UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

AUTOMATIZACIÓN PARA LA OBTENCIÓN E INTERPRETACIÓN DE INFORMACIÓN EN UNA RED DE DATOS

INFORME DE TRABAJO PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN TELECOMUNICACIONES

P R E S E N T A:

GUADALUPE HERNÁNDEZ CABRERA

DIRECTOR:

ING. JAVIER ORTIZ VILLASEÑOR

2015

ÍNDICE

AGRADECIMIENTOS

Mis agradecimientos:

A la Universidad Nacional Autónoma de México:

Que me ha proveído de conocimientos desde mi formación de preparatoria que hoy me permiten integrarme satisfactoriamente a la vida laboral.

A mis padres Juan de la Cruz y Luis Marcela:

Por su gran esfuerzo y enseñanza tanto en el ámbito emocional, económico y sentimental, gracias a su apoyo y esfuerzo hoy me permito contar con una carrera.

A mis hermanos Marcela y Juan Luis:

Por ser mis compañeros de aventuras, caminos y explicaciones.

Al Ing. Javier Ortiz:

Por su profundo intereses en transmitir y generar conocimiento en su entorno.

A mis maestros:

Que se esforzaban diariamente en preparar un tema nuevo que transmitir, con el fin de dar mejores ciudadanos a este país.

A mis amigos:

Por su apoyo, solidaridad y comprensión en todos los momentos.

RESUMEN

Mi nombre es Guadalupe Hernández Cabrera y desde el 17 de septiembre de 2013 presto mis servicios profesionales en la empresa Consorcio Red Uno S.A. de C.V., laborando en el área de Gestión de Fallas Corporativo que pertenece a la gerencia de Gestión de Fallas Acceso y a la Subdirección de Operación de Red de Datos, desempeñando el cargo de Ingeniero de Red Staff. Dentro de las actividades que se realizan día a día está el monitoreo de la red, la atención de fallas tanto de medio de transmisión, software, hardware o configuración, así como encontrar el motivo o la causa raíz que las provocan, para el desarrollo de estas actividades se tiene el apoyo de áreas que acuden directamente a sitio y realizan una revisión física, a los cuales remotamente se orienta para localizar las fallas mediante el acceso e información que se logra obtener en los equipos o las herramientas de monitoreo que se tienen en el área.

En cuanto a fallas de hardware y software, una vez realizada una revisión previa y teniendo un diagnóstico, se corrobora con el proveedor tecnológico del equipo el diagnóstico al cual se ha llegado y se puede determinar si se trató únicamente de falla de software, la cual no necesita un remplazo de la pieza físicamente, o sí se trata de una falla de hardware la cual necesita ser atendida remplazando la pieza o piezas que no funcionan correctamente.

En el caso de ser una falla de software es necesario identificar la causa y validar si es posible realizar la instalación de complementos o programas, dependiendo de las versiones de Sistema operativo con la finalidad de reparar esos errores de software y evitar fallas futuras; en caso de no tener una solución y ser un error del equipo identificado, contar con un registro en la base de datos identificando el motivo de la falla y si se tiene algún procedimiento que la repare, con la finalidad de que en caso de ser reincidente ya se tiene identificado y se sabe cómo actuar. Para lo cual se tiene el apoyo del proveedor tecnológico del equipo y con un área interna más especializada llamada Soporte Técnico Reactivo, en conjunto se revisa a detalle la información que se recabó, los eventos que se registraron, se simulan las condiciones en que se presentó la falla en software de simulación, en equipos de laboratorio o en ventanas de mantenimiento, las cuales se notifican al cliente con una descripción de la actividad y es así como esta área

Soporte Técnico Reactivo puede llegar a la obtención de una causa raíz del evento presentado.

Las fallas de configuración son aquellas que se presentan cuando algún parámetro de la configuración que se ha introducido dentro de los dispositivos de red no se ha realizado correctamente según los estándares establecidos en las normas determinadas, lo cual es necesario corregir o verificar por qué el parámetro no está funcionando correctamente, así como las fallas de ruteo, es decir encontrar el motivo del por qué un paquete no está llegando a su destino y una vez localizado ser reparado.

Para realizar estas actividades se hace uso de herramientas de software desarrolladas por proveedores externos que son de gran ayuda para interpretar y localizar las fallas que se tienen en la operación de la red de datos; sin embargo, se desarrollan diferentes herramientas locales para poder obtener, analizar y clasificar la información que proporcionan los diferentes dispositivos de red, haciendo uso de diferentes lenguajes de programación y servidores de red.

Esta actividad forma parte de los proyectos de mejora que se implementan dentro del área para aumentar la eficiencia de las actividades internas que se desarrollan día a día, y poder manipular la información de manera fácil y rápida, ya que dentro de la red corporativa el tiempo en él que una falla es reparada forma parte de las métricas, y no debe rebasar los 120 minutos establecidos en los acuerdos de niveles de servicios.

Como parte del plan de entrenamiento ofrecido por la empresa, he recibido capacitación en los siguientes rubros:

- Configuración de *router*s marca Cisco de diferentes modelos
- Configuración de *router*s marca Juniper de diferentes modelos
- Protocolos de ruteo.
- Fundamentos de ITIL

Las certificaciones reconocidas en la industria con las que cuento actualmente son:

- Fundamentos de ITIL
- Cisco Certified Network Associate Routing and Switching

OBJETIVO

Describir la operación e interacción de los lenguajes de programación con los diferentes dispositivos y protocolos que forman parte de una red de Proveedor de Servicios de Internet, para desarrollar herramientas de automatización que permitan:

- ✓ Agilizar búsquedas.
- ✓ Tratamiento, almacenamiento y organización de información.
- ✓ Obtener datos y estatus de los equipos en un momento determinado de manera automática.
- ✓ Evitar saturación de memoria dando la capacidad de obtener la información y almacenarla en diferentes localidades.
- ✓ Interpretación de datos.
- ✓ Actualización de bases de datos.
- ✓ Realizar comparaciones de los cambios de configuración realizados en determinadas fechas.
- ✓ Almacenar de manera organizada los mensajes que los diferentes dispositivos generan a partir de eventos que acontecen dentro de ellos.
- ✓ Encontrar a un cliente mediante un identificador único dentro de toda la red, relacionándolo con un determinado perfil, dispositivo y localidad en donde se encuentra configurado.

1 DESCRIPCIÓN DE LA EMPRESA

1.1 Antecedentes

En la actualidad en un mundo donde diversas tecnologías y servicios están creciendo y se están desarrollando, donde los nuevos mercados de negocios, entretenimiento y telecomunicaciones buscan satisfacer sus necesidades, demandando mejores tecnologías y nuevos servicios, las redes de datos tienen gran aplicación en las organizaciones tanto públicas como privadas, posibilitando la transmisión de información a través del intercambio de datos, permitiendo la centralización de la administración y haciendo posible que software y hardware se comparten, teniendo como consecuencia el aumento de fiabilidad y rapidez en el intercambio de información , así como la disminución de costos a las organizaciones.

La gran capacidad que hoy en día tienen los dispositivos de red para llevar a cabo una comunicación punta a punta con tanta eficiencia y rapidez, ha traído en consecuencia una configuración para la operación de los servicios más compleja , donde la obtención de datos no solo depende de una, sí no de múltiples variables que disponen de valores variantes, que entre más precisos y rápidos se obtengan, permite una mayor eficiencia y rapidez en la respuesta de los resultados que se quieren obtener e interpretar como usuario final con el objetivo de poder valorar la calidad del servicio.

Resulta poco eficiente buscar de manera visual o manual un dato que se quiere obtener o interpretar para realizar un análisis o evaluación.

El hecho de tener una herramienta de automatización para la obtención de información tiene como consecuencia incrementar la productividad dentro, y a lo largo de las organizaciones, así como mejorar la eficiencia y efectividad de la información que se desea obtener.

Es por ello que se adaptan herramientas automatizadas basadas en algún lenguaje de programación que permita realizar actividades específicas, con la finalidad de no hacer uso de un recurso humano.

Dentro de la Red perteneciente y administrada por Consorcio Red Uno, se cuenta con una compleja infraestructura, para poder operar y brindar los servicios de internet dedicado empresarial (IDE), Red Privada Virtual (RPV) e Infinitum que abarca el servicio de internet masivo a nivel residencial.

La cual es necesario administrar y gestionar mediante:

- Configuración.
- Atención y resolución de Incidentes y problemas.
- Planeación de capacidad de Red.
- Seguridad de la red.

Dentro de Configuración se encuentran las actividades de modificar la configuración que se tiene en los elementos de red, ya sea con la finalidad de incorporar un nuevo servicio, un nuevo cliente, la operación de un nuevo protocolo o funcionalidad.

Dar de alta enlaces o interconexiones nuevas, conexión o desconexión de hardware, actualización o modificación de software.

Para la atención y resolución de incidentes y problemas se encuentran las actividades de monitoreo, acceso a los equipos para obtención de información de la falla, ya sea motivos, inicio, impacto, fin, afectación, y en caso de no reconocer la causa raíz, éste pasaría a ser un problema el cual hace uso de herramientas más específicas para recaudar información antes, durante y después de la falla, basándose en servidores de respaldos, en el acceso a los equipos para obtención de información, equipos de monitoreo, analizadores de paquetes, entre otros.

Planeación de capacidad de Red, dentro de la planeación se puede definir proyectos que dependiendo del crecimiento que se tiene en la red, en cuanto a servicios, protocolos y funcionalidades operando, ayuden a operar de una manera más eficiente la red o derivado de incidentes o problemas reincidentes que necesitan para su solución definitiva modificaciones dentro de la red, se toma en cuenta dentro de este campo.

Seguridad de la red, actualmente es uno de los rubros de mayor importancia dentro de las redes de datos, podría mencionar por decir solo algunas razones la confidencialidad de datos, protección de información de atacantes maliciosos, uso no permitido o indebido de la infraestructura perteneciente a la empresa, etc.

Para poder llevar a cabo esta administración y gestión se hace uso de herramientas y aplicaciones como:

- Aprovisionadores.
- Interfaz de línea de comandos,(*command-line interface* (CLI))
- Aplicaciones para la gestión de la red. (*Network Management System*(NMS))
- Sistemas de control de accesos mediante protocolos AAA *Authentication, Authorization and Accounting (*Autenticación, Autorización y Contabilización.*)*
- Servidores de uso múltiple

Aprovisionadores, se trata de herramientas automáticas para introducir configuración dentro de los dispositivos de red.

Interfaz de línea de comandos, CLI es un método que permite a los usuarios de los dispositivo de red dar instrucciones para configurar o verificar información por medio de una línea de texto simple y una conexión vía telnet.

Aplicaciones para el manejo de la red se encuentran herramientas para almacenar y consultar la base de datos, herramientas de monitoreo.

Aplicaciones que utilicen el protocolo AAA (*Authentication*, *Authorization* and *Accounting*) corresponde a un tipo de protocolos que realizan tres funciones: Autenticación, Autorización y Contabilización.

La función Autenticación es aquella que verifica que el usuario y contraseña sean válidos para permitir el acceso al dispositivo de red.

Autorización: Una vez que se ha permitido el acceso al usuario verifica los permisos que tiene este para introducir comandos dentro del dispositivo ya sean de verificación o configuración.

Contabilización se refiere a dejar un historial de los movimientos o comandos realizados por el usuario.

Servidores de uso múltiples en donde se almacenan diferentes programas basados en protocolos y herramientas que permiten monitorear, controlar, consultar y almacenar información de los dispositivos de la red.

1.2 Descripción de la Empresa

Consorcio Red Uno es la empresa líder en el mercado mexicano de telecomunicaciones, dedicada al diseño e integración de soluciones corporativas de comunicación de voz, datos, video y a la interconexión de redes corporativas, así como a su mantenimiento.

Inició operaciones en 1991 y tiene cobertura a lo largo de la República Mexicana y el continente Americano.

Su compromiso es mejorar de modo constante, integrar nuevas tecnologías, favorecer el crecimiento de sus colaboradores y trabajar por México.

Es una empresa que se ha distinguido como una entidad socialmente responsable, congruente con sus Valores y Principios y además, por fortalecer internamente la conducta ética de sus integrantes.

Misión, Visión y valores:

1. Misión

"Ser un grupo líder en telecomunicaciones, proporcionando a nuestros clientes soluciones integrales de gran valor, innovadoras y de clase mundial, a través del desarrollo humano, y de la aplicación y administración de tecnología de punta."

2. Visión

"Consolidar el liderazgo de Consorcio Red Uno en el mercado nacional, expandiendo su penetración de servicios de telecomunicaciones en todos los mercados posibles, para ubicarnos como una de las empresas de más rápido y mejor crecimiento a nivel mundial."

3. Valores

"Los Valores de nuestra cultura corporativa son:

   a. *Trabajo*
   b. *Crecimiento*
   c. *Responsabilidad Social*
   d. *Austeridad*

Nuestros Valores apoyan nuestra Misión y sustentan tanto nuestros Principios Empresariales como nuestros Principios de Conducta.

Nuestros Valores son las cualidades que nos distinguen y nos orientan. Es necesario que nuestra labor cotidiana los tenga presentes siempre, y los lleve a la práctica."

Estructura y Organización:
La estructura y la organización se dividen en 6 aéreas:

1. Desarrollo de la red de datos.
2. Explotación de la Red.
3. Finanzas y Administración.
4. Operación Red de Datos.
5. Ingeniería de la Red.
6. Desarrollo de productos.

2 MARCO TEÓRICO

2.1 Fundamentos de las redes de datos

“Una red es un conjunto de dispositivos y sistemas finales conectados, como las computadoras y servidores, que pueden comunicarse entre sí.”(Ariganello, 2015, p.25)

Las redes transportan datos en muchos tipos de escenarios, incluyendo hogares, pequeñas y grandes empresas. En una gran empresa, puede haber una serie de lugares que necesitan comunicarse entre sí, y se puede describir esos lugares en términos de donde los trabajadores se encuentran.

La ruta que toma un mensaje desde el origen hasta el destino puede ser tan sencilla como un solo cable que conecta una computadora con otra o tan compleja como una red que literalmente abarca el mundo. Esta infraestructura de red es la plataforma que da soporte a la red. Proporciona el canal estable y confiable por el cual se producen las comunicaciones.

La infraestructura de red contiene tres categorías de componentes de red:

- Dispositivos
- Medios
- Servicios.

Los dispositivos y los medios son los elementos físicos o el hardware, de la red. Por lo general, el hardware está compuesto por los componentes visibles de la plataforma de red, como una computadora portátil, una PC, un *switch, un router*, un punto de acceso inalámbrico o el cableado que se utiliza para conectar esos dispositivos.

Los componentes de red se utilizan para proporcionar servicios y procesos, que son los programas de comunicación, denominados “software”, que se ejecutan en los dispositivos

conectados en red. Un servicio de red proporciona información en respuesta a una solicitud. Los servicios incluyen muchas de las aplicaciones de red comunes que utilizan las personas a diario, como los servicios de *hosting* de correo electrónico y web *hosting*. Los procesos proporcionan la funcionalidad que direcciona y traslada mensajes a través de la red.

Los dispositivos de red con los que las personas están más familiarizadas se denominan “dispositivos finales” o “hosts”. Estos dispositivos forman la interfaz entre los usuarios y la red de comunicación subyacente.

