IMPLEMENTACIÓN DEL ÁREA DE SEGURIDAD DEL MODELO FCAPS EN LA INFRAESTRUCTURA DE RED DE LA ALCALDÍA DE ENVIGADO

ANDRÉS FELIPE ARROYAVE ARREDONDO
Institución Universitaria de Envigado – Facultad de Ingeniería
Alcaldía de Envigado – Dirección de Informática
afelipearroyave95@gmail.com

Resumen: El Modelo FCAPS (Fault-Fallas, Configuration-Configuración, Accounting-Contabilidad, Performance-Desempeño, Security-Seguridad) de la Organización Internacional de Normalización (ISO, por sus siglas en inglés), es un modelo muy utilizado en empresas y redes de gran envergadura para una mejor gestión de dicha red. Abarca 5 principales áreas vitales para un correcto funcionamiento de dicha red: La Gestión de Fallas, la Gestión de la Configuración, la Gestión de la Contabilidad, la Gestión del Desempeño y la Gestión de la Seguridad. La ISO proporciona para cada área una descripción muy detallada de qué hacer en cada una para lograr una correcta Gestión de Redes.

Palabras claves: *FCAPS, ISO, Fallas, Configuración, Contabilidad, Desempeño, Seguridad, Redes, Gestión.*

Abstract: The FCAPS model (Fault, Configuration, Accounting, Performance, Security) of the International Organization for Standardization (ISO, for its acronym in English), is a useful model for companies and networks large for better management of the network. It covers five main areas vital to the proper functioning of the network: The Fault Management, Configuration Management, Accounting Management, Performance Management and Security Management. The ISO provides for each area a very detailed description of what to do in each to ensure efficient network management.

Key words: *FCAPS, ISO, Fault, Configuration, Accounting, Performance, Security, .Network, Management.*

1. INTRODUCCIÓN

El modelo de FCAPS implementado por la ISO y recomendado por la ITU, es un sistema de gestión de redes muy utilizado actualmente en redes de gran envergadura, desde redes de mypimes que constan de pocos elementos de red, hasta redes de multinacionales con sedes en varias ciudades del mundo.

FCAPS abarca 5 grandes áreas, que al ser incluidas en éste modelo, son vitales para el correcto funcionamiento de las redes: Fallas, Configuración, Contabilidad, Desempeño y Seguridad.

Cada área se enfoca en actividades referentes a sus funciones, pero no trabajan por separado. Las 5 áreas deben trabajar juntas para poder logran una excelente gestión de la red

2. MODELO FCAPS

El Modelo FCAPS es el Modelo Funcional de Gestión de Redes definido por la Organización Internacional de Normalización (ISO, por sus siglas en inglés *International Standard Organization*) y recomendado por la Unión Internacional de Telecomunicaciones (ITU, por sus siglas en ingles *International Telecommunication Union*), que se divide en 5 grandes áreas en Gestión de Redes: Gestión de Fallas, Gestión de Configuración, Gestión de Contabilidad o Gestión de Desempeño y Gestión de la Seguridad.

Éste sistema define una serie de niveles que interactúan con la Base de Datos de tipo MIB. (*Barba, 1999*).

El Modelo FCAPS se divide en 5 grandes áreas de Gestión de Redes: Gestión de Fallas, Gestión de Configuración, Gestión de Contabilidad, Gestión de Desempeño y Gestión de Seguridad.

FCAPS es un acrónimo de un modelo que categoriza de los objetivos de trabajo de gestión de red.

- **F-Fallas:** En éste nivel, los problemas de red son encontrados y corregidos.

Los posibles futuros problemas si identifican y se toman medidas para evitar que ocurran o que se repitan. De esta manera, la red se mantiene operando y el tiempo de inactividad se minimiza.

