**INSTITUTO TECNOLOGICO DE CULIACAN**

****

***INGENIERIA EN SISTEMAS COMPUTACIONALES***

***ADMINISTRACION DE REDES***

***CASO DE ESTUDIO FCAPS***

***ALUMNOS****:*

*ROSALES CORVERA HERNAN ENRIQUE*

*MOLINA LEAL JOSE LUIS*

*BELTRAN MEDINA ARMANDO*

***DOCENTE****: LUIS ERNESTO LIZARRAGA BOLAÑOS*

*CULIACAN SINALOA, 19 DE JUNIO DEL 2019*

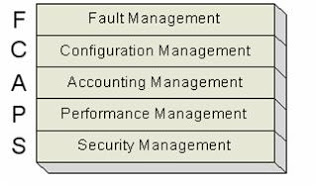
# **INTRODUCCION**

La gestión de redes de telecomunicación se define como cualquier acción para planificar, instalar, mantener, explotar y administrar redes y servicios de telecomunicación, con el objetivo de preservar la calidad del servicio y maximizar su rendimiento.

En esta pequeña investigación, se pretende analizar un caso de uso para la gestión de un switch empresarial, como es el propuesto por la ISO ( International Organization for Standardization ). Se trata del modelo FCAPS (Fault, Configuration, Accounting, Performance, Security). Este modelo define los objetivos que debe cumplir un sistema de gestión de redes, para administrar a esta de forma integral. Deberá adaptarse a las necesidades del entorno real según las necesidades del mismo.

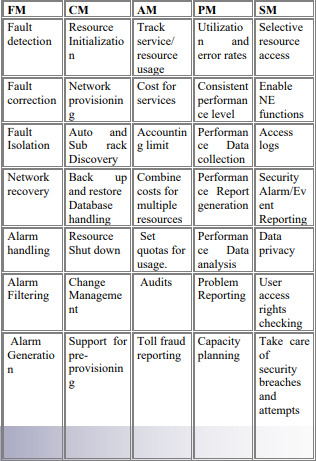
# **DEFINICION**

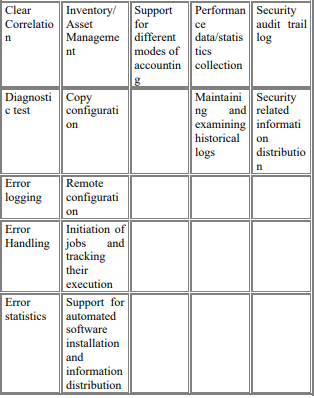
FCAPS es el modelo y framework de red de gestión de telecomunicaciones de ISO para la gestión de redes. FCAPS es un acrónimo de Fault, Configuration, Accounting, Performance, Security (Falla, Configuración, Contabilidad, Desempeño, Seguridad) que son las categorías en las cuales el modelo ISO define las tareas de gestión de redes. En algunas redes Contabilidad se reemplaza con Administración



# **FUNCIONALIDADES DE FCAPS**

La siguiente tabla enlista las funciones de administración soportadas por cada uno de los componentes.





A lo largo de este capítulo nos basaremos en el modelo comentado para describir la gestión de un Switch de una empresa, donde el flujo de la información y el uso de las redes informáticas es indispensable en el día a día de los trabajadores, teniendo una gran importancia su correcto funcionamiento diario.

**1.- GESTION DE FALLOS**

La gestión de fallos persigue la detección, aislamiento y solución de los fallos entendiendo éstos como errores persistentes. La gestión de fallos puede entenderse de forma proactiva o reactiva. La gestión proactiva de fallos busca la detección de estos antes de que ocurran. Para ello, caracteriza comportamientos tendentes a la producción de fallos y monitoriza el comportamiento del sistema de forma que detecte los fallos antes de su ocurrencia. Las herramientas para la gestión proactiva de fallos se basan, por lo tanto, en la monitorización de ciertos parámetros del sistema (p.ej. número de llamadas simultáneas, retardo extremo a extremo, pérdidas en la red). La gestión reactiva de los fallos persigue minimizar el tiempo desde que un fallo se produce hasta que se soluciona. Para ellos será necesario en primer lugar detectar la ocurrencia de un fallo (si es posible, antes que los usuarios), después aislar el fallo (determinar qué lo está causando) y finalmente solucionarlo.

**PROBLEMÁTICA A RESOLVER**

# Nuestra empresa utiliza un switch Catalyst serie 3750 para el control de las redes internas. En determinado punto de funcionamiento, el switch sufre una falla interna, una nueva actualización ha deshabilitado algunos parámetros y configuraciones internas y han provocado problemas de seguridad en los datos.

* El acceso a HTTP seguro se pierde cuando se actualiza el software Cisco IOS
* No se puede iniciar sesión a través de Secure Shell y Telnet

**CONFIGURACION DEL ACCESO A HTTP:**

Después de actualizar el software CISCO IOS® en switches Cisco Catalyst de la serie 3750, puede perder el acceso seguro al dispositivo. Si desactiva y vuelve a habilitar el acceso, no se restablece el acceso. Como medida de Correcion, el encargado de redes de la empresa ha puesto en aislamiento la información y ha guardado una copia de restauración antes de efectuar cualquier cambio en la configuración, esto como medida preventiva para cualquier situación anormal que pueda presentarse en la configuración del switch.

Para corregir el problema se llevan a cabo las siguientes funciones de configuración:

* Desactive el servidor HTTP seguro.
* **no ip http secure-server**
* Elimine la configuración de Trustpoint CA o Trustpoint PKI.
* **no crypto ca trustpoint *name***

or

* **no crypto pki trustpoint *name***
* Siga los pasos mencionados en las directrices de configuración de SSL para volver a configurar el servidor HTTP seguro.

**NO SE PUEDE INICIAR SESIÓN ATRAVEZ DEL SECURE SHELL Y TELNET**

Para corregir el segundo problema se llevan a cabo las siguientes funciones de configuración:

Los intentos de inicio de sesión fallan al intentar conectarse a un switch 3750 a través de una sesión de Telnet o de Secure Shell. Ambas conexiones solicitan una contraseña, pero no permiten iniciar sesión. Puede conectarse al switch a través de HyperTerminal HTTP con ese nombre de usuario y esa contraseña.

Para obtener acceso al switch a través de SSH o Telnet, utilice esta configuración:

* 3750\_Switch(config)#line vty 0 4
* 3750\_Switch(config-line)#no password <removed>
* 3750\_Switch(config-line)#login local
* 3750\_Switch(config-line)#transport input ssh
* 3750\_Switch(config)#line vty 5 15
* 3750\_Switch(config-line)#no password <removed>
* 3750\_Switch(config-line)#login local
* 3750\_Switch(config-line)#transport input ssh
* Inicie sesión con este nombre de usuario y contraseña:
* username swadmin password 0 <removed>

Una vez resueltas las problemáticas, el administrador de red deberá volver a poner en funcionamiento la red interna de la empresa, a su vez, deberá elaborar un log de información, en donde deberá relacionar las fallas presentadas asi como la implementación de la solución. Esto con el fin de ser capaz de prevenir y resolver futuras fallas en la red.