Algunos ejemplos de dispositivos finales son:

- Computadoras (estaciones de trabajo, computadoras portátiles, servidores de archivos, servidores web)
- Impresoras de red
- Teléfonos VoIP
- Terminales de TelePresencia
- Cámaras de seguridad
- Dispositivos portátiles móviles (como *smartphones*, Tablet, PC, PDA y lectores inalámbricos de tarjetas de débito y crédito, y escáneres de códigos de barras)

Un dispositivo host es el origen o el destino de un mensaje transmitido a través de la red, para distinguir un host de otro, cada host en la red se identifica por una dirección. Cuando un host inicia la comunicación, utiliza la dirección del host de destino para especificar a dónde se debe enviar el mensaje.

Los dispositivos intermediarios interconectan dispositivos finales. Estos dispositivos proporcionan conectividad y aseguraran que los datos fluyan a través de la red.

Los siguientes son ejemplos de dispositivos de red intermediarios:

- Acceso a la red (*switches* y puntos de acceso inalámbrico)

- *Internetworking (routers)*
- Seguridad (*firewalls*)

La administración de datos, así como fluye en la red, es también una función de los dispositivos intermediarios. Estos dispositivos utilizan la dirección host de destino, conjuntamente con información sobre las interconexiones de la red para determinar la ruta que deben tomar los mensajes a través de la red.

Los procesos que se ejecutan en los dispositivos de red intermediarios realizan las siguientes funciones:

- Volver a generar y transmitir las señales de datos.
- Conservar información acerca de las rutas que existen a través de la red y de *internetwork.*
- Notificar a otros dispositivos los errores y las fallas de comunicación.
- Dirigir los datos a lo largo de rutas alternativas cuando hay una falla en el enlace.
- Clasificar y dirigir los mensajes según las prioridades de calidad de servicio (*QoS, Quality of Service).*
- Permitir o denegar el flujo de datos de acuerdo con la configuración de seguridad.

La comunicación a través de una red es transportada por un medio. El medio proporciona el canal por el cual viaja el mensaje desde el origen hasta el destino.

Las redes en la actualidad utilizan principalmente tres tipos de medios para interconectar los dispositivos y proporcionar la ruta por la cual pueden transmitirse los datos:

- Hilos metálicos dentro de cables
- Fibras de vidrio o plástico (cable de fibra óptica)
- Transmisión inalámbrica

La codificación de la señal que se debe realizar para que se transmita el mensaje es diferente para cada tipo de medio. En los hilos metálicos, los datos se codifican dentro de impulsos eléctricos que coinciden con patrones específicos. Las transmisiones por fibra óptica dependen de pulsos de luz, dentro de intervalos de luz visible o infrarroja. En las transmisiones inalámbricas, los patrones de ondas electromagnéticas muestran los distintos valores de bits.

Los diferentes tipos de medios de red tienen diferentes características y beneficios. No todos los medios de red tienen las mismas características ni son adecuados para el mismo fin. Los criterios para elegir medios de red son los siguientes:

- La distancia por la que los medios pueden transportar una señal correctamente
- El entorno en el que se instalarán los medios
- La cantidad de datos y la velocidad a la que se deben transmitir
- El costo del medio y de la instalación

2.2 Gestión de Redes de Datos

Hoy en día los servicios de Tecnologías de la Información (TI) se han convertido en verdaderos artículos de uso cotidiano y son esenciales para alcanzar los resultados del negocio.

El negocio espera que los servicios de TI estén ahí cuando los necesitan, desempeñando las tareas que se espera que desempeñen.

Los mismos principios de gestión de servicios encontrados en las organizaciones tradicionales de servicios, ahora aplican a TI. Toda organización de TI debe actuar como un proveedor de servicios, usando los principios de gestión de servicios para garantizar que entreguen los resultados requeridos por el cliente.

Gestión de Servicios de TI:

- Está compuesta de funciones y procesos para gestionar los servicios a lo largo de un ciclo de vida

- Se enfoca en la estrategia, diseño, transición, operación y mejoramiento continuo

- Posiciona a la organización como un agente de cambio para facilitar la transformación del negocio.

“Conforme los proveedores de servicios de TI incrementan y maduran sus capacidades de gestión de servicios, son capaces de entregar niveles más altos de Utilidad y Garantía sin un aumento proporcional de recursos, concretamente costos y personal.” (Pink Elephant,2013,p.31)

Partes interesadas en la Gestión de Servicios:

- Clientes: aquellos que compran bienes o servicios; persona o grupos que define y aceptan los objetivos de nivel de servicio.
- Usuarios: las personas que utilizan el servicio en el día a día.
- Proveedores: terceros responsables del suministro de bienes o servicios que se requieren para ofrecer servicios de TI.

Objetivos de la Gestión de Servicios de TI:

1. Asegurar los niveles de calidad en la red, que permitan el cumplimiento de los acuerdos de niveles de servicio firmados con el cliente.

2. Incremento de calidad en los niveles operativos que permitan la competitividad en el mercado y la generación de ofertas de servicios diferenciados.

3. Desarrollo de infraestructura que permita los niveles de calidad adecuados en los tiempos convenientes para el negocio.

2.3 Protocolos para la Gestión de Redes IP

Para Ernesto Ariganello (2015)

> Los protocolos son aquellos que describen el conjunto de normas y convenciones que establecen la forma en que los dispositivos de una red llevan a cabo el intercambio de información.
>
> La siguiente tabla muestra los protocolos que operan en cada capa de los modelos de referencia OSI y TCP/IP.

OSI	TCP/IP	protocolos
Aplicación Presentación Sesión	Aplicación	Telnet, FTP, LDP, SNMP,TFTP,SMTP, NFS,HTTP,X Windows
Transporte	Transporte	TCP, UDP
Red	Internet	ICMP, BOOTP, ARP, RARP, IP
Enlace de Datos Física	Red	Ethernet,Fast- Ethernet, Token Ring, FDDI

(p.52)

2.3.1 Protocolo ICMP

“El protocolo de Mensajes de Control de Internet permite que los ruteadores envíen mensajes de error o de control hacia otros ruteadores “(Comer,1996,p.126)

Herramientas como:

- Ping(*Packet Internet Groper*) herramienta de diagnóstico para verificar el estado, velocidad y calidad de la red; probando conectividad de sitio a sitio

- Traceroute comando que utiliza el principio de funcionamiento del ping pero mostrando e identificando cada salto a lo largo de la ruta y disminuyendo el valor de TTL(Tiempo de vida del paquete (*Time To Live*)) en cada salto.

Utilizan ICMP para poder funcionar, enviando un paquete a la dirección destino específico y esperando una determinada respuesta.

2.3.2 Protocolo SNMP

SNMP (*Simple Network Management Protocol*) el Protocolo Simple de Administración de Red es un protocolo que facilita el intercambio de información de administración entre dispositivos de red, como servidores, estaciones de trabajo , *router*s, *switch*es y dispositivos de seguridad en una red IP.

SNMP es un protocolo de capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. SNMP es un componente de la suite de protocolo de Internet como se define por el IETF.

Permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.

SNMPv3 es un protocolo interoperable basado en estándares para administración de redes. La versión actual de SNMPv3 resuelve las vulnerabilidades de las versiones anteriores, incluyendo tres nuevas características de seguridad.

- Integridad del mensaje: asegura que le paquete no ha sido manipulado en su tránsito por la red.
- Autenticación: determina que el mensaje proviene de un origen valido.
- Cifrado: encripta los contenidos de un paquete para evitar que pueda ser visualizado por una fuente no autorizada.

“SNMP esta basado en administradores NMS(*Network Management Systems*), agentes que son los nodos administrados, y las MIB(*Management Information Bases*) que son las bases de información de administración. El administrador SNMP puede obtener y cambiar información del agente y cambiar variables de configuración o iniciar acciones determinadas en los dispositivos.”(Ariganello,2015,p.252)

Los agentes SNMP aceptan comandos y solicitudes de los sistemas de administración SNMP solo si estos forman parte de una comunidad SNMP(*community string*):

- RO: proporciona acceso de solo lectura
- RW: proporciona acceso de lectura-escritura.

La arquitectura de administración de la red propuesta por el protocolo SNMP se basa en tres elementos principales:

- *Los dispositivos administrados* son los elementos de red (*switch*es , *hubs* , *router*s o servidores) que contienen "objetos administrados" que pueden ser información de hardware, elementos de configuración o información estadística.
- *Los* agentes, es decir, una aplicación de administración de red que se encuentra en un periférico y que es responsable de la transmisión de datos de administración local desde el periférico en formato SNMP.
- *El sistema de administración de red (NMS)*, este es una interfaz o interprete a través del cual los administradores pueden llevar a cabo tareas de administración.

El marco de SNMP tiene tres partes:

- Un SNMP *manager* (administrador SNMP)
- Un SNMP *agent* (agente SNMP)
- Una MIB

El administrador SNMP es el sistema utilizado para controlar y supervisar las actividades de hosts (elemento de red) de la red utilizando SNMP. El sistema de gestión más común se llama un Sistema de Gestión de Red (*Network Management System* NMS).

El término NMS se puede aplicar a cada uno de los dispositivos dedicados para la gestión de la red, o las aplicaciones utilizadas en un dispositivo de este tipo. Una gran variedad de aplicaciones de gestión de red están disponibles para su uso.

Este rango de características van desde una simple aplicación de línea de comandos hasta aplicaciones graficas complejas.

El agente SNMP es el componente de software en el dispositivo gestionado que mantiene los datos para el dispositivo e informa de estos según sea necesario a los sistemas de gestión.

La Base de Información de Gestión MIB (*Management Information Base*) reside en el dispositivo de red (*router*, servidor de acceso, o *switch*).

La Base de Información de Gestión (MIB) es aquella que almacena la información virtual para la información de gestión de red, que se compone de colecciones de objetos gestionados.

El agente SNMP contiene variables MIB cuyos valores el administrador SNMP puede solicitar o cambiar a través de obtener o establecer operaciones. Un administrador puede obtener un valor a partir de un agente o almacenar un valor en ese agente. El agente recopila datos desde el MIB, el repositorio para la información sobre los parámetros del dispositivo y los datos de la red. El agente también puede responder a las peticiones del gestor para obtener o establecer datos.

La siguiente figura muestra la relación de comunicación entre el administrador (*manager*) SNMP y el agente (*agent*).

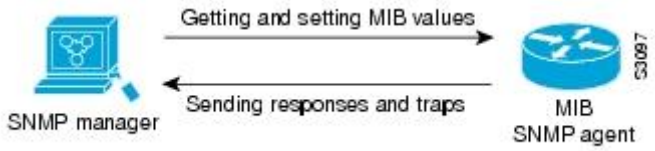


Figura1.-Interaccion Componentes SNMP

[Simple Network Management Protocol; Disponible en : http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/managed_services/8_6_1/cucm/managed_services/snmp.html]

Un administrador puede enviar las solicitudes de agentes para obtener y establecer los valores MIB. El agente puede responder a estas peticiones. Independiente de esta interacción, el agente puede enviar notificaciones no solicitadas (excepciones o informes) con el administrador para notificar al administrador de condiciones de la red.

2.3.3 Protocolo Telnet y SSH

Telnet (*Teletype Network*) es el nombre de un protocolo de red que nos permite manejar remotamente otro dispositivo como si se estuviera en él.

Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23.

“Es un protocolo de Internet estándar que permite conectar terminales y aplicaciones en Internet. El protocolo proporciona reglas básicas que permiten vincular a un cliente (sistema compuesto de una pantalla y un teclado) con un intérprete de comandos (del lado del servidor).”(Ariganello,2015,p.248)

Las especificaciones Telnet no mencionan la autenticación porque Telnet se encuentra totalmente separado de las aplicaciones que lo utilizan. Además, el protocolo Telnet no es un protocolo de transferencia de datos seguro, ya que los datos que transmite circulan en la red como texto sin codificar (de manera no cifrada).

Telnet sólo sirve para acceder en modo terminal, es decir, sin gráficos, pero es una herramienta muy útil para arreglar fallos a distancia, sin necesidad de estar físicamente en el mismo sitio que la máquina que los tenía. También se usaba para consultar datos a distancia

Las especificaciones básicas del protocolo Telnet se encuentran disponibles en la RFC 854.

SSH (*Secure Shell*) ha remplazado a telnet como practica recomendada para proveer administración remota con conexiones que soportan confidencialidad e integridad de la sesión. Provee una funcionalidad similar a una conexión telnet de salida, con la excepción de que la conexión esta cifrada y opera en el puerto 22.

2.3.4 Protocolo FTP/TFTP

FTP (*File Transfer Protocol*, 'Protocolo de Transferencia de Archivos') en informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (*Transmission Control Protocol*), basado en la arquitectura cliente-servidor.

Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

El servicio FTP es ofrecido por la capa de aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 20 y el 21. Un problema básico de FTP es que está pensado para ofrecer la máxima velocidad en la conexión, pero no la máxima seguridad, ya que todo el intercambio de información, desde el *login* y *password* del usuario en el servidor hasta la transferencia de cualquier archivo, se realiza en texto plano sin ningún tipo de cifrado, con lo que un posible atacante puede capturar este tráfico, acceder al servidor y/o apropiarse de los archivos transferidos.

TFTP (*Trivial File Transfer Protocol* "Protocolo de transferencia de archivos trivial").

Es un protocolo de transferencia muy simple semejante a una versión básica de FTP. TFTP a menudo se utiliza para transferir pequeños archivos entre ordenadores en una red.

.

Algunos detalles del TFTP:

- Utiliza UDP (en el puerto 69) como protocolo de transporte (a diferencia de FTP que utiliza los puertos 20 y 21 TCP).
- No puede listar el contenido de los directorios.
- No existen mecanismos de autenticación o cifrado.
- Se utiliza para leer o escribir archivos de un servidor remoto.

Ya que TFTP utiliza UDP, no hay una definición formal de sesión, cliente y servidor, aunque se considera servidor a aquel que abre el puerto 69 en modo UDP, y cliente a quien se conecta.

Sin embargo, cada archivo transferido vía TFTP constituye un intercambio independiente de paquetes, y existe una relación cliente-servidor informal entre la máquina que inicia la comunicación y la que responde.

- La máquina A, que inicia la comunicación, envía un paquete RRQ (*read request* /petición de lectura) o WRQ (*write request*/petición de escritura) a la máquina B, conteniendo el nombre del archivo y el modo de transferencia.
- B responde con un paquete ACK (*acknowledgement* /confirmación), que también sirve para informar a A del puerto de la máquina B al que tendrá que enviar los paquetes restantes.
- La máquina origen envía paquetes de datos numerados a la máquina destino, todos excepto el último conteniendo 512 bytes de datos. La máquina destino responde con paquetes ACK numerados para todos los paquetes de datos.
- El paquete de datos final debe contener menos de 512 bytes de datos para indicar que es el último. Si el tamaño del archivo transferido es un múltiplo exacto de 512 bytes, el origen envía un paquete final que contiene 0 bytes de datos.

2.3.5 Syslog

Los *router*s pueden registrar información en relación a los cambios de configuración, violaciones de las ACL, el estado de las interfaces y muchos otros eventos. Además pueden enviar mensajes de registro a muchos destinos diferentes. El *router* puede estar configurado para enviar mensajes de registro a uno o mas destinos:

- Consola: los mensajes se registran en la consola y pueden ser visualizados cuando se modifica o se prueba el *router* usando software de emulación de terminal. El registro de consola esta habilitado por defecto. Este tipo de registro no se almacena en el *router*.