- **C-Configuración:** En éste nivel, el funcionamiento en red es monitoreado y controlado. El hardware y la programación e cambios, incluyendo la anexión de equipos y programas nuevos, la modificación de los sistemas existentes y la eliminación de los equipos obsoletos, están coordinados. Hace parte de este nivel, el inventario de los equipos y programas, que debe mantenerse actualizado periódicamente.
- **A-Contabilidad:** El nivel A, que recibe también el nombre de 'Asignación', se dedica a la distribución de los recursos de manera óptima y equitativa entre los usuarios de red. Esto hace que el uso más eficaz de los sistemas disponibles, minimizando los costos de la operación. También este nivel es responsable de asegurar que los usuarios se facturan correctamente.
- **P-Desempeño:** Éste involucrado en la gestión del rendimiento global de la red. El rendimiento se maximiza, los cuellos de botella se evitan, y se identifican los problemas potenciales. Una parte vital del esfuerzo es la identificación de las mejoras que se deben realizar para el incremento de la integridad de la red.
- **S-Seguridad:** En éste nivel, la red está protegida contra los piratas informáticos, los usuarios sin autorización de acceso, y el detrimento físico y electrónico. La Confidencialidad de la información del usuario se debe mantener, sea justificado o necesariamente. Los sistemas de seguridad también permiten a los gestores de la red controlar lo que cada usuario autorizado puede y no puede hacer con su sistema. (*Harrell*).

2.1 Organización Internacional de Normalización:

ISO (Organización Internacional de Normalización) es el mayor desarrollador mundial de las Normas Internacionales voluntarias. Las Normas Internacionales dan el estado de las especificaciones del arte de productos, servicios y buenas prácticas, ayudando a hacer que la industria sea más eficiente y eficaz. Desarrollado a través de un consenso global, que ayudan a eliminar las barreras al comercio internacional.[1]

2.1.1 Funciones de la ISO: ISO desarrolla normas internacionales. Fue fundada en Londres en 1947, y desde entonces ha publicado más de 19.500 normas internacionales que abarcan casi todos los aspectos de la tecnología y los negocios. De la seguridad de los alimentos a los computadores, y a la agricultura a la salud.[2]

2.1.2. Miembros: La ISO es una red de organismos nacionales de normalización. Estos organismos de normalización nacionales constituyen la membrecía ISO y representan cada país.[3]

Actualmente, el cuerpo de de membrecía está compuesto por 113 países, entre ellos Colombia cuya organización de normalización nacional es el ICONTEC (*Instituto Colombiano de Normas Técnicas y Certificación*), hay 49 países correspondientes con la organización y 7 países subscritos a ella.[4]

2.2 Unión Internacional de Telecomunicaciones:

La ITU es el organismo especializado de la Organización de las Naciones Unidas (ONU) para las Tecnologías de la Información y la Comunicación (TIC). Ésta organización atribuye el espectro radioeléctrico y las orbitas de satélite a nivel mundial, igualmente elabora normas técnicas que garantiza la interconexión de las redes y las tecnologías, y es notable su esfuerzo para mejorar el acceso a las TICs de las comunidades menos favorecidas a nivel mundial.

La ITU se encuentra comprometida en conectar a toda la población mundial, sin importar su ubicación geográfica ni de los medios con que

[1] About ISO. What is ISO
[2] About ISO. What we do
[3] About ISO. Who we are
[4] About ISO. ISO Members.

cuente. Por medio de su labor, protege y apoya el derecho fundamental de todas las personas a comunicar.[5].

2.2.1 Miembros: La ITU es una organización basada en la unión público-privada desde su creación, la ITU cuenta actualmente con 193 países miembros y más de 700 entes del sector privado e igualmente instituciones académicas. Con su sede principal en la Ciudad de Ginebra, Suiza, cuenta con 12 oficinas regionales y de zona alrededor del mundo.

