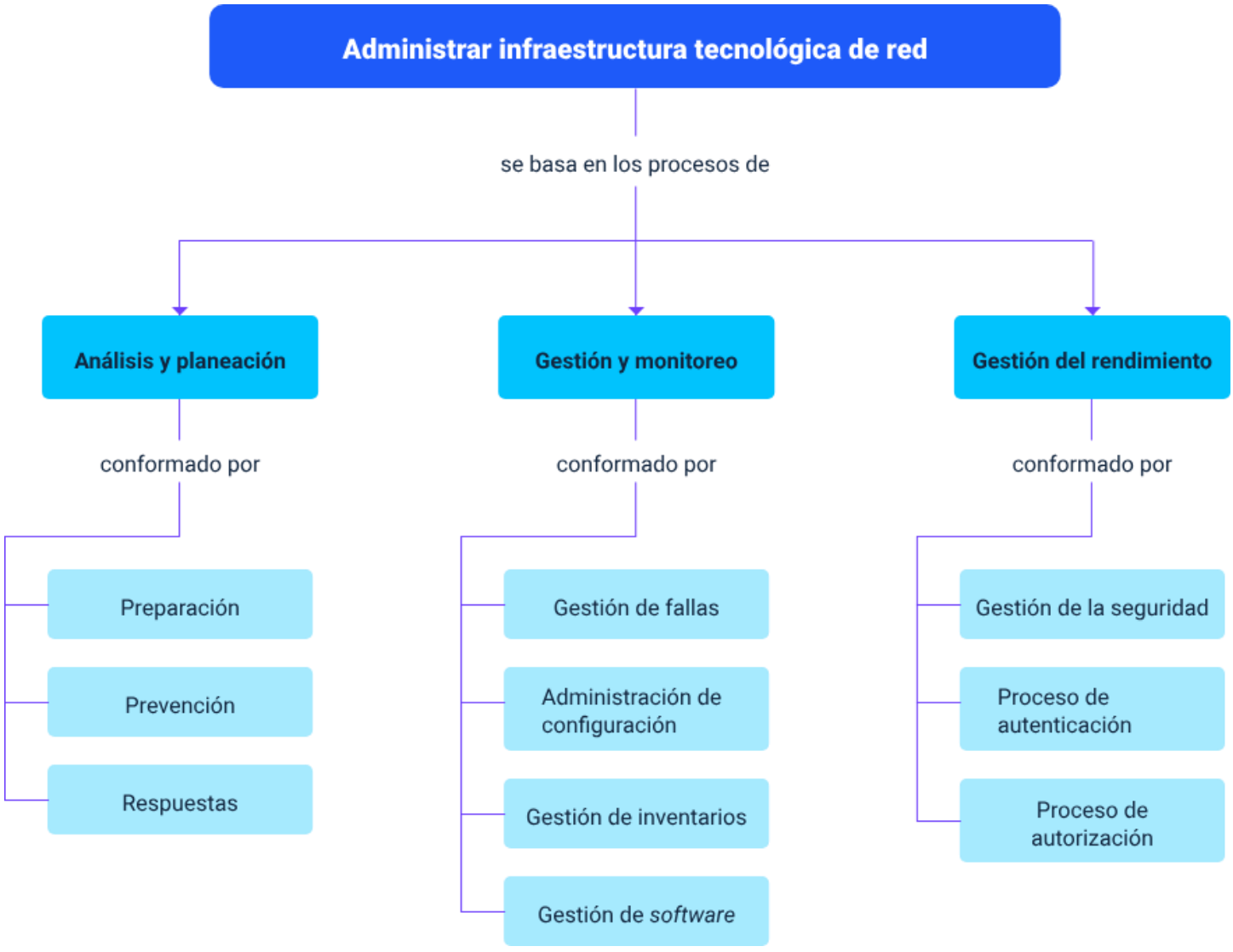
- Ataque para obtener información.
- Ataque de acceso no autorizado.
- Ataque con revelación de información.
- Ataque de denegación de servicio.

Defensas para estas amenazas

- Esquema de seguridad de sistemas operativos.
- Identificación o autenticación seguras.
- Cortafuegos (“firewalls”).
- Criptografía.
- Antivirus.
- Análisis de vulnerabilidades.
- Sistema de detección de intrusos.
- Estándares para sistemas de gestión de seguridad.

Síntesis

La administración de la infraestructura tecnológica requiere de procesos de planificación, implementación de sistemas de gestión y monitoreo en la red. En el siguiente esquema se presentan lo desarrollado en el componente.



Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
1.1.2 Análisis de Riesgos	Cisco. (2020). CCNA: Switching, Routing, and Wireless Essentials. Cisco Networking Academy.	Sitio web	https://www.netacad.com/courses/networking/ccna-switching-routing-wireless-essentials
2. Gestión y monitoreo	SJteam. (2020). Monitorea tu red sin ser experto en seguridad informática.	Video	https://www.youtube.com/watch?v=Oseq3wh2J4c&ab_channel=SJteam
3. Gestión del rendimiento	Díaz, G., Alzórriz, I., Sancristóbal, E., y Alonso M. (2014). Procesos y herramientas para la seguridad de redes. UNED	Libro	https://books.google.com.co/books?hl=en&lr=&id=dG4lAwAAQBAJ&oi=fnd&pg=PP1&dq=gesti%C3%B3n+de+la+seguridad+en+redes&ots=N7ZStUK8Eb&sig=cAvWdpzsHjtY4Zvs3VQidyQjkJE&redir_esc=y#v=onepage&q=gesti%C3%B3n%20de%20la%20seguridad%20en%20redes&f=false

Glosario

Biométrico: sistema que utiliza rasgos humanos únicos como medio de seguridad.

“Bug”: propiedad no deseada de un sistema.

DevOps: metodología de desarrollo de “software” que integra las capas de desarrollo, pruebas, implementación, calidad y gestión.

Referencias bibliográficas

Cisco. (2005). Política de seguridad de la red: informe oficial de mejores prácticas. https://www.cisco.com/c/es_mx/support/docs/availability/high-availability/13601-secpol.html

Díaz, G., Alzórriz, I., Sancristóbal, E., y Alonso M. (2014). Procesos y herramientas para la seguridad de redes. UNED.

Google Cloud. (2020). Medición de DevOps: notificación proactiva de fallas. https://cloud.google.com/solutions/devops/devops-measurement-proactive-failure-notification/?hl=es

Hurtado, C., L., Villarreal-López, E., y Villarreal-López, L. (2016). Detección y diagnóstico de fallas mediante técnicas de inteligencia artificial, un estado del arte. DYNA, 83(199). https://www.redalyc.org/journal/496/49648868002/html/

Créditos

Nombre	Cargo	Centro de Formación y Regional
Claudia Patricia Aristizábal	Responsable del Ecosistema	Dirección General
Rafael Neftalí Lizcano Reyes	Responsable de Línea de Producción	Centro Industrial del Diseño y la Manufactura - Regional Santander
Jorge Eliécer Loaiza Muñoz	Instructor	Centros de Servicios y Gestión Empresarial - Regional Antioquia
Carlos Mauricio Tovar Artunduaga	Instructor	Centros de Servicios y Gestión Empresarial - Regional Antioquia
Claudia López Arboleda	Experto Temático	Centro de Teleinformática y Producción Industrial - Regional Cauca
Deivis Eduard Ramírez Martínez	Diseñador instruccional	Centro para la Industria de la Comunicación Gráfica - Bogotá D.C.
Silvia Milena Sequeda Cárdenas	Evaluadora instruccional	Centro de gestión industrial - Regional distrito Capital
José Gabriel Ortiz Abella	Corrector de Estilo	Centro para la Industria de la Comunicación Gráfica - Regional distrito Capital
Miroslava González Hernández	Diseñadora instruccional	Centro Industrial del Diseño y la Manufactura - Regional Santander
Juan Daniel Polanco	Diseñador de Contenidos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Camilo Andres Bolaño Rey	Desarrollador Full-Stack	Centro Industrial del Diseño y la Manufactura - Regional Santander
Wilson Andrés Arenales Cáceres	Storyboard e Ilustración	Centro Industrial del Diseño y la Manufactura - Regional Santander

Nombre	Cargo	Centro de Formación y Regional
Carmen Alicia Martínez Torres	Animador y Producción audiovisual	Centro Industrial del Diseño y la Manufactura - Regional Santander
Daniela Muñoz Bedoya	Locución	Centro Industrial del Diseño y la Manufactura - Regional Santander
Emilsen Bautista	Actividad Didáctica	Centro Industrial del Diseño y la Manufactura - Regional Santander
Zuleidy María Ruiz Torres	Validador de Recursos Educativos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Luis Gabriel Urueta Alvarez	Validación de Recursos Educativos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Daniel Ricardo Mutis Gómez	Evaluador para Contenidos Inclusivos y Accesibles	Centro Industrial del Diseño y la Manufactura - Regional Santander