- Líneas de terminal: las sesiones pueden ser configuradas para recibir mensajes de registro en cualquiera de las líneas de terminal. Este tipo de registro no se almacena en el *router*.

- Registro de buffer: el registro de buffer es un poco mas útil como herramienta de seguridad porque los mensajes quedan almacenados en la memoria del *router* por un cierto tiempo.

- SNMP Traps: los eventos de los *router*s, como la superación de un umbral, pueden ser procesados por el *router* y reenviados como traps SNMP a un servidor SNMP externo. Los traps SNMP son una herramienta de registro de seguridad viable, pero requieren la configuración y mantenimiento de un sistema SNMP.

- SYSLOG: Los *router*s pueden ser configurados para reenviar mensajes de registro a un servicio externo. Este servicio puede residir en uno o muchos servidores o estaciones de trabajo.

“SYSLOG es el estándar para registra eventos del sistema. SYSLOG es la herramienta de registro de mensajes mas popular, ya que proporciona capacidades de almacenamiento

de registro de largo plazo y una ubicación central para todos los mensajes del *router*. “ (Ariganello,2015,p 253.)

Las implementaciones SYSLOG contienen dos tipos de sistemas:

- Servidores SYSLOG: también conocidos como hosts de registro, estos sistemas aceptan y procesan mensajes de registro de clientes SYSLOG.
- Clientes SYSLOG: *router*s u otros tipos de dispositivos que generan y reenvían mensajes de registro a servidores SYSLOG.

2.3.6 Protocolo NTP

NTP(*Network Time Protocol)*es un protocolo diseñado para sincronizar los relojes de los ordenadores en una red.

Permite a los *router*s de la red sincronizar sus configuraciones de tiempo con un servidor NTP. Un grupo de clientes NTP puede obtener información de fecha y hora de una sola fuente y tener configuraciones mas consistentes. NTP utiliza UDP como su capa de transporte, usando el puerto 123. Está diseñado para resistir los efectos de la latencia variable.

Cuando se implementa NTP en la red, puede configurarse para que se sincronice con un reloj privado o puede sincronizarse con un servidor NTP disponible públicamente en internet.

Muchos servidores NTP en Internet no solicitan autenticación de sus pares.

2.4 Gestión de Seguridad de la Red

Para la mayoría de las organizaciones, el objetivo de seguridad se cumple cuando:

a) La información es observada por o es revelada sólo a aquellos que tienen el derecho de conocerla (confidencialidad)

b) La información está completa, es precisa y está protegida contra la modificación no autorizada (integridad)

c) La información está disponible y puede ser utilizada cuando se requiere y los sistemas que la proporcionan pueden resistir apropiadamente ataques y recuperarse de o prevenir fallas (disponibilidad)

d) Las transacciones de negocios, así como los intercambios de información entre las empresas o con los socios, pueden ser confiables (autenticidad y no rechazo)

2.4.1 Protocolos AAA

El acrónimo AAA corresponde a un tipo de protocolos que realizan tres funciones: Autenticación, Autorización y Auditoría (en inglés, *Authentication, Authorization and Accounting*).

La expresión protocolo AAA no se refiere pues a un protocolo en particular, sino a una familia de protocolos que ofrecen los tres servicios citados.

Mediante un conjunto de herramientas, procedimientos y protocolos que garantizan un tratamiento coherente de las tareas de autenticación, autorización y registro de actividad de las entidades que tienen acceso a un sistema de información.

2.4.1.1 Autenticación

Autenticación se refiere al proceso en el que se identifica la identidad de una entidad que típicamente, se realiza proporcionando evidencia de que tiene una identidad digital en específico, como un identificador y las credenciales correspondientes.

Es el proceso por el que una entidad demuestra que es quien dice ser, probando así su identidad frente a un sistema u otra entidad. En general, una entidad es un cliente, y la otra es un servidor ante el cual se requiere autenticación.

Se basa en la idea de que cada individuo tendrá una información única que le identifique o que le distinga de otros.

2.4.1.2 Autorización

La función de autorización determina si una determinada entidad está autorizada para llevar a cabo una actividad determinada, generalmente heredado de autenticación al iniciar sesión en una aplicación o servicio.

La autorización podrá ser determinada en base a una serie de restricciones.

Es el proceso de aceptar o denegar el acceso de un usuario a los recursos de la red una vez que el usuario ha sido autenticado con éxito. La cantidad de datos y servicios a los que el usuario podrá acceder dependen del nivel de autorización que tenga establecido.

2.4.1.3 Contabilidad

Contabilidad se refiere al seguimiento del consumo de recursos de red por usuarios.

Puede grabar eventos tales como la autenticación y errores de autorización, e incluyen funcionalidad de auditoría, que permite verificar la exactitud de los procedimientos llevados a cabo sobre la base de los datos contables.

La información típica que se recoge en la contabilidad es la identidad del usuario u otra entidad, la naturaleza del servicio de entrega, cuando comenzó el servicio, y cuando terminó, y si hay un estado que reportar.

Es el proceso de rastrear la actividad del usuario mientras accede a los recursos de la red, incluso la cantidad de tiempo que permanece conectado, los servicios a los que accede así como los datos transferidos durante la sesión. Los datos registrados durante este proceso se utilizan con fines estadísticos, de planeación de capacidad, facturación, auditoría y planeación de costos.

AAA está diseñado para que el administrador de la red pueda configurar dinámicamente el tipo de autenticación y autorización que se quiera, puede ser por línea (por usuario) o por servicio.

2.4.2 Protocolo TACACS

TACACS es un protocolo de autenticación, autorización y contabilidad (AAA), desarrollado originalmente para el Departamento de Defensa de Estados Unidos para la autenticación de los dispositivos de red tales como *router*s, *switch*es y *firewalls*.

Simplifica la administración y aumenta la seguridad de la red.

Lo hace mediante la centralización de la gestión de los usuarios de la red y permite establecer políticas de acceso por usuarios y grupos, comando, ubicación, hora del día, subred o tipo de dispositivo.

El protocolo TACACS también le da un registro completo de inicio de sesión de cada usuario y qué comandos fueron utilizados. TACACS se recomienda para el cumplimiento de la mayoría de los estándares de seguridad de red para el comercio electrónico, la atención sanitaria, finanzas, y las redes gubernamentales.

2.4.3 Protocolo RADIUS

RADIUS (acrónimo en inglés de *Remote Authentication Dial-In User Service*). Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.

Su uso principal es para proveedores de servicios de Internet, aunque puede también ser utilizado en cualquier red que necesita una autenticación centralizada y / o servicio de auditoría para sus estaciones de trabajo.

El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como. Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros

2.5 Características de los desarrollos en casa, comercial y de código abierto

En la actualidad las organizaciones de Tecnologías de información que ofrecen servicios orientados a las Telecomunicaciones han adquirido la necesidad de la implementación de software con el objetivo de automatizar y aumentar la eficiencia en el desempeño de las actividades diarias como el monitoreo, obtención y almacenamiento de información, compartimiento de recursos de hardware, transferencia y acceso de información tanto confidencial como publica.

Es por eso que al tomar decisiones sobre el desarrollo de estas herramientas es necesario plantear un panorama de las recursos disponibles tanto internos, públicos y privados que permitirán un desarrollo e implementación de las mismas, cubriendo las necesidades de la organización.

Es muy común que se haga un cuestionamiento a los ingenieros de sistemas y se decida si es necesario un desarrollo en casa, comercial o de código abierto.

2.5.1 Desarrollos en casa

Estos desarrollos son denominados así debido a que para su implementación se hace uso de los recursos internos con los que cuenta la empresa, es decir disponer del personal y de las herramientas que son pertenecientes a la empresa sin necesidad de recurrir a un tercero o incorporar opciones públicas.

Para poder lograr estos desarrollos es indispensable que la organización necesita de expertos internos que comprenden a los procesos y necesidades internas de la organización.

En asuntos de seguridad estos desarrollos son los más convenientes ya que permiten tener el máximo control sobre el proceso y la información requerida para su desarrollo.

Son aplicaciones independientes que permiten modificaciones futuras que van a acorde a las necesidades que se van identificando en la operación.

2.5.2 Desarrollo Comercial

Estos desarrollos son llevados a cabo por un proveedor tecnológico externo a la empresa al cual se tienen que proporcionar las especificaciones y la información necesaria para poder llevar a cabo su elaboración.

Su principal ventaja es que cuentan con lo último en tecnología y estándares industriales a la hora de la elaboración del producto.

Obtiene las mejores prácticas de la industria, hace al distribuidor responsable por el mantenimiento a largo plazo del software.

Podría ser más caro y difícil de personalizar, aparte que podría dejar al usuario vulnerable a depender de un solo proveedor.

Limita a los usuarios para cambiar el software esto porque no se tiene acceso al código fuente del software.

Muchos proyectos grandes de desarrollo de software que han sido subcontratados a terceros han fracasado debido a la falta de entendimiento de estos acerca las funciones de la compañía.

Podría resultar caro y riesgoso, por lo tanto queda a expensas de la autorización de las aéreas directivas para liberar el presupuesto destinado a estos desarrollos , aumentando el tiempo de la elección del proveedor que podría ser un proceso tardado y no dan una solución inmediata al problema.

2.5.3 Desarrollos de Código Abierto

Estos desarrollos ofrecen al usuario un código base disponible libremente como punto de inicio, como si se *hub*iera desarrollado en casa y en la mayoría de los casos, cumpliendo estándares de programación.

El usuario puede obtenerlo gratis y libremente para probarlo, y saber si cumple con sus requerimientos, sin correr el riesgo de pagar el costo de licenciamiento de un software que podría no funcionarle.

Cuenta con el aporte de muchas organizaciones, empresas o personas que han colaborado en su desarrollo, y que han permitido llegar a versiones muy estables de la solución.

Con el código fuente en la mano, el usuario puede decidir sobre un soporte y actualización futura, si ninguna modificación es requerida, el software de código abierto puede ser implementado rápidamente tal como los software comerciales empaquetados, si se requiere el usuario ya tiene un avance significativo con un código base desarrollado, por lo tanto las empresas pueden continuar con la personalización del software a través de su propio personal o hacer uso de la experiencia de la comunidad de desarrolladores.

Las actualizaciones son proporcionadas por toda una comunidad de desarrolladores que aportan su experiencia y capacidad para ir mejorando la solución, lo cual es algo muy importante a nivel de costos a largo plazo.

3 DEFINICIÓN DEL PROBLEMA, ANÁLISIS Y METODOLOGÍA EMPLEADA

Situación actual:

En la red de UniNet se tienen algunos miles de equipos operando, los cuales cambian constantemente los estatus de sus parámetros tanto de software como de hardware, generan en promedio 339,780 mensajes de SYSLOG mensuales lo cual da un promedio de 11,326 mensajes al día.

Los mensajes de SYSLOG proveen información de los eventos que ocurren en los equipos, que son de ayuda para el análisis de encontrar la falla o el origen de un evento en el equipo.

Los trabajadores hacen sus respaldos manualmente toma tiempo realizarlos y encontrar información de intereses dentro de los mismos.

Actualmente todos los ingenieros del centro de operaciones dependen de una memoria limitada con la que cuenta el equipo para almacenar los mensajes de SYSLOG, memoria que se sobrescribe con mensajes nuevos en caso de alcanzar su máxima capacidad, lo cual no les garantiza que dentro de ese espacio en memoria se tengan almacenados los mensajes o las alarmas que requieren.

Cada ingeniero hace sus respaldos con los parámetros que consideran personalmente, por lo cual no se tiene una homologación de la información que se considera universalmente de interés.

No se tiene un registro en cual se pueda corroborar dentro de la configuración de los equipos cuales han sido los cambios realizados, ni una homologación de comandos específicos seleccionados previamente para analizar el hardware y el software.

No se tiene un punto de referencia, con el cual se pueda comparar una configuración modificada.

Necesidad:

Se requiere recopilar información específica de los diferentes dispositivos de red de una manera homogénea independientemente de la plataforma, configuración y sistema operativo con el que cuenten, por medio de la vinculación de los lenguajes de programación con los dispositivos de red a través del protocolo de Telnet emulando la interacción del humano con estos dispositivos.

Almacenar esta información de manera organizada para poder acceder a ella en un determinado momento y realizar consultas de los estatus de dispositivos con alguna finalidad, ya sea por falla, auditoria, consulta o comparación.

Realizar un programa informático que acceda a esta información desplegando únicamente la información de interés, y de una manera más eficiente.

Objetivos:

General:

Recabar información de los diferentes dispositivos de red ,tanto de software como de hardware en un momento especifico, sin hacer uso del recurso humano , almacenar esta información de manera permanente y organizada para poder realizar consultas con diferentes finalidades.

Almacenar los mensajes de SYSLOG de manera permanente, organizada e independiente de la memoria limitada con la que cuenta los dispositivos de red.

Específicos:

Crear una herramienta de software que permita recabar información de los dispositivos de red de manera automatizada, homologando la información que se desea obtener independientemente de la plataforma con la que cuente el dispositivo de red al cual se esté conectando.

Configurar la comunicación entre un servidor y los dispositivos de red mediante un protocolo estándar de la industria, que cumpla con las políticas de seguridad que se tienen en operación.

Propuesta de solución y metodología.

Dentro de la red de la empresa se cuenta con servidores disponibles, los cuales establecen una comunicación con todos los elementos de la red, debido que cuentan con un direccionamiento interno que los hace formar parte de la red interna.

Se cuenta con servidores de almacenamiento de información.

Las plataformas tecnológicas con las que se cuenta, proporcionan las características necesarias para poder desplegar en pantalla información específica mediante comandos de verificación, los cuales permiten recabar información de los dispositivos con una mayor eficiencia.

Dentro de los elementos de la red de UniNet se cuenta con servidores dedicados, el cual dedica sus recursos a atender solicitudes de los equipos del cliente.

Algunos tipos son:

- FTP/TFTP: aquellos que permiten almacenar y transferir archivos.
- SYSLOG: estándar para el envío de mensajes de registro en una red informática IP.

Por SYSLOG se conoce tanto al protocolo de red como a la aplicación o biblioteca que envía los mensajes de registro.

Este servidor permite almacenar y administrar los mensajes que generan los dispositivos de red, después de un evento ocurrido dentro del dispositivo.

Requerimientos:

- Se requiere un servidor de desarrollo con IP enrutable en la red del proveedor:

Solicitar la asignación de una IP perteneciente a la red interna para poder ser asignada al servidor.

Incorporar esta IP a la tabla de ruteo de los demás Dispositivos de red a manera que conozcan la forma de llegar al servidor y poder mandar la información solicitada.

Del dispositivo más cercano al servidor mandar una ruta mediante un protocolo de ruteo dinámico a todos los demás dispositivos, para que se incorpore a su tabla de ruteo en el caso de la red de Red Uno se realiza por medio de OSPF.

- Configuración de seguridad para acceder a los dispositivos de red:

Crear una cuenta de usuario que tenga permisos únicamente para correr comandos de verificación, es decir que no tenga permisos para realizar cambios en la configuración si no únicamente comandos de consulta de información.

Verificar que el programa que ingrese a los equipos permanezca establecida esta conexión únicamente durante el tiempo que se están ejecutando los comandos de verificación, para no consumir recursos de los dispositivos de red.