Todos los miembros de la ITU representan una sección transversal del sector mundial de las TIC, pasando por los mayores fabricantes, los operadores a nivel mundial, hasta los pequeños actores innovadores que cuenta con tecnologías emergentes, junto con las principales instituciones académicas.[6]

3. GESTIÓN DE FALLAS

La Gestión de Fallas se encarga de la supervisión de la red para asegurarse de que todo se encuentra funcionando en correcto estado y reacciona cuando este no es el caso. La eficaz Gestión de fallas es crítica para asegurar que los usuarios no experimenten la interrupción del servicio, y cuando esto sucede, la interrupción afecte al mínimo a los usuarios.

La funcionalidad de la gestión de fallos incluye más no se limita a lo siguiente:

- Supervisión de la red, incluida la gestión de alarma básica, así como las más avanzadas funciones de procesamiento de alarmas.
- Diagnostico de fallos, análisis de causa raíz y solución de problemas.
- Mantener registro de alarmas.
- Gestión proactiva de fallos.

3.1 Descripción General de la Supervisión de la Red:

La Supervisión de la red incluye funciones que permiten a una organización de proveedores de la red ver si la red está funcionando como se esperaba, para realizar un seguimiento de su estado actual, y para visualizar el estado. Esta funcionalidad es primordial para ser capaz de reconocer y reaccionar a las condiciones de fallo en la red a medida que ocurren.

3.2 Diagnóstico de Fallas y Solución de Problemas:

La Gestión de alarmas es un aspecto significativo de la gestión de fallos, tan significativo, de hecho, que los dos términos se usan como sinónimos. Sin embargo, hay más en la gestión de fallos que en la gestión de alarmas. Otro aspecto de interés es el diagnóstico y la solución de problemas.

El Diagnóstico de la red no es conceptualmente muy diferente de diagnóstico médico. La diferencia radica, por supuesto, en el tipo de paciente. Para llegar a un diagnóstico médico para un conjunto de síntomas el médico puede que desee echar un vistazo a los datos de seguimiento adicionales (por ejemplo, al tomar la temperatura del paciente y la presión de la sangre) y puede llevar a cabo su propia serie de pruebas, como la prueba de los reflejos o pedirle al paciente que respire profundamente mientras se escucha con un estetoscopio.

Cuando se produce un fallo en la red, la capacidad de diagnosticar el problema, es decir, para identificar rápidamente cuál fue la causa, es la clave para minimizar su impacto en los usuarios. El diagnóstico adecuado a continuación, es la base para la selección de la acción de reparación adecuada. El proceso de análisis que conduce a un diagnóstico a menudo también se conoce como análisis de la causa raíz. Una alarma general le avisa sólo un síntoma, no la causa de ello.

3.3 Gestión proactiva de fallos:

La mayoría de la funcionalidad de gestión de fallos, tales como la gestión de alarmas, es reactiva, se trata de fallas después de que hayan ocurrido. Sin embargo, la gestión proactiva de fallos también es la adopción de medidas para evitar las condiciones de fallo antes de que ocurran. Esto incluye, por ejemplo, pruebas de varios tipos en la red para detectar el deterioro en la calidad del servicio y las condiciones de fallo inminente, antes de que ocurran. La Gestión proactiva de fallos también puede incluir el análisis de alarma que reconoce patrones de alarmas causadas por pequeños fallos que apuntan a la inminente problemas mayores.

[5] Acerca de la IUT. Visión General.
[6] Acerca de la IUT. Miembros.

4. GESTIÓN DE CONFIGURACIÓN

La segunda letra en FCAPS es la C, que corresponde a la administración de configuración. Para que la red haga lo que tiene que hacer, podría necesitar que se les diga qué es primero, configurado qué tiene que hacer. Dependiendo del tipo de equipo de red, su configuración puede ser mucho más complicada o no. Además, en una red, es posible que tenga un gran número de dispositivos, los cuales necesitan ser configurados de manera coordinada para que haya una correcta interconexión entre ellos

La Gestión de la configuración incluye funciones para realizar operaciones que entregue y modifique los valores de configuración en el equipo en la red. Esto incluye la configuración inicial de un dispositivo para que esté conectado correctamente a la red.