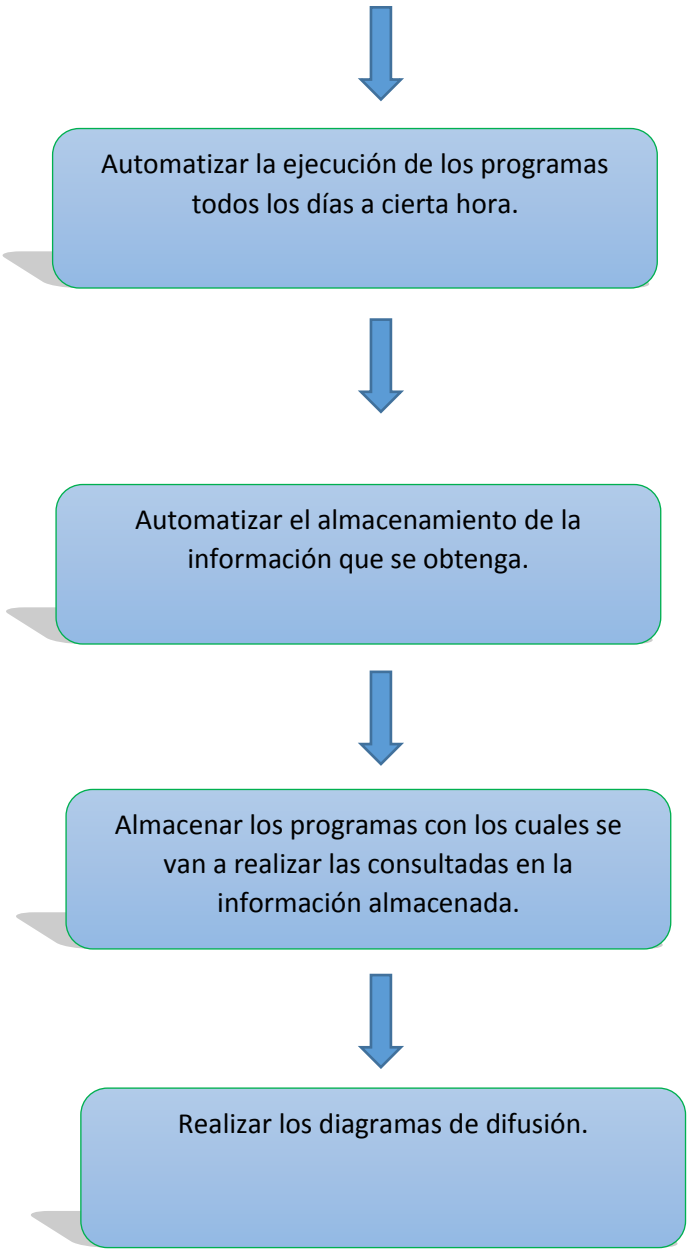
- Configurar SNMP

Configurar SNMP en los todos los dispositivos de red independientes de la plataforma con la que cuenten IOS, IOS XR o JunOs.

- Configurar SYSLOG

Configurar el envío de mensajes de SYSLOG hacia el servidor SNMP y almacenarlos en los todos los dispositivos de red independientes de la plataforma con la que cuenten IOS, IOS XR o JunOs.

3.1 Metodología


Automatizar la ejecución de los programas todos los días a cierta hora.
Automatizar el almacenamiento de la información que se obtenga.
Almacenar los programas con los cuales se van a realizar las consultadas en la información almacenada.
Realizar los diagramas de difusión.

Para el desarrollo de esta propuesta de solución se utilizaron los siguientes servidores:

- Servidor dedicado para los servicios de red: estos equipos gestionan aquellos servicios necesarios propios de la red y sin los cuales no se podrían interconectar, al menos de forma sencilla. Haciendo uso del servicio *Domain Name System* (DNS) para poder nombrar los equipos sin tener que recurrir a su dirección IP numérica.

  Es decir en este servidor se guarda una lista de relación de nombres de equipo con su formato correspondiente y su dirección IP. Ejemplo:

  ```
  router-17  10.10.2.95
  ```

- Servidor de autenticación: es el encargado de verificar que un usuario pueda conectarse a la red en cualquier punto de acceso, ya sea inalámbrico o por cable, basándose en el estándar 802.1x y puede ser un servidor de tipo RADIUS.

  Se guarda una relación de usuarios y sus contraseñas válidas para entrar en modo usuario o privilegiado.
- Los servidores de bases de datos pueden almacenar grandes cantidades de datos en una ubicación centralizada y ponerlos a disposición de los usuarios, quienes no tienen la necesidad de descargar toda la base de datos. La base de datos reside en el servidor y sólo se descarga en el equipo cliente el resultado de la solicitud.

  En este caso de este servidor Se utilizó la funcionalidad de guardar el inventario que contiene cada uno de los *router*s en la red, realizando una relación del nombre del equipo, modelo, elementos instalados y en operación con su número de serie correspondiente.
- Servidor de aplicaciones: ejecuta ciertas aplicaciones. Usualmente se trata de un dispositivo de software que proporciona servicios de aplicación a las computadoras cliente. Un servidor de aplicaciones gestiona la mayor parte (o la totalidad) de las funciones de lógica de negocio y de acceso a los datos de la aplicación. Los principales beneficios de la aplicación de la tecnología de servidores de aplicación son la centralización y la disminución de la complejidad en el desarrollo de aplicaciones.

Se utilizó la funcionalidad de programar de manera automática a cierta hora y ciertos días ejecutar los scripts para obtener, organizar y almacenar la información que nos proporcionan comandos de verificación de los equipos de red en este caso los *router*s.

Como por ejemplo estatus de usuarios, tráfico y errores dentro de las interfaces, versión de sistema operativo, log de eventos, direcciones IP asignadas en cada una de las interface y subinterfaces, parámetros físicos de los componentes, como temperatura, voltaje, potencia

- Servidores de monitorización y gestión: ayudan a simplificar las tareas de control, monitorización, búsqueda de averías, resolución de incidencias, etc. Permiten, por ejemplo, centralizar la recepción de mensajes de aviso, alarma e información que emiten los distintos elementos de red (no solo los propios servidores).

Para llevar a cabo esta propuesta de solución se hizo uso del protocolo SNMP para obtener y almacenar los mensajes de eventos que genera un dispositivo, enfocándonos en los mensajes de SYSLOG y el protocolo NTP para sincronizar los relojes de los ordenadores en una red, con la finalidad de que la detección o registro de un evento en cualquier dispositivo de la red tengan concordancia en el horario.

“En informática un script, es un archivo de órdenes, que por lo regular se almacena en un archivo de texto plano. “(Header,2010,p.272)

Los script son casi siempre interpretados, pero no todo programa interpretado es considerado un script. El uso habitual de los scripts es realizar diversas tareas como combinar componentes, interactuar con el sistema operativo o con el usuario. Por este uso es frecuente que los shells sean a la vez intérpretes de este tipo de programas.

Estos scripts son desarrollados en diferentes lenguajes de programación, dependiendo del desarrollador o de las características con las que este cuenta para poder desarrollar la tarea que se requiere, tomando en cuenta la portabilidad, las librerías con las que cuenta, etcétera.

Los scripts ofrecen a los autores dentro de una red de datos, la posibilidad de agilizar búsquedas, tratamiento, almacenamiento y organización de información, sistemas de respaldo automáticos, evitar saturación de memoria dando la capacidad de obtener la información y almacenarla en diferentes localidades, interpretación de datos de manera

gráfica, actualización de bases de datos, realizar comparaciones de los cambios de configuración realizados en determinadas fechas, poder almacenar de manera organizadas los mensajes que los diferentes dispositivos generan a partir de eventos que acontecen dentro de ellos, encontrar a un cliente mediante un identificador único dentro de toda la red, relacionándolo con un determinado perfil, dispositivo y localidad del dispositivo en donde se encuentra configurado, controlar la asignación de direccionamiento e identificadores.

Un script de shell es un programa informático diseñado para ser ejecutado por el shell de Unix, un intérprete de línea de comandos.

Está incluido en las instalaciones básicas de prácticamente todas las distribuciones de GNU/Linux.

Un lenguaje de programación sirve para automatizar y comunicar información de lo que se necesita en un lenguaje máquina de tal forma que se pueda especificar al dispositivo que datos o información es el que se requiere que se visualice y cuál será el tratamiento que se debe hacer.

Para el desarrollo de los programas descritos posteriormente se utilizaron principalmente dos lenguajes de programación:

AWK, cuyo nombre deriva de la primera letra de los apellidos de sus autores Alfred Aho, Peter Weinberger y Brian Kernighan, es un lenguaje de programación que fue diseñado con el objetivo de procesar datos basados sobre texto y una de las primeras herramientas en aparecer en Unix. Utiliza listas en un índice ordenado por cadenas clave (listas asociativas) y expresiones regulares.

Es un lenguaje ampliamente utilizado para la programación de guiones ejecutables.

AWK está diseñado principalmente para trabajar con archivos estructurados y patrones de texto. Debido a que dispone de características internas para descomponer líneas de entrada en campos y compara con patrones que se especifiquen. Debido a estas posibilidades, resulta apropiado para trabajar con archivos que contienen información estructurada en campos.

Para el desarrollo e implementación de estas herramientas, e interpretación de estos lenguajes de programación se hace sobre el sistema operativo Unix.

Unix es un sistema operativo que controla los recursos de una computadora y los asigna entre los usuarios. Permite a los usuarios correr sus programas. Controla los dispositivos de periféricos conectados a la máquina. Además es un sistema multiusuario, en el que existe la portabilidad para la implementación de distintas computadoras.

Las características que lo hacen uno de los sistemas operativos más utilizados para la implementación de servidores, son principalmente:

- Mayor eficiencia en la utilización de la memoria virtual. Lo que permite al usuario, que se pueda utilizar una serie de programas al mismo tiempo, usando sólo una pequeña localidad de la memoria física.
- Amplia colección de utilidades y comandos que están diseñados para llevar a cabo tareas específicas.
- Capacidad de encadenar diversas utilidades y comandos juntos, en un número ilimitado de configuraciones, con el fin de lograr una variedad de tareas complicadas.
- Disponible para usarse en una variedad de diferentes tipos de máquinas.
- La interfaz es la línea basada en comandos, permite mayor seguridad a comparación de una interfaz gráfica.
- Provee mecanismos de seguridad para permitir el acceso a determinados usuarios dando control mediante un usuario y una contraseña, rechazando accesos no permitidos.
- Permite la creación de grupos de usuarios con determinados permisos y accesos a recursos del sistema.
- Realiza un riguroso control de acceso al sistema de archivos. Cada uno se encuentra protegido por una secuencia de bits. Sólo se permite el acceso global al "root" o "super usuario".
- Los componentes más importantes en un servidor de Unix son la memoria y el CPU. Por ello, se puede tener un servidor con varios procesadores ejecutando los procesos.
- Es un sistema operativo multitarea es decir, el sistema se encarga de repartir el tiempo de uso de procesador de cada aplicación que esté funcionando.
- Dispone de un lenguaje de control programable llamado "Shell".
- Es de código libre, es decir que no se necesita una licencia para su uso e instalación.

- Constantes actualizaciones en paquetería que permite habilitar múltiples funcionalidades al sistema.

Debido a estas características en Consorcio Red Uno se cuenta con servidores con el sistema operativo Unix instalado.

3.1.1 Análisis de recursos disponibles

Se cuenta con protocolos que se encargan de establecer la comunicación entre un servidor y los dispositivos de red, obteniendo información específica que se encuentra almacenada en los dispositivos de red.

La implementación de este proyecto cumple con los estándares de seguridad ya que se piensa ingresar a los equipos con una autenticación de un usuario mediante un protocolo AAA y delimitar sus permisos de ejecutar comandos de verificación.

Se cuenta con servidores de almacenamiento en los cuales se tiene la capacidad y las características para poder almacenar de manera ordenada toda esta información.

Se tienen disponibles los desarrollos en casa, comercial y de código abierto.

Se va a descartar el desarrollo comercial debido a que estos desarrollos deben de contar con una previa autorización a nivel dirección para poder destinar un presupuesto y llevar a cabo una licitación para poder elegir el proveedor que lo va a desarrollar.

Se cuenta aun con desarrollos en casa y de código abierto. Se va a optar por un desarrollo en casa ya que al realizar este análisis se llega a la conclusión que en la empresa se cuenta con los recursos de hardware y software necesarios para poder desarrollar la herramienta y se cuenta con los conocimientos y la identificación de los requerimientos, alcances y especificaciones que debe tener la herramienta para entrar en operación.

Ayudándonos de programas de código abierto, ya que nos tienen exentos de licenciamiento y proporcionan las características necesarias para desarrollar el código en un lenguaje de programación que nos permite acceder a los equipos en modo terminal y almacenar la información en texto plano, para poder realizar consultas mas adelante y almacenar la información sin consumir demasiados recursos de los servidores de almacenamiento.

3.2 Diseño de la propuesta de solución

3.2.1 Diseño de la solución

Previo a la implementación de este proyecto ya se tiene un servidor configurado con el servicio SNMP.

Se requiere configurar dentro de los dispositivos de red la conectividad con el servidor SNMP donde mandaran los mensajes que se generan a partir de eventos:

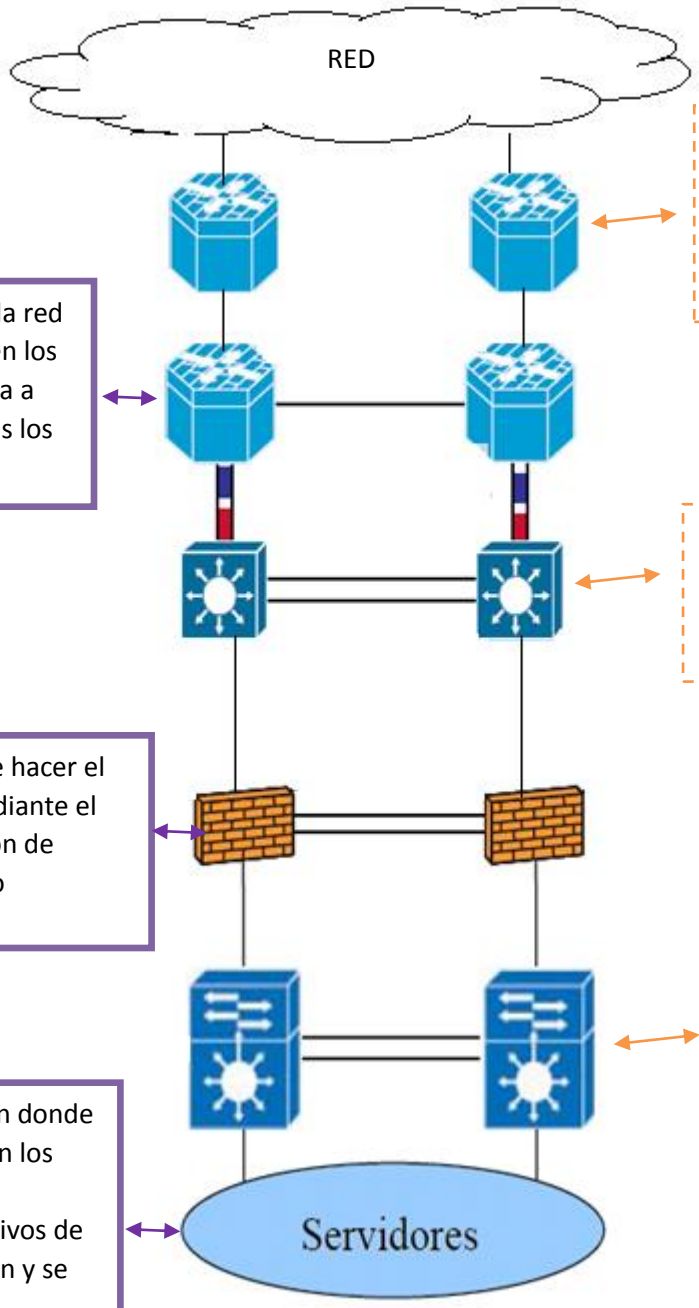
Es necesario almacenar los mensajes de SYSLOG dentro del servidor administrador SNMP y realizar un script para realizar búsquedas por equipo y un rango de días determinados:

Es necesario desarrollar un programa para conectarse vía TELNET a todos los equipos de la red de forma automática.

Ejecutar comandos de verificación de manera homogénea sin importar la plataforma y versión de sistema operativo con el que cuente el dispositivo de red.

Almacenar y organizar la información recabada.

3.2.2 Arquitectura



Dispositivo de red frontera el cual se va a encargar de distribuir por medio de un protocolo dinámico de enrutamiento la forma de acceder a los servidores y a los diferentes dispositivos de red

Router que da salida a la red LAN a la que pertenecen los servidores, este conecta a los servidores con todos los dispositivos de la red.

Switch que se encarga de distribuir el trafico entre LAN´s (en este caso solo se observa diagrama de red LAN de servidores)

Firewall, se encarga de hacer el filtrado de tráfico, mediante el bloqueo o la aceptación de ciertas direcciones IP o protocolos.

Switch que se encarga de interconectar los servidores y distribuir el tráfico al servidor que corresponde.

Servidores de Gestión en donde se almacenan y ejecutan los scripts, se realizan las solicitudes a los dispositivos de red de cierta información y se almacena lo obtenido.

3.3 Implementación

3.3.1 Configuración de SNMP

CONFIGURACIÓN DE SNMP PARA IOS

Se configuro SNMPv2 para obtener información de dispositivos de red, para realizar esta configuración de SNMP se realizó en modo de configuración global.

1 .- Se configuro el nombre de la comunidad y el nivel de acceso en esta caso solo de lectura con el comando:

```
snmp-server community nombre-de-la-comunidad ro
```

2 .- Se especifica la ubicación del dispositivo mediante el comando:

```
snmp-server location texto
```

3 .- Se especificó el contacto del sistema usando el comando:

```
snmp-server contact texto
```

4.-Se restringió el acceso de SNMP solo a los servidores SNMP que están permitidos por una lista de acceso(ACL), la lista de acceso se definió previamente y luego se hizo referencia a la lista de acceso con el comando:

```
snmp-server community nombre-de-la-comunidad lista-de-acceso
```

5.-Se especificó la dirección IP del servidor , la versión de SNMO y la contraseña, mediante el comando:

```
Snmp-server host 192.168.1.3 version 2c contraseña
```

6.-Se habilitaron los *traps* en los agentes SNMP con el comando:

```
Snmp-server enable traps
```

CONFIGURACIÓN DE SNMP PARA JUNOS

Por default en los dispositivos con sistema operativo Junos SNMP está desactivado, y se debe de incluir la configuración en el nivel de jerarquía [edit snmp]. Se debe de incluir la sentencia “community< nombre de la comunidad >” en la configuración y esto permite acceso de sólo lectura a los datos de la MIB a cualquier sistema o cliente.

Si la sentencia de configuración “clientes” no es aplicada, por defecto se permite a cualquier sistema o cliente obtener información. Por lo que se recomienda que siempre se incluya la opción “restrict” con la finalidad de limitar el acceso a la información al dispositivo vía SNMP.

Configuración propuesta:

```
[edit snmp]
user@switch# show

name "Nombre del Router";
description "Juniper Router";
location "Localización física del Router [ Piso, Fila, Gabinete]";
contact "Información del administrador [Nombre, teléfono, e-mail ]";
```

Información de contacto para el dispositivo.

```
client-list list0 {
10.10.0.0/24;
}
```

Se define una lista de clientes que podrán realizar peticiones SNMP.

```
community mi-comunidad {
```

Definir la comunidad es lo mínimo requerido en Junos.

```
 authorization read-only;
```

Es la autorización por defecto.

```
  clients {
   10.11.0.0/24 restrict;
 }
}
```

Se define la subred que no tendrá respuesta a las peticiones SNMP.

```
trap-group mi-grupo-trap {
versión v2;
```

Envía notificaciones SNMPv2 con respecto a los eventos a

```
 destination-port 155;

 categories {
  chassis;
  link;
 }

 targets {
  10.10.0.100;
 }
}
```

interfaces y el chasis.

Es posible definir un puerto específico, por defecto es el 162.

Ver tabla “SNMP Traps” para más opciones.

Se define el NMS[1] para la entrega de traps.

3.3.2 Adquisición de datos

Se pide a los administradores del servidor de almacenamiento que guarden la información recabada de manera organizada por fechas, es decir crear un directorio por cada día con el formato DDMMAA y crear un archivo con el nombre del equipo del que se reciben los mensajes.

En el programa con el que se va a establecer la comunicación se agrega mi usuario y contraseña ya que es solo ha manera de prueba y una vez exitoso se pedirá a seguridad crear el perfil con el se establecerá la conexión a todos los dispositivos.

- **Conecta:**

Este es un script para conectarte vía TELNET a los equipos de la red de forma automática.

Para poder hacer uso de este script es necesario guardar en un archivo llamado `pass` en el cual especifique mi usuario, contraseña de usuario y contraseña de usuario privilegiado con el siguiente formato:

```
usuario contraseña_de_usuario contraseña_de_usuario_privilegiado
```

Los motivos que se identificaron por los cuales se puede tener una conexión fallida son:

El usuario y la contraseña, no son validos, esto se puede deber a que el usuario no esta dado de alta y es inexistente en los sistemas de control de accesos; como método de seguridad estos sistemas de control de accesos se actualizan cada cierto tiempo con los usuarios vigentes, por lo cual otro motivo podría deberse a que el usuario no se encuentra vigente en el momento de la conexión o sus contraseñas no fueron actualizadas.

Se puede tener una conexión rechazada debido a que el dispositivo de red se encuentra inalcanzable para el servidor desde el cual se establece la comunicación debido a una falla de software o hardware que se tiene en el dispositivo de red inalcanzable.

La conexión se queda en modo de espera debido a que el dispositivo de red al que se conecto no puede acceder a los sistemas de control de accesos y no puede verificar si el usuario es válido, o a una falla de software no permite responder al equipo.

- obt_info_confreg:

Este script ejecuta una estructura de control, ciclo FOR mediante la cual recorre una lista de los tres dispositivos de cada una de las plataformas que se tiene disponible, almacenada en el archivo llamado `bb_rtrs ,` el cual contiene una relación de nombre de equipos con su dirección IP.

A los cuales se va a conectar para obtener los comandos de verificación.

Ejemplo del contenido del archivo:

```
router-4      10.6.28.9

router-42    10.14.8.189

router-15   10.18.19.21
```

- **sho versión:**

Este script es el que va a ejecutar los comandos de verificación dependiendo de la plataforma en la que se encuentre, haciendo una validación del modelo y la versión de sistema operativo con el que cuenta el dispositivo de red, y de acuerdo a esta información va a tomar una matriz de comandos los cuales va a ejecutar una vez realizada esta clasificación, ya que como mencione anteriormente los comandos de verificación varían según la plataforma en la que se encuentre.

3.3.3 Procesamiento de datos

El desarrollo de esta fase tiene como objetivo almacenar la información recopilada en un servidor de almacenamiento y desarrollar programas para hacer una clasificación de la información que se desea consultar.

Una vez conectados los dispositivos de red con el servidor administrador de SNMP, se notificó a los administradores del servidor para que se organice la información por días creando un archivo en formato zip donde contenga todos los mensajes de SYSLOG de los equipos, se organizó de la siguiente manera:

```
$ cd  /uninet/Syslogs/DDMMAA

$ ls

syslog_DDMMAA.zip
```

Para el caso del almacenamiento de los comandos de verificación se pidió nuevamente al administrador del servidor de almacenamiento masivo organizar la información en carpetas con el formato:

DDMMAA

En dicha carpeta se va a crear un archivo con el nombre del equipo en el cual se ejecutaron los comandos de verificación.

```
$ cd  /uninet/comandos/DDMMAA

$ ls

      router-4

      router-42

      router-15
```

Se realizó un script utilizando Shell y AWK para realizar la búsqueda de los mensajes de SYSLOG generados de un equipo en un día rango de días determinados.

Para la búsqueda de cierta información dentro del archivo en donde se tengan capturados los comandos de verificación se hará por medio de filtros, dicha utilidad se explicara más adelante.

3.3.4 Implementación de la comunicación de los dispositivos de red con un servidor de almacenamiento mediante el protocolo SNMP

Durante esta primera etapa se va a configurar dentro de los dispositivos de red *router*s la conectividad con el servidor SNMP donde mandaran los mensajes que se generan a partir de eventos:

1. Entrar al dispositivo de red en este caso *router* el cual se desea mande los traps(mensaje que se genera después de un evento que ocurre dentro del dispositivo de red).
2. Especificar el identificador para el host remoto, con la siguiente sintaxis:

```
Router(config)# snmp-server engineID remoteremote-ip-addr remote-engineID
```

Donde los parámetros a modificar son:

remoteremote-ip-addr: Dirección IP del administrador SNMP (servidor).

remote-engineID: Es el identificador con el que nuestro dispositivo de red *router* va a identificar al servidor SNMP.

Quedando de la siguiente manera.

```
Router(config)# snmp-server engineID 10.101.150.87 00007240603EF87T20
```

3. Especificar el nombre de usuario con el cual se va a establecer la comunicación y autenticar al servidor administrador snmp.

- **Sintaxis:**

```
Router(config)# snmp-server user username groupname [remote host [udp-port port] {v1 |v2c | v3 [encrypted] [auth {md5 | sha} auth-password]} [access access-list]
```

```
Router(config)# snmp-server user USUARIO GRUPO V3 auth md5 CONTRA
```

Donde:

USUARIO: Es el nombre del usuario existente en el servidor con el cual el *router* se va a autenticar.

GRUPO: Es el nombre del grupo al que pertenece el usuario previamente configurado en el servidor.

V3: es la versión de SNMP que se va a utilizar actualmente existen 3 versiones.

md5: Es el algoritmo que se va a utilizar para autenticación está disponible MD5 y SHA.

CONTRA: contraseña con la que se autenticara el usuario con el servidor administrador de SNMP.

4. Especificar donde se quieren enviar las notificaciones ya sean traps o información

-**Sintaxis y parámetros validos:**

```
Router(config)# snmp-serverhost host[traps | informs][version {1 | 2c | 3 [auth | noauth | priv]}]community-string [notification-type]
```

```
Router(config)# snmp-server host 10.101.150.87 traps
```

- Se especifica que al servidor con dirección IP **10.101.150.87 se envíen los traps.**

5. Se especifica el tipo de traps que se quiere se envíen al servidor administrador SNMP:

-**Sintaxis:**

```
Router(config)# snmp-server enable traps[notification-type [notification-options]]
```

En este caso se va a habilitar únicamente los traps de tipo SYSLOG que son los que se va a almacenar y manipular en el servidor.

```
Router(config)# snmp-server traps syslog
```

3.3.5 Almacenamiento y organización de información

El desarrollo de esta fase tiene como objetivo almacenar los mensajes de dentro del servidor administrador SNMP y realizar un script para realizar búsquedas por equipo y un rango de días determinados.

-**Código:**

```
#!/bin/bash


strF=$1


ls -1 ../../../uninet/logs/ | sort -b -k1.5,1.6 -k1.3,1.4 -k1.1,1.2 |
nawk -v strFind="$strF" '$1 ~ /'$2'/ , $1 ~ /'$3'/ {system("zipgrep
"strFind" ../../../uninet/logs/"$1"/syslog_"$1".zip")}'
```

-Explicación del código:

#!/bin/bash

strF=$1←Primer parámetro nombre del equipo

ls -1 ../../../uninet/Syslogs/ | ← Ruta donde se guarda el archivo syslog_DDMMAA.zip

sort -b -k1.5,1.6 -k1.3,1.4 -k1.1,1.2 | ← Se toma el rango de carpetas de fecha de inicio y fecha de fin en forma de lista

nawk -v strFind="$strF" '$1 ~ /'$2'/ , $1 ~ /'$3'/ {system("zipgrep "strFind" ../../../uninet/logs/"$1"/syslog_"$1".zip")}' ← Se busca mediante AWK en todas las carpetas generadas entre fecha inicio y fecha fin el nombre del equipo y se captura los mensajes de SYSLOG.

-**Ejecución del script:**

1. Se carga el script dentro del servidor administrador SNMP.
2. Se crea archivo:

`bash-3.00$ **touch findsyslog**` ←El nombre con el que invoques al script

3. Se dan privilegios de lectura, escritura y ejecución:

`bash-3.00$ **chmod 777 findsyslog**` ← Se dan privilegios de rwx

4. Se verifica que se creó correctamente:

`bash-3.00$ **ls -lha | grep findsyslog**` ←Revisa que se creó y los privilegios

```
-rwxrwxrwx   findsyslog
```

5. Se copia el script dentro de este archivo y se verifica:

```
$ cat findsyslog

#!/bin/bash

strF=$1

ls -1 ../../../uninet/logs/ | sort -b -k1.5,1.6 -k1.3,1.4 -k1.1,1.2 |
nawk -v strFind="$strF" '$1 ~ /'$2'/ , $1 ~ /'$3'/ {system("zipgrep
"strFind" ../../../uninet/logs/"$1"/syslog_"$1".zip")}'
```

6. Se ejecuta el script

Para ejecutar un script en servidor UNIX se necesita especificar la ruta en donde se encuentra y dar los parámetros correspondientes:

$ ./findsyslog *router*-4 111114 121114

tmp/syslog_111114.log:Nov 11 02:17:06 *router*-4 26827: Nov 11 02:17:05: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial9/1/6:30, changed state to down

tmp/syslog_111114.log:Nov 11 02:17:06 *router*-4 26828: Nov 11 02:17:06: %BGP-5-ADJCHANGE: neighbor 10.10.12.10 vpnvrf V2:VPN_0 Down Interface flap

tmp/syslog_111114.log:Nov 11 02:17:43 *router*-4 26829: Nov 11 02:17:42: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial9/1/6:30, changed state to up

tmp/syslog_111114.log:Nov 11 02:18:50 *router*-4 26830: Nov 11 02:18:48:%BGP-5-ADJCHANGE: neighbor 10.10.132.106 vpnvrf V2:VPN_0 Up

tmp/syslog_111114.log:Nov 11 02:33:06 *router*-4 26831: Nov 11 02:33:04: %BGP-5-ADJCHANGE: neighbor 10.10.147.46 vpnvrf V10:VPN_BUS_0 Down Interface flap

tmp/syslog_111114.log:Nov 11 02:33:06 *router*-4 26832: Nov 11 02:33:05: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0:10, changed state to down

tmp/syslog_111114.log:Nov 11 02:33:34 *router*-4 26833: Nov 11 02:33:33: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0:10, changed state to up

tmp/syslog_111114.log:Nov 11 02:33:44 *router*-4 26834: Nov 11 02:33:43: %BGP-5-ADJCHANGE: neighbor 10.10.1.46 vpn vrf V10:VPN_BUS_0 Up

```
tmp/syslog_111114.log:Nov 11 02:44:13 router-4 26835: Nov 11 02:44:12:
%BGP-5-ADJCHANGE: neighbor 10.10.14.46 vpn vrf V10:VPN_BUS_0 Down
Interface flap
```

3.3.6 Conectividad, obtención y almacenamiento de comandos de verificación en los dispositivos de red

Como se había mencionado anteriormente en la red de UniNet se tiene un aproximado de algunos miles de equipos operando de los cuales se necesita conocer su estatus en un determinado momento, con fines estadísticos, de respaldo, conocimiento de estatus, obtención de información en caso de una falla en la búsqueda de la causa, etc.