4.1 Configuración de recursos gestionados:

En el centro de gestión de la configuración están las actividades y operaciones que se utilizan para configurar lo que se está gestionando. En última instancia, se trata de cambiar su configuración vía consola de comandos. En algunos casos, esto implica solamente un dispositivo de aislamiento, tales como la configuración de una interfaz de un puerto. En otros casos, las operaciones de configuración que se realizan en los dispositivos son simplemente parte de una operación más grande a nivel de red que implica el cambio de la configuración de múltiples dispositivos a través de la red.

5. GESTIÓN DE CONTABILIDAD

Las organizaciones que ofrecen servicios de comunicación a través de una red, en última instancia tienen que generar ingresos para los servicios que prestan. Incluso si la organización no es un proveedor de servicios, pero, por ejemplo, un departamento interno de TI proporciona esos servicios a su propia compañía, la medición de los servicios efectivos prestados y consumidos sigue siendo necesaria. Esto es necesario para poder evaluar la relación coste/beneficio de la explotación de dichos servicios, para mantener los costos bajo control en relación con los servicios que se prestan en realidad, y para utilizar los datos en firme para las decisiones sobre la utilidad de prestar servicios en la empresa o subcontratarlos.

6. GESTIÓN DE RENDIMIENTO

6.1 Métricas de Rendimiento:

El rendimiento de las redes se caracteriza por una multitud de características de rendimiento, medido de acuerdo a las métricas. Algunos ejemplos de indicadores de desempeño son los siguientes:

6.1.1 El rendimiento, medido por un número de unidades de comunicación realizadas por unidad de tiempo. Las unidades de comunicación dependen de la capa, el tipo de red, y el servicio de red en cuestión.

6.1.2 El Retraso, medido en una unidad de tiempo. Una vez más, se puede medir diferentes tipos de retardo, en función de lo que la capa de red o servicio que usted está tratando.

6.1.3 La Calidad, es en muchos aspectos también relacionados con el rendimiento y se puede medir de manera diferente, dependiendo del servicio de red

7. GESTIÓN DE SEGURIDAD

La letra final en FCAPS, "S", cubre los aspectos de gestión relacionados con la seguridad de su red de amenazas, tales como ataques de hackers, la propagación de gusanos y virus, y los intentos de intrusiones maliciosas. Dos aspectos que se pueden diferenciar: la seguridad de la gestión, lo que garantiza que la propia administración es segura, y la gestión de la seguridad de la red.

7.1 Seguridad de la Gestión:

La Seguridad de la Gestión asegura que las mismas operaciones de gestión son seguras. Una gran parte de esto se refiere al aseguramiento y que el acceso a la gestión está restringido a usuarios no autorizados.

Por ejemplo, el acceso a las interfaces de gestión de los dispositivos de la red debe mantenerse para evitar cambios no autorizados en las configuraciones de red. Además, la red de gestión debe ser asegurada para evitar la interrupción de la gestión del tráfico.

Como regla general, las amenazas de seguridad desde el interior son más difíciles de defender comparadas con las amenazas del exterior. Sin embargo, mediante la realización de las siguientes

tareas, se puede recorrer un largo camino en la defensa contra las peores amenazas y prevenir interrupciones en el funcionamiento de su red:

- Establecer procesos y procedimientos adecuados para garantizar el funcionamiento ordenado.
- Asignar privilegios de acceso sólo a aquellos que realmente necesitan estos privilegios para su función de trabajo inmediata.
- Requerir contraseñas "seguras" que no puedan ser fácilmente vulneradas.
- Requerir que las contraseñas se cambien en intervalos regulares.
- Establecer instalaciones adecuadas para las copias de seguridad y la restauración de datos críticos de gestión.