Para llevar a cabo esta tarea de automatización se hizo uso de múltiples scripts, los cuales voy a explicar su funcionamiento de manera individual y posteriormente su interacción entre ellos.

- **Conecta:**

Para poder hacer uso de este script es necesario guardar en un archivo llamado `pass` en el cual se especifique usuario, contraseña de usuario y contraseña de usuario privilegiado del perfil asignado por el área de seguridad con el siguiente formato:

```
usuario contraseña_de_usuario contraseña_de_usuario_privilegiado
```

Ya que el programa hará uso de este usuario para poder hacer la conexión via telnet en cada uno de los dispositivos de red.

Adicionalmente realiza la validación de los posibles errores que se pueden tener al momento de conectarse vía TELNET hacia un dispositivo, verifica que:

- Usuario y contraseñas sean válidos.
- La conexión no sea rechazada
- Verifica que la conexión no se quede en un modo de espera.
- Despliega un mensaje del motivo por el cual se tuvo una conexión fallida

Este es el código:

```
#!/usr/bin/ksh

PATH=/usr/xpg4/bin:$PATH
TMP=$DIR/tmp
OUT=$TMP/salidas
ERR=$TMP/errores

if [ ! -f $HOME/.pass ]; then
     echo "Error - No existe tu archivo de password" >> $ERR/$2
exit
fi

tail -f $TMP/$2 | telnet $1 > $OUT/$2 &

tID=`ps -fe | grep "tail -f $TMP/$2$" | grep -v grep | grep -v "   1 "
| awk '{print $2}'``
TID=`ps -fe | grep " $tID " | grep tail | grep -v grep | awk '{print
$3}'``

echo "$tID  $TID" >> $ERR/$2.pid

sleep 1

if [ "`grep Unable $ERR/$2`" ]; then
     kill -9 $tID
     echo "Error - Conection refused" >> $ERR/$2
     exit
fi
```

```
if [ "`grep Unknown $ERR/$2`" ]; then
     kill -9 $tID
     echo "Error - Unknown host" >> $ERR/$2
     exit
fi

trying=`wc -l $OUT/$2 | awk '{print $1}'`

i=0
while [ $trying -lt 2 ]
do
    let i=i+1
    if [ $i -eq 80 ]; then
       kill -9 $tID $TID
echo "Error - Conection timeout" >> $ERR/$2
exit
    fi
    trying=`wc -l $OUT/$2 | awk '{print $1}'`
done

user=`awk '{print $1}' $HOME/.pass`
pass=`awk '{print $2}' $HOME/.pass`
enap=`awk '{print $3}' $HOME/.pass`

while [ ! "$last" ]
do
        last=`grep -e Username -e Password -e User: -ie Local -e ">" -e
Login: $OUT/$2 | awk '{print $1}'`
done
```

```
last=`echo $last | strings -n1`

case $last in
      Login: )
           echo "$user" >> $TMP/$2

           while [ ! "$PASS" ]
           do
                   PASS=`grep Password $OUT/$2 | awk '{print $1}'`
                AUTFAIL=`grep -ie Authentication -ie invalid -ie
timeout $OUT/$2`
                if [ "$AUTFAIL" ]; then
                   kill -9 $tID $TID
                   cp $OUT/$2 $OUT/$1.log
                   cp $ERR/$2 $ERR/$1.log
                 echo "Error - Usuario invalido" >> $ERR/$2
                 exit
                fi
           done

           echo "$pass" >> $TMP/$2

           while [ ! "$prompt" ]
           do
                   prompt=`tail -1 $OUT/$2 | grep -e ">" -e "#"`
                AUTFAIL=`grep -ie failed -ieAuthentication -ie "Login
invalid" $OUT/$2`
                if [ "$AUTFAIL" ]; then
                   kill -9 $tID $TID
                   cp $OUT/$2 $OUT/$1.log
                   cp $ERR/$2 $ERR/$1.log
```

```
                echo "Error - Falla de autenticacion" >> $ERR/$2
                exit
               fi
               TIMEOUT=`grep -i timeout $OUT/$2`
               if [ "$TIMEOUT" ]; then
                  kill -9 $tID $TID
                  cp $OUT/$2 $OUT/$1.log
                  cp $ERR/$2 $ERR/$1.log
                  echo "Error - Timeout expired" >> $ERR/$2
                  exit
               fi
         done

      if [ "$3" = "ena" ]; then
         echo "enable" >> $TMP/$2
         sleep 2

           echo "$enap" >> $TMP/$2

         while [ ! "$prompt2" ]
         do
                 prompt2=`tail -2 $OUT/$2 | grep -e "#" -e
"(enable)"`
               TIMEOUT=`grep -ie timeout -ie denied $OUT/$2`
               if [ "$TIMEOUT" ]; then
                  kill -9 $tID $TID
                  cp $OUT/$2 $OUT/$1.log
                  cp $ERR/$2 $ERR/$1.log
                  echo "Error - Timeout expired" >> $ERR/$2
                  exit
               fi
```

```
            done
           fi ;;

      Username: )
            echo "$user" >> $TMP/$2

            while [ ! "$PASS" ]
            do
                    PASS=`grep Password $OUT/$2 | awk '{print $1}'`
                  AUTFAIL=`grep -ie Authentication -ie invalid -ie
timeout $OUT/$2`
                  if [ "$AUTFAIL" ]; then
                     kill -9 $tID $TID
                     cp $OUT/$2 $OUT/$1.log
                     cp $ERR/$2 $ERR/$1.log
                   echo "Error - Usuario invalido" >> $ERR/$2
                   exit
                  fi
            done

            echo "$pass" >> $TMP/$2

            while [ ! "$prompt" ]
            do
                    prompt=`tail -1 $OUT/$2 | grep -e ">" -e "#"`
                  AUTFAIL=`grep -ie failed -ieAuthentication -ie "Login
invalid" $OUT/$2`
                  if [ "$AUTFAIL" ]; then
                     kill -9 $tID $TID
                     cp $OUT/$2 $OUT/$1.log
                     cp $ERR/$2 $ERR/$1.log
```

```
                echo "Error - Falla de autenticacion" >> $ERR/$2
                exit
              fi
              TIMEOUT=`grep -i timeout $OUT/$2`
              if [ "$TIMEOUT" ]; then
                 kill -9 $tID $TID
                 cp $OUT/$2 $OUT/$1.log
                 cp $ERR/$2 $ERR/$1.log
                 echo "Error - Timeout expired" >> $ERR/$2
                 exit
              fi
        done

      if [ "$3" = "ena" ]; then
         echo "enable" >> $TMP/$2
         sleep 2

           echo "$enap" >> $TMP/$2

         while [ ! "$prompt2" ]
         do
                 prompt2=`tail -2 $OUT/$2 | grep -e "#" -e
"(enable)"`
              TIMEOUT=`grep -ie timeout -ie denied $OUT/$2`
              if [ "$TIMEOUT" ]; then
                 kill -9 $tID $TID
                 cp $OUT/$2 $OUT/$1.log
                 cp $ERR/$2 $ERR/$1.log
                 echo "Error - Timeout expired" >> $ERR/$2
                 exit
              fi
```

```
            done
fi ;;

      Password: )
            echo "Error - $1 no tiene TACACS" >> $ERR/$2
            exit ;;

      Password )
            echo "Error - $1 no tiene password" >> $ERR/$2
            exit ;;

        User: )
            echo "Error - $1 Dispositivo no Cisco" >> $ERR/$2
            exit ;;
      Local )
            echo "Error - $1 No tiene password" >> $ERR/$2
            exit ;;

      *\> )
            echo "Warning - $1 no tiene login" >> $ERR/$2 ;;

      * )
            echo "Error - $1 problema en la conexion" >> $ERR/$2
      exit ;;

esac
```

- obt_info_confreg:

Este script ejecuta una estructura de control, ciclo for mediante la cual recorre una lista en la cual ya están contemplados todos los dispositivo de red almacenada en el archivo llamado `bb_rtrs ,` el cual contiene una relación de nombre de equipos con su dirección IP.

A los cuales se va a conectar para obtener los comandos de verificación.

Ejemplo del contenido del archivo:

```
router-4      10.6.28.9
router-42    10.14.8.189
router-15   10.18.19.21
router-10    10.3.22.205
router-11    10.25.97.13
router-9     10.15.87.130
router-32     10.15.10.169
router-10      10.125.0.48
router-14      10.38.193.19
router-17      10.38.193.25
router-41      10.14.12.207
```

Este es el código:

```
DIR=~/fallas

COUNT=0
NR=`wc -l pes_rtrs | awk '{print $1}'`


for RTR in `cat bb_rtrs`
do
    CONT=`ps -fea | grep show_version | grep -v grep | wc -l`

    while [ $CONT -ge 10 ]
    do
         CONT=`ps -fea | grep show_version | grep -v grep | wc -l`
    done
```

```
    let COUNT=COUNT+1

    echo "Conectando a router $RTR $COUNT"

    $DIR/show_version $RTR &

Done
```

- **sho versión:**

Si se necesita obtener cierta información de la red lo que se hace es agregar a este script los comandos necesarios.

Verificando agregar dependiendo de la plataforma con la que cuenta el dispositivo de red el comando que nos proporcione la información requerida, de acuerdo a esta información va a tomar una matriz de comandos los cuales va a ejecutar una vez realizada esta clasificación.

```
#!/usr/bin/ksh
DIR=~/fallas
BIN=$HOME/bin
TMP=$DIR/tmp
ERR=$TMP/errores
OUT=$TMP/salidas
BKP=$DIR/bkp
ARC=$1

export PATH=/usr/xpg4/bin:$PATH
export DIR

cat /dev/null > $TMP/$ARC
```

```
$BIN/conecta $1 $ARC 2> $ERR/$ARC

error=`tail -1 $ERR/$ARC | awk '{print $1}'`
tID=`tail -1 $ERR/$ARC.pid | awk '{print $1}'`
TID=`tail -1 $ERR/$ARC.pid | awk '{print $2}'`

if [ "$error" = "Error" ]; then
     echo "$1:  \c"; tail -1 $ERR/$ARC
exit
fi

grep Warning $ERR/$ARC


juniper=`l0 $equipo  | grep lo0 `

if [ ! "$juniper" ]; then
          echo "show configuration | no-more"
echo "show configuration | display set | no-more"
echo "show interfaces descriptions | no-more"
echo "show bgp summary"
echo "show chassis hardware detail"
echo "show chassis routing-engine"
echo "show chassis craft-interface "
echo "show version invoke-on all-routing-engines"

else

echo "terminal monitor"
echo "terminal length 0"
```

```
echo "show running-config"
echo "admin show version brief"
echo "admin show diag"
echo "admin show platform"
echo "admin show led"
echo "admin show hw-module fpd location all"
echo "show power-mgr detail"
echo "admin show environment power-supply"
echo "admin show environment temperatures"
echo "admin show environment voltages"
echo "admin show install active"
echo "admin show media location all"
echo "admin show inventory"
echo "show boot"
echo "show cdp neighbor det"
echo "show redundancy"
echo "show interface brief"
echo "show interfaces description"
echo "show bgp ipv4 unicast summary"
echo "show bgp vpnv4 unicast summary"
echo "show ospf neighbor"
echo "show ospf interface brief"
echo "show mpls interfaces"
echo "show mpls ldp neighbor brief"
echo "show context"
echo "show memory summary"
echo "show bgp vrf all summary "
echo "show bgp vrf all summary "
echo "show loggin"

     fi
```

```
echo "term len 0" >> $TMP/$ARC

    echo "show version | i Config" >> $TMP/$ARC


echo "exit" >> $TMP/$ARC

while [ "$TID" ]
do

    TID=`ps -fe | grep  " $TID " | grep telnet | awk '{print $2}'`

done

kill -9 $tID
```

La interacción de los scripts la lleve a cabo de la siguiente manera:

Primero el script *obt_info_confreg* ejecuta un ciclo for para una lista de hostnames (nombres/identificadores de los dispositivos de red) que se encuentran enlistados en un archivo. Dentro de éste script se ejecuta a su vez el script *show_version* el cuál contiene los comandos que se van a ejecutar en los equipos en cuestión. Dentro del script *show_version* se manda ejecutar el script *conecta* que es el que establece y controla la conexión Telnet con el equipo especificado.

3.3.7 Manuales de difusión

BÚSQUEDA DE SYSLOG DE LOS EQUIPOS EN UN RANGO DE DÍAS DETERMINADO.

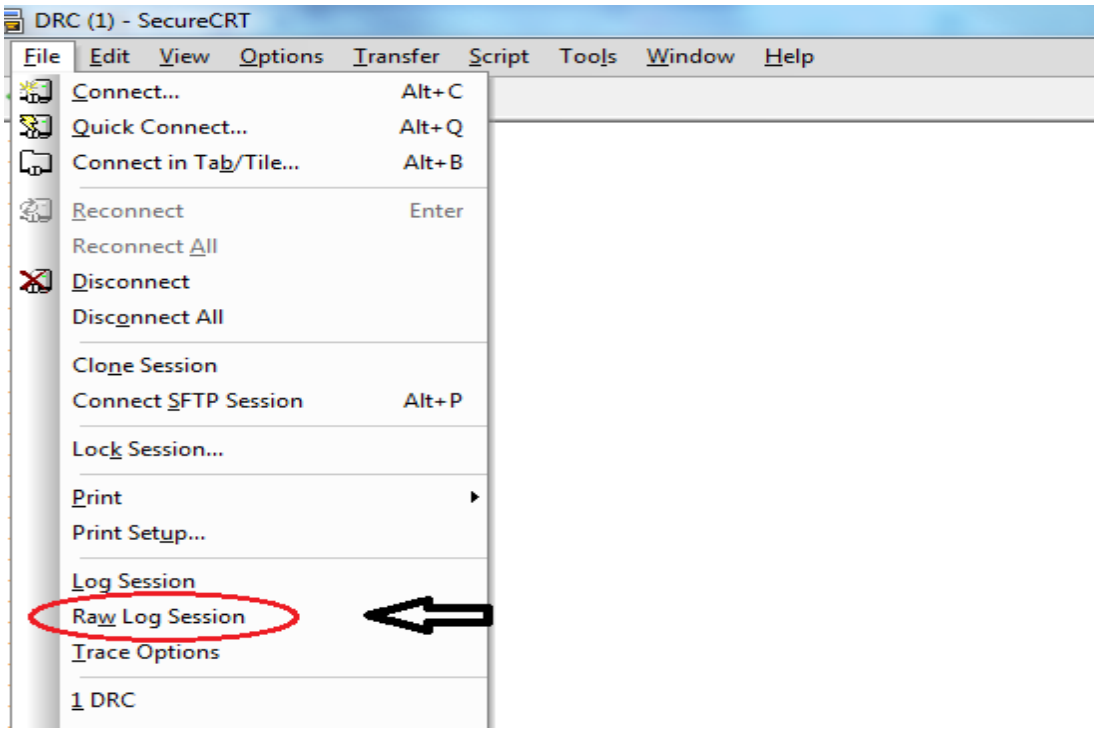
Objetivo: Obtener el SYSLOG de un equipo en específico en un rango de fechas determinado.

PROCEDIMIENTO:

1. Entrar al servidor
    - 10.88.33.4

2. Entrar a la carpeta
    - $ cd /export/home/hernandg

3. Guardar la sesión (ya que la información la despliega en pantalla únicamente)



4. Introducir la siguiente sentencia

- ./findsyslog equipo fechainicial fechafinal

  Con el formato:

  - ✓ Equipo [hostname]: router-3
  - ✓ Fecha inicial: ddmmaa
  - ✓ Fecha final: ddmmaa

  Ejemplo:

  $ ./findsyslog *router*-3 010514 050514

5. Se empezara a desplegar en pantalla la información solicitada.

CONSULTA DE ESTATUS DE LOS DISPOSITIVO DE RED MEDIANTE COMANDOS DE VERIFICACIÓN

Objetivo: Obtener información del estatus en el que se encontraba tanto el software, hardware y configuración de un dispositivo de red en un día determinado.

PROCEDIMIENTO:

1) Entrar al servidor
   - 10.10.3.4

2) Entrar a la carpeta
   - $ cd /uninet/comandos/
   - $ls

     050115
     050215
     060115
     060215
     070115
     070215
     080115

3) Entrar a la carpeta del día que se desea consultar con el formato DDMMAA.
   - $ cd DDMMAA

4) Buscar el dispositivo de red de interés, utilizando el filtro *grep*

- $ ls | grep *router*-42

  router-42

5) Consultar la información dentro del archivo se tienen 2 opciones:

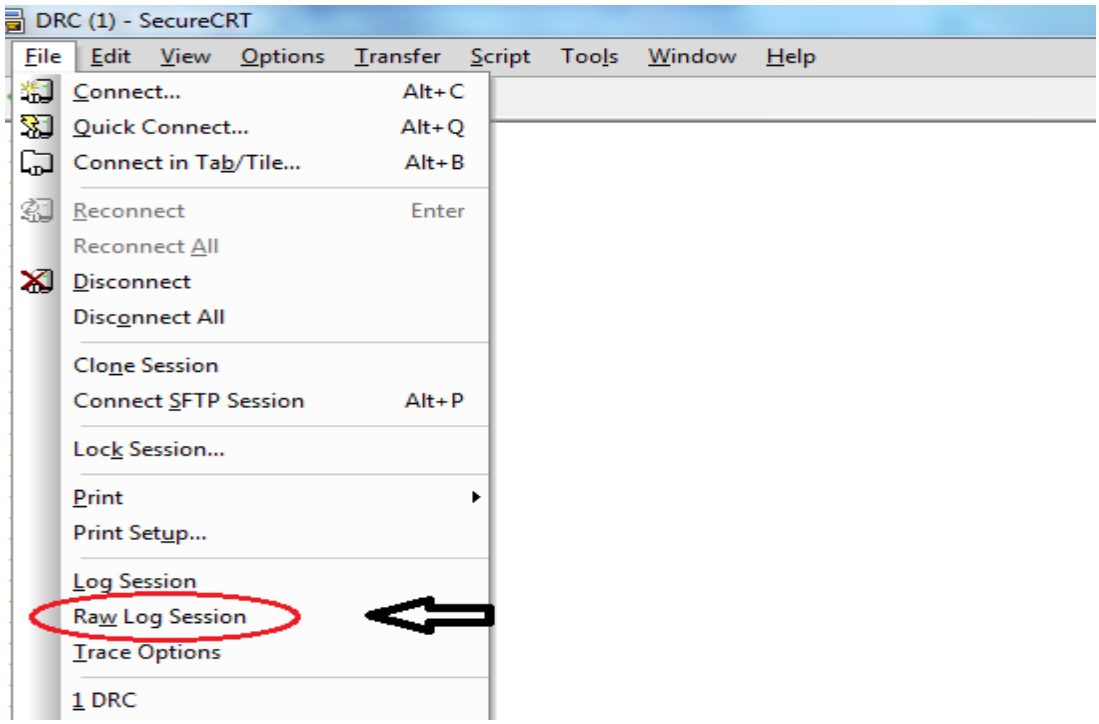
   La primera es mostrar en pantalla, hacer uso del filtro sed y observar la información de interés.

   Ejemplo si se quiere observar solo el comando show versión quedaría de la siguiente manera:

- $ head cat *router*-42 | sed '/show version/p'

   La otra opción es guardar la sesión, desplegar en terminal la información y guardarlas capturas de los comandos de verificación en un archivo de texto plano.

   a. Guardar la sesión (ya que la información la despliega en pantalla únicamente)



b. Introducir la siguiente sentencia

- $cat *router*-42

c. Se empezara a desplegar en pantalla la información.

4 PARTICIPACIÓN PROFESIONAL, RESULTADOS Y APORTACIONES

4.1 Puesto de trabajo y aportaciones

El puesto desempeñado actualmente es el de Ingeniero Red Staff en el área de Gestión de Fallas Corporativo (GFC) , GFC es un área que pertenece a la subdirección Operación Red de Datos, a la Gerencia Gestión de Fallas Red Acceso y a la Jefatura Red Acceso Corporativo.

El organigrama del área consta de un Jefe red de Acceso, Supervisores e Ingenieros los cuales dependiendo de su experiencia, desarrollo y conocimiento del área pueden ser Staff, Junior o Senior

Las actividades del aérea están basadas en el Proceso de Incidentes, este proceso tiene como objetivo:

- Restaurar la operación normal del servicio en el menor tiempo posible.
- Minimizar eL impacto de las interrupciones del servicio.
- Atender los eventos que puedan causar afectación
- Asegurar el cumplimiento de los acuerdos de niveles de servicio.

Dividiendo su implementación en etapas y roles que determinan las actividades de los participantes del proceso.

Como área se tienen los objetivos de:

- El 80 % de los incidentes deben ser restaurados en menos de 120 minutos.
- No tener causas de incumpliendo en la restauración de incidentes.

- Realizar únicamente cambios de configuración que estén normados y documentarlos.
- No causar incidentes por actividades o intervenciones.
- Mejora continua de:
    - Servicio
    - Métricas
    - Operación de la red
    - Conocimiento desarrollo del personal.

Los servicios a los que se brinda soporte en el área son Internet dedicado, red privada virtual y voz sobre IP.

El puesto que desarrollo en la empresa es el de Ingeniero Staff, durante el desarrollo de este rol he llevado a cabo diferentes actividades, que conllevan diferentes responsabilidades, según la actividad a realizar por lo cual me permito hacer una clasificación de actividades, con sus responsabilidades respectivas:

ACTIVIDADES	RESPONSABILIDADES
Incidentes	▪ Atender solicitudes por Teléfono/Correo/Gestor de alarmas. ▪ Aplicar Proceso de Gestión de Incidentes. ▪ Documentar las actividades realizadas. ▪ Restaurar incidentes en tiempos compromiso.
Intervenciones Emergentes	Realizar actividades para modificar software o hardware de los equipos que causan o pueden ser motivo de provocar fallas en el servicio.
Peticiones de servicio	Modificaciones a un servicio puntual de manera temporal para realizar pruebas.

Conocimiento	▪ Conocer y entender los servicios *end-to-end* que atiende el área. ▪ Conocer y entender las normas de los servicios y elementos de red. ▪ Conocer y entender los procesos que aplican en el área. ▪ Conocer y entender los procedimientos que aplican en el área. ▪ Conocer y entender los niveles de servicio acordados y los acuerdos operativos.
Proyectos	▪ Planear, desarrollar, implementar y difundir. ▪ Asegurar el planear, desarrollar, implementar, difundir y medir.
Administrativas	▪ Programación de vacaciones. ▪ Contar con acceso actualizados para uso de las herramientas. ▪ Aplicar Acuerdos Operativos. ▪ Asistencia a juntas definidas por supervisión o subgerencia.
Recursos del área	▪ Identificar, usar y reportar el mal funcionamiento de las herramientas de gestión ▪ Cuidado de mobiliario (ACD, Equipo Computo)

Cabe resaltar que durante el desarrollo de la actividad Proyectos, realice las actividades que involucran el proyecto que se describe durante el desarrollo de este reporte.

4.2 Resultados

Por medio de la vinculación de los lenguajes de programación con los dispositivos de red a través del protocolo de Telnet emulando la interacción del humano con estos dispositivos y la administración de la información, pude lograr optimizar las tareas que se realizan día con día, aumentando la efectividad de la operación y disponibilidad del servicio ayudando en múltiples actividades tales como:

Auditorias:

1. Contabilizar con exactitud cuántos equipos se tienen en operación con cada sistema operativo y cada una de sus versiones.

2. Se tiene un proyecto de ingeniería de migrar todos los equipos que prestan el servicio de voz a una versión más reciente de sistema operativo, la fecha planeada de fin es solo una aproximación ya que durante las migraciones se han presentado eventos no contemplados que han hecho variar el porcentaje de avance, por lo cual se decide validar que porcentaje es realmente el que se ha avanzado, para poder determinar si es posible dejar esa fecha planeada de fin o cual es la tolerancia que se necesitara para terminar el proyecto.

Fallas:

1. Se encuentra una interface en estatus administrativamente *down* y no se sabe si fue dada de baja por un usuario o por falla en el equipo. Es necesario verificar todo el log de eventos del equipo para determinar que fue la causa del cambio de estatus de esta interface.

2. Se está realizando un diagnostico de causa raíz y se necesita los mensajes de SYSLOG de un equipo durante los últimos tres meses.

3. Cliente reporta que un servicio se queda fuera después que un enlace E1 restablece y es el único servicio que queda *down*, se requiere determinar en que estatus se encontraba antes de la caída del enlace a nivel de E1.

4. Un equipo no reconoce una tarjeta en la ranura (slot) 8, se necesita saber cuál es el número de serie de la tarjeta dañada para pedir a proveedor la pieza que se va a remplazar, sin embargo el equipo ya no la reconoce en este momento y no despliega la información correspondiente, se revisa en respaldos un historial del inventario de hardware y se logra obtenerlas especificaciones de hardware a remplazar.

5. Un comando dentro de la configuración de una interface no es compatible con el tipo de encapsulación que se tiene y provoca oscilaciones físicas en la interface, esta configuración se tenía contemplada en un proyecto ya que teóricamente es correcto aunque ya operacionalmente provoca este comportamiento, que no se presenta inmediatamente, por lo cual se necesita encontrar en que interface se encuentra realmente configurado en los diferentes dispositivos de red, se hace una búsqueda automática en la configuración de las interfaces y se logra determinar cuáles son las que tienen este parámetro configurado y se logra eliminar.

Al aumentar la efectividad en el desarrollo de estas tareas se logró obtener resultados favorables para el negocio como el reforzar el aseguramiento de la disponibilidad, para poder cumplir los acuerdos de niveles de servicio (los cuales establecen un contrato en el cual el proveedor del servicio se compromete a cierta calidad en cuanto a tiempo de respuesta, horarios de disponibilidad y personal asignado a la operación) , cumplir métricas internas como por ejemplo el tiempo de restauración, se logró tener fiabilidad en la información almacenada ya que se obtiene directamente de lo que se tiene en operación.

Acciones que se traducen a ofrecer al cliente un servicio de calidad que cumpla con sus expectativas, requerimientos para su negocio y el cumplimiento de los acuerdos respecto a la operación del servicio.

Haciendo que el proveedor se vuelva una empresa fiable, con prestigio y altamente recomendada en la industria para prestar servicios de tecnologías de la información.

4.3 Capacidades y habilidades aplicadas, adquiridas y desarrolladas.

Durante mi preparación en la adquisición de los conocimientos necesarios al estudiar la carrera de ingeniería en Telecomunicaciones y durante el desarrollo de mi vida profesional he aplicado conocimientos de las ciencias básicas Física y Matemáticas , para realizar cálculos en las asignaciones de direcciones del protocolo IP en sus diferentes versiones 4 y 6, así como el entendiendo de su funcionamiento, en las mediciones de los voltajes que necesitan los equipos para trabajar correctamente, en los niveles de potencia que se reciben en cada uno de los enlaces y lograr determinar cuáles son los rangos mínimos y máximos con los que se puede operar.

He adquirido y aplicado conocimientos correspondientes a señales y sistemas electrónicos y de computación al analizar y diseñar programas que se conecten de manera automática con los diferentes dispositivos de red conociendo previamente las funcionales que cada una de las plataformas de los diferentes proveedores tecnológicos nos ofrece ya sea Huawei, Juniper o Cisco,

He logrado entender cuál es su arquitectura de los dispositivos de red tanto de software como de hardware, cuales son los parámetros que se necesitan para que funcione cada uno de sus elementos, ya sean de configuración, o físicos como voltajes, temperaturas o potencias.

Así como diseñar, planear, organizar, producir, instalar y desarrollar diferentes herramientas para hacer las actividades del día a día en el trabajo de una manera más eficiente haciendo uso de software y programas ejecutables que permiten simular la interacción del humano con los diferentes dispositivos de red o agregar nuevas funcionalidades a los equipos que son nuestra herramienta de trabajo.

He desarrollado la capacidad de operar y administrar el principal sistema de telecomunicaciones del país, he entendido a detalle los servicios que ofrece , la interacción entre diferentes redes de proveedores de servicios, e identificado cuales son los componentes de cada uno de los modelos de los equipos de los dispositivos de red,

cuál es su diferencia , sus ventajas y desventajas, sus funcionales , la capacidad que tienen y como se traduce a número de usuarios, así como sus principales fallas con las que se cuenta dando diagnósticos cada vez más rápidos y certeros.

He aprendido a modelar, simular, operar y mantener las redes de comunicaciones, en diferentes software de simulación realizando las prácticas necesarias para aprobar los cursos y las certificaciones de la industria con las que cuento actualmente.

He llevado a cabo mi trabajo bajo condiciones que me demandan gran concentración, y para dar solución a los problemas que se plantean hago uso del análisis matemático y físico

En el área de GFC somos un grupo interdisciplinarios estamos de diferentes instituciones y carreras afines, he aprendido a Integrar y coordinar personas y grupos interdisciplinarios, durante el desarrollo de proyectos y resolución de fallas, ya que se necesitan tanto conocimientos como trabajo en equipo de múltiples áreas.

He asimilado plenamente las formulaciones teóricas, he reforzado la capacidad de hacer, he asegurado los conocimientos con los que cuento y desarrolle la sensibilidad sobre los fenómenos que se estudian, todo mediante la comprensión sistemática de las predicciones teóricas con las observaciones de laboratorio y campo.

He desarrollado mi capacidad de trabajar en equipo solicitando y compartiendo conocimiento y opiniones de diferentes diagnósticos para poder llegar a una solución a la falla que esté presente.

He desarrollado mi capacidad de identificar los puntos importantes y la forma de comunicarlos de manera concisa, ya sea a proveedores tecnológicos, a jefes, al cliente o a mis compañeros de trabajo.

Transmitir conocimiento e interactuar con personal técnico, dando información a un nivel que nos permita interactuar.

Me comunico con personal en otros países por lo cual he desarrollado las habilidades de escuchar, escribir, leer y hablar el idioma inglés, ya que es el único idioma que tenemos en común y con el que se puede interactuar.

El campo de las telecomunicaciones es un sector que se desarrolla muy rápidamente por lo cual he logrado adaptarme a los cambios de las tecnologías en este campo.