7.2 Gestión de la Seguridad:

La Gestión de la seguridad consiste en "la gestión de la seguridad" de la propia red, en lugar de la seguridad de su gestión. Lamentablemente, las amenazas de seguridad en línea son muy comunes. En muchos casos, las amenazas a la seguridad no se dirigen tanto a la red, pero los dispositivos conectados a la red como los PC de los usuarios finales, por ejemplo, o los sistemas donde los sitios web son acogidos para las empresas. Además, la propia infraestructura de red puede estar bajo ataque. Amenazas a la seguridad comunes incluyen, pero no son en modo limitado a lo siguiente:

- Los ataques de piratas que tratan de obtener un control inadecuado de un sistema que está conectado a la red.
- Ataques de Denegación de Servicio (DoS por sus siglas en inglés *Denial of Service*) intentan sobrecargar a la red mediante la generación ilegitimo, evitando el tráfico ilegítimo. Una variante de este ataque es el de Denegación de Servicio (DDoS por sus siglas en inglés *Distributed Denial of Service*), que coordina los ataques desde diferentes fuentes, lo que hace que sea más difícil de combatir.
- Los virus y gusanos que intentan corromper y posiblemente destruir los sistemas junto con sus archivos, que están conectados a la red o que son los propios dispositivos de red. En relación a esto son los troyanos, un código malicioso que se hace pasar por un programa útil e inocente que, al abrirse por un usuario, puede causar estragos.
- El spam, también es considerado un problema de seguridad, ya que su volumen puede abrumar una red y sus servidores (*Clemm, 2007*).

CONCLUSIONES Y RECOMENDACIONES

La Gestión de Redes, con el tiempo se ha ido convirtiendo en un área en todas las empresas de vital importancia, debido al crecimiento de sus redes internas y al crecimiento de las redes externas como el internet y todos sus servicios, aumentando también la cantidad de fallas que se presente en la red, el aumento de elementos de red, lo cual conlleva a un aumento de configuraciones, aumento del tráfico de la red, el aumento del consumo de recursos y de software y hardware que quiere atentar contra dicha red.

Estos aumentos son vigilados por un modelo que integra todos estos aumentos, monitoreándolos constantemente para el bienestar de la red.

Verdaderamente, el modelo FCAPS es el soporte que pueden tener tanto las grandes empresas como las Mipymes, ya que es un formato de gestión de redes muy versátil respecto a la red que se quiera gestionar.

Es un modelo versátil, ya que la red no siempre va a estar en un estado 'estable', siempre va estar bajo algún ataque, por ella va cruzar constantemente un tráfico propenso a colisiones de paquetes, y el modelo siempre se va a adaptar a estos cambios y tratará de devolverle ese estado de estabilidad a la red.

REFERENCIAS

About ISO. What is ISO? http://www.iso.org/iso/home/about.htm

About ISO. What we do? http://www.iso.org/iso/home/about.htm

About ISO. Who we are? http://www.iso.org/iso/home/about.htm

About ISO. ISO Members. http://www.iso.org/iso/home/about/iso_members.htm

Acerca de la IUT. Visión General. http://www.itu.int/es/about/Pages/default.aspx

Acerca de la IUT. Miembros. http://www.itu.int/esabout/Pages/default.aspx

Cisco Network Management Fundamentals. A guide to understandig how networking management technology really works.CLEMM, Alexander. Ph.D. Ciscopress.com

Gestión de Red. BARBARA Martí, Antoni. Edicions UPC. Septiembre de 1999

Network Management Fundamentals. E-Guide. HARRELL, Robbie. SearchingNetworking.com. 2007

C.V.:

Andrés Felipe Arroyave Arredondo: Tecnólogo en Gestión de Redes de la Institución Universitaria de Envigado, miembro del Semillero de Investigación de Seguridad Informática. Practicante en la Dirección de Informática adscrita a la Secretaría Administrativa de la Alcaldía del Municipio de Envigado.