He desarrollado una actitud emprendedora y de liderazgo, que me ha permitido ser promotor del cambio frente a la competitividad internacional, y participado en eventos de inclusión digital para todo el país como lo es “aldea digital” ya que tengo plena conciencia de la problemática nacional en este campo.

He contado con constancia y tenacidad en las actividades emprendidas, ya que es un sector que evoluciona rápidamente y demanda estudio constante.

CONCLUSIONES

De acuerdo a los objetivos determinados al inicio del proyecto, se puede afirmar que fueron logrados de manera exitosa y cumpliendo las expectativas contempladas ya que se tuvo una planeación adecuada, se analizó y diseñó una manera de alcanzar el objetivo de implementar una opción de automatización de obtención e interpretación de información en una red de datos.

A lo largo del desarrollo de este proyecto se determino que el manejo de información que nos provee un dispositivo de red para poder analizar los eventos y los estatus en los que se encuentran son muy abundantes y más cuando se tiene una red con miles de equipos operando y cada uno de ellos con una configuración compleja y robusta, ya que los servicios que se tienen operando en cada uno de ellos, cada vez dependen de mas parámetros con la finalidad de aumentar la eficiencia en la operación de cada uno de ellos.

Así como es de suma importancia contar con la capacidad de interpretar y clasificar la información, contemplando que el hecho de contar con una información y no utilizarla es como si no se tuviera, así como la interpretación en un corto plazo ya que los acuerdos de niveles de servicio establecen un tiempo determinado en el cual se tiene que solucionar una falla para poder lograr las métricas de disponibilidad en el servicio, por lo cual el tiempo en el que es encontrada e interpretada la información es determinante para poder encontrar una solución con mayor rapidez.

Cabe mencionar que para poder llegar a esta implementación final de los scripts fue durante un gran periodo de pruebas ya que es cierto que la teoría da las bases para poder determinar cuál es la estructura que se debe dar a un programa para poder obtener la información que se requiere, sin embargo de manera práctica se determina que se cuenta con muchas otras variantes que no dependen de los programas en sí, si no de variables externas que llegan a afectar la operación , como por ejemplo todas las validaciones que se tuvieron que realizar en el archivo *conecta* en el cual se tienen que tomar en cuenta todas los posibles motivos por los cuales no se puede lograr una conexión exitosa en todos los equipos, las cuales no todas surgieron al primer intento si no después de poner

en operación el script y verificar el por qué no se logró una ejecución exitosa del programa.

Se comprendió la importancia de saber exactamente las diferentes opciones que nos da cada una de las plataformas para poder determinar cuáles son realmente los comandos de verificación que nos proporcionan la información que se necesita en la atención de fallas y auditorias que se fueron dando durante este tiempo que llevo laborando en la empresa.

Se identificó que es necesario hacer un análisis de las fallas que son mas recurrentes y cuáles son las necesidades propias como las del equipo de trabajo, para poder elegir cuales son las tareas de automatización necesarias y cuales serían los alcances y objetivos de estas herramientas.

Se aprendió que es posible relacionar diferentes tipos de conocimientos que aunque a simple vista parecen no tener relacionar entre sí al momento de hacer una tarea en conjunto haciendo una incorporación de diferentes conocimientos, permiten el desarrollo de estas herramientas que han ayudado al desarrollo de las actividades propias del área.

Se logró cumplir los objetivos de desarrollar una herramienta que permitiera:

- Agilizar búsquedas.
- Realizar el tratamiento, almacenamiento y organización de información.
- Estructurar un sistema de respaldos automáticos.
- Evitar saturación de memoria dando la capacidad de obtener la información y almacenarla en diferentes localidades.
- Interpretar de datos.
- Actualizar bases de datos.

Realizar comparaciones de los cambios de configuración realizados en determinadas fechas, poder almacenar de manera organizadas los mensajes que los diferentes dispositivos generan a partir de eventos que acontecen dentro de ellos.

- Encontrar a un cliente mediante un identificador único dentro de toda la red, relacionándolo con un determinado perfil, dispositivo y localidad del dispositivo en donde se encuentra configurado.

Un factor importante y determinante que ayudo a lograr el desarrollo de este proyecto fue el conocimiento que aporto la facultad de ingeniería tanto en el ámbito teórico, como en el de proveerme del desarrollo de mis capacidades de trabajo en equipo e identificación de puntos de mejora que se pueden implementar.

Ya que aunque la empresa cuenta con proveedores externos de herramientas y áreas internas dedicadas exclusivamente a la implementación de estas, siempre es importante tratar de identificar un punto de mejora y poder desarrollar una herramienta que pueda cubrir las especificaciones de acuerdo a las necesidades que se identifiquen en la operación del área.

Sumando a esto que para poder contactar a un proveedor externo que nos de la solución a esta necesidad es un proceso un tanto tedioso, ya que se tiene que exponer la necesidad a nivel dirección y posteriormente contemplarla en el reparto de presupuesto, haciendo un proceso administrativo de larga duración , lo cual resulta poco efectivo para cubrir estas necesidades y es necesario hacer uso de desarrollos locales que además de proveerlos con mayor rapidez, es fácil pedir al grupo de trabajo que se mantenga en evaluación y recibir retroalimentación específica de cada miembro del grupo referente a las mejoras que se pueden hacer a la herramienta.

Se aprendió a identificar las diferencias entre los modelos de *router*s, que se traducen en ventajas y desventajas, dependiendo del servicio para el que se va a asignar este dispositivo, se identificó que tanto las configuraciones físicas como las lógicas tienen que ser convergentes, por lo cual es importante especificar y saber identificar elementos físicos, que sean congruentes con la configuración lógica de las interfaces y los protocolos de enrutamiento que se vayan a utilizar.

De los conocimientos adquiridos a lo largo de la carrera , se aplicaron aquellos obtenidos dentro de asignatura como electricidad y magnetismo, circuitos eléctricos, circuitos y

dispositivos de radio frecuencia, ya que la instalación de estos equipos se realiza de manera remota con personal en sitio y el personal va dando una descripción de las actividades realizadas, donde el responsable es quien da las indicaciones remotamente, por lo cual únicamente el personal en sitio funge como ojos y manos, pero las indicaciones de la instalación de los equipos se realizan vía remota, no sin antes analizar las especificaciones contenidas en los manuales y los planos de las instalaciones de las diferentes centrales de datos.

Referente a las materias sistemas de comunicaciones ópticas, comunicaciones digitales, telefonía digital, fundamentos de sistemas de comunicaciones dentro la red, en la configuración de las interfaces que corresponden a un cliente se asignan referencias las cuales dependen del ancho de banda y servicio para el cual el enlace es ocupado, así que para determinar la posición exacta del canal donde se encuentra configurado el servicio de algún cliente en particular, se tienen que saber identificar cuantos E1s se tienen en un STM1,asi como sus especificaciones de cada uno al igual que un E3 para poder identificar errores de medio es necesario conocer los principios para medir, revisar y validar los parámetros más significativos en la sincronización de enlaces en interfaces POS(*packet over sonet*) habilitados sobre medios SDH/SONET o WDM, así como los fundamentos del modo en el que se sincronizan los elementos de una red de transporte óptica SDH/SONET.

Del mismo modo, conocer detalles para identificar y solucionar los puntos de falla asociados a problemas que afectan la sincronía de enlaces conectados con interfaces (POS) cuyo transporte es SDH, SONET o WDM.

Redes de datos I, redes inalámbricas y móviles, redes inalámbricas avanzadas fueron asignaturas que permitieron aplicar los conocimientos adquiridos de protocolos de enrutamiento como BGP, OSPF, LDP, y conocer gracias a los fundamentos adquiridos protocolos más complejos como eBGP y MPLS por mencionar algunos.

Cabe mencionar que el hecho de no nombrar alguna de las materias contenidas dentro del plan de estudios, no significa que no fueron de importancia o que los conocimientos adquiridos no han sido utilizados dentro de la experiencia laboral, si no por el contrario recordemos que la licenciatura es todo una ramificación de conocimientos que se complementan unos con otros y al final permiten ocuparlos y entender de manera más clara el funcionamiento de un proceso o de algún producto quel con lleva a mezcla de

diferentes áreas del conocimiento que al final permiten agregar efectividad a la prestación de un servicio, a la manufactura o a alguna actividad que se realice en el día a día.

Los retos futuros con los que cuento es continuar con la academia de estudio de los diferentes proveedores tecnológicos para obtener más certificaciones de la industria que me permitan obtener un conocimiento más especializado, el cual pueda aplicar en el desarrollo profesional.

Contribuir al desarrollo de herramientas internas del área para realizar con mayor eficiencia las actividades disminuyendo el tiempo invertido por el recurso más importante, el recurso humano.

Concluir con mi estudio del idioma inglés.

Aplicar mis conocimientos para aumentar mi desempeño en mi puesto de trabajo y seguir contribuyendo en proyectos de mejora, con la ayuda de diferentes áreas interdisciplinarias.

Estudiar una maestría en la gestión de servicios de tecnologías de la información.

GLOSARIO DE TÉRMINOS

A

Acuerdo de Nivel de Servicio (*SLA Service Level Agreement*) Acuerdo escrito entre un proveedor de servicio y un Cliente, el cual documenta los servicios y los Niveles de Servicio pactados.

Archivo *running-config.* En los *Switches* y *routers* es el nombre del archivo que reside en la memoria RAM y que almacena la configuración que actualmente se está usando en el dispositivo.

Archivo *startup-config*: en los *Switches* y *router* es el nombre del archivo que reside en la memoria NVRAM y almacena la configuración de dispositivo que se cargará en la RAM a modo de archivo *running-config* cuando se recargue el dispositivo o se encienda.

Autenticación: En seguridad, se trata de verificar la identidad de una persona o de un proceso.

Autorización En seguridad, consiste en determinar los derechos que se le permiten a un usuario o dispositivo especifico.

C

Causa Raíz: Es un término de resolución de errores que se refiere a la razón de la existencia de un problema, concretamente una razón por la que, si ésta cambia, el problema se resolvería o se convertiría en un problema diferente.

Clasificación. Es el proceso de agrupar formalmente elementos de configuración y cambios por tipo.

Conmutación de paquetes: Es la referencia genérica de los servicios de red, en la que el servicio examina el contenido de los datos transmitidos para tomar alguna decisión de envío.

Contabilidad: En seguridad es mantener un registro de las actividades realizadas por un usuario o dispositivo.

Convergencia: Es el tiempo necesario para que los protocolos de enrutamiento reaccionen a los cambios que se producen en la red.

D

Desencapsulación: Es el proceso por el que el dispositivo interpreta las cabeceras de la capa inferior y, al terminar con cada cabecera, elimina esta cabecera y coloca una de capa superior.

Detección de errores: Proceso consistente en descubrir si una trama a nivel de enlace de datos ha cambiado o no durante la trasmisión.

Dirección IP: Es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un dispositivo de red.

Dirección MAC: Dirección de capa de enlace de datos estándar necesaria para cada dispositivo que conecte con una LAN.

E

Elemento de Configuración (*Configuration Ítem* – CI). Componente de infraestructura o elemento que está o estará, bajo gestión.

Error conocido - Problema que ha sido diagnosticado y del cual se ha identificado la causa raíz, procedimiento para solucionarlo temporalmente y/o solución definitiva.

Escalación: Ocurre cuando se involucra a personal de mayor autoridad y/o experiencia, en el momento que un Incidente o Problema no puede ser solucionado dentro del tiempo acordado.

Evento. Un cambio en el estado que es importante para la Gestión de un Elemento de Configuración (CI) o un Servicio.

H

Host: Cualquier dispositivo que utiliza una dirección IP.

Hub: Es un dispositivo LAN que proporciona un punto de conexión centralizado para el cableado de una LAN , repitiendo cualquier señal eléctrica recibida por todos los puertos.

I

IEEE: Institución de ingenieros eléctricos y electrónicos (*Institute of Electrical and Electronics Engineers*).Es una organización profesional que desarrolla estándares de comunicaciones y redes , entre otras actividades.

Impacto. Determina la importancia del incidente, problema o cambio dependiendo de cómo éste afecta al negocio.

Incidente: Evento que no es parte de la operación normal del servicio y causa, o puede causar, una interrupción, o reducción en la calidad del servicio.

IP: Protocolo de Internet. Protocolo de la capa de red de la pila TCP/IP, que ofrece estándares y servicios de enrutamiento y direccionamiento lógicos.

ISO: Organización internacional para la normalización (*International Organization for Standardization*), tiene a su cargo una amplia gama de estándares, incluyendo los relativos al campo de redes.

N

Niveles de Servicio. Atributos medibles con los que cuenta un Servicio determinado, los cuales se plasman dentro de los Acuerdos de Niveles de Servicio

P

Problema. La causa desconocida de uno o más Incidentes.

Procedimiento. Forma especificada para llevar a cabo una actividad o un proceso.

Proceso. Conjunto estructurado de actividades diseñado para conseguir un objetivo específico.

Protocolo: conjunto de reglas lógicas que los dispositivos deben seguir para comunicarse.

R

Reparación. El reemplazo o la corrección de un elemento de configuración que ha fallado.

Resolución. Acciones tomadas para eliminar la causa raíz de un incidente / problema o para implementar un procedimiento para solucionarlo temporalmente o solución definitiva.

Restauración. Tomar medidas para devolver un Servicio a los usuarios después de la reparación y recuperación de un incidente.

Router: Es un dispositivo que envía paquetes de datos a lo largo de las redes. Un *router* está conectado al menos a dos redes, comúnmente dos LAN o WAN o LAN y su red del proveedor de servicios de internet.

S

Servicio. Medio para entregar valor a los clientes al facilitar los resultados que desean conseguir sin apropiarse de costos y riesgos específicos.

Switch: Dispositivo de red que filtra, envía e inunda tramas Ethernet basándose en la dirección de destino de cada trama.

T

Trama: Agrupación lógica de información que se envía como una unidad de capa de enlace de datos a través de un medio de transmisión

Trap: mensaje que se genera después de un evento que ocurre dentro de un dispositivo de red.

BIBLIOGRAFÍA

LIBROS:

Manual de inducción Red Uno

Código de ética. El valor de lo que se debe ser…y hacer. Red Uno

Wendell ,O.(2008) .CCENT/CCNA ICND1. (2ª ed).Madrid: Pearson Educación, S.A..

Header,A. (2010). LPI Linux Certification in a Nutshell.(3ª ed). Estados Unidos Americanos: O´Reilly.

Ariganello, E. (2015). Redes Cisco. Guía de estudio para la certificación CCNA Routing y Switching: Ra-Ma.

Comer, D, (1996).Redes globales de información con Internet y TCP/IP.(3ª ed). Estados Unidos Americanos: Prentice-hall.

Robbins,A.(2005).Classic Shell Scripting. Estados Unidos Americanos: O´Reilly.

Juniper Networks Inc.(2012). Junos Routing Essentials Student Guide(12a Revision).Estados Unidos Americanos:Juniper Networks Education Services.

Wendell ,O.(2008) .CCENT/CCNA ICND2. (2ª ed).Madrid: Pearson Educación, S.A..

Pink Elephant(2013).Fundamentos de ITIL. Canada:Syllabus.

PÁGINAS WEB:

http://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/configuration/guide/ffun_c/fcf014.pdf

http://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/7244-snmp-trap.html

http://www.hanantek.com/Software_en_Casa_Comercial_CodigoAbierto