Universidad Nacional Autónoma de México
Facultad de Ingeniería

"Sistema para Seguridad de Centrales Telefónicas"

Informe que presenta
Joseph Jaime Rosales Roque

Para obtener el título de
Ingeniero en Computación

México D.F. Mayo de 2008

SEGURIDAD PARA CENTRALES TELEFONICAS

INDICE

Objetivo……..Pág. 5

Panorama General……..Pág. 5

Introducción……Pág. 10

Definición del Problema……Pág. 11

Desarrollo……..Pág.12
- *Arquitectura*
- *Instalación*
- *Operación del Sistema SACET-GESTOR*
- *Configuración general de central*

Análisis y Metodología……..Pág. 24
- *Contingencias en el security-gateway*
- *Problemas RCDT*

Participación Profesional……..Pág. 32
- *Desarrollo de interfaz para monitoreo del sistema*
- *Instalación de parches*
- *Configuración de hardware*
- *Dar de alta tareas y programar archivos*
- *Generar rutas estáticas del security-gateway a RCDT*

Conclusiones……..Pág. 47

Anexos……Pág. 51

Bibliografía……...Pág. 55

Relación de Figuras

Figura 1.1 Arquitectura del sistema SACET.....*Pág. 12*

Figura 1.2 Listado General de Centrales.....*Pág. 15*

Figura 1.3 Catálogo de Administradores.....*Pág. 16*

Figura 1.4 Catálogo de Regiones.....*Pág. 17*

Figura 1.5 Plantilla de Alta de Centrales.....*Pág.20*

Figura 1.6 Pantalla de Configuración General.....*Pág. 21*

Figura 1.7 Ejemplo de Configuración de interfaz PR1. Proceso de desenmascaramiento de puertos.....*Pág. 30*

Figura 1.8 Menú del Sistema.....*Pág. 36*

Figura 1.9 Salida del FTP.....*Pág. 38*

Figura 1.10 Salida del Telnet.....*Pág. 40*

Figura 1.11 Submenú del sistema (por división).....*Pág. 43*

Figura 1.12 Estatus de los puertos en SACET.....*Pág. 54*

Objetivo

Proporcionar, administrar, monitorear el sistema Sacet, los equipos con los cuales cuenta, así como también proporcionar soporte a los usuarios que tengan problemas con dichas centrales, teniendo así un mejor servicio y previniendo el mal uso de la información que se maneja en la empresa.

Proporcionar y administrar la seguridad a las centrales telefónicas por cualquiera de sus métodos de acceso: puertos asíncronos por equipo PAD CODEX o CISCO PAD, puertos X.25 con protocolo MTP o puertos ethernet con protocolo TCP/IP. Así como establecer mecanismos de seguridad que impidan el acceso no autorizado a la red de conmutación, permitiendo solo el acceso por medio de las aplicaciones de gestión corporativas (NMA, Rant Sucor, Pisa, Auditoria de Servicios, DCMS´s). Filtrar los comandos que son enviados a las centrales telefónicas, asegurándose de que son realizados por usuarios registrados y con el nivel o perfil de seguridad suficiente. Todo esto con ayuda de con ayuda de *Sacet* el cual es un sistema de seguridad de acceso a centrales telefónicas institucional de Telmex.

Panorama General

Importancia Tecnológica, Social y Económica. El teléfono, objeto que fascinó a nuestros abuelos y que hoy parece tan familiar, es el resultado de muchos esfuerzos e invenciones para lograr que la voz humana se transmita a través de grandes distancias. Su historia comenzó en el taller de Charles Williams, en la ciudad de Boston, donde se investigaba sobre la electricidad. El entonces nuevo descubrimiento que llenó de admiración al mundo entero inició la carrera para construir piezas y mejorar las maquinarias y aparatos electrodomésticos, abriendo nuevos caminos a la creatividad. En dicho taller trabajaba Tomas A. Watson, quien sentía entusiasmo y simpatía por todo lo nuevo y se dedicaba de tiempo completo a la invención y perfeccionamiento de artilugios que funcionaran con electricidad.

Ahí tuvo lugar el feliz encuentro entre este inventor y Alejandro Graham Bell, quien tenía la cátedra de Fisiología vocal en la Universidad de Boston, y se había especializado en la enseñanza de la palabra visible (sistema inventado por su padre con el fin de que una persona sorda pudiera aprender a hablar). El profesor estaba interesado en mejorar su “telégrafo armónico”, aparato de su invención con el que esperaba transmitir en clave Morse 6 u 8 mensajes simultáneos. Así llegó al taller con la finalidad de buscar cauce tecnológico para su invento y ambos creativos comenzaron a trabajar juntos.

Más adelante Graham Bell le dijo a Watson estas palabras: “Si pudiera hacer que una corriente eléctrica variara en intensidad precisamente como el aire varía en densidad durante la producción del sonido, podría transmitir la palabra telegráficamente”. Clave del invento que después se llamó teléfono.

Tras varios intentos, el sueño de Graham Bell pudo materializarse en 1876, con una conversación entre ambos personajes transmitida de una habitación a otra por medio de un aparato. Por primera vez se escucharon las palabras: “Señor Watson, venga, le necesito”. Esta transmisión se considera como el nacimiento del teléfono. El nuevo invento fue presentado como una realidad en la Exposición del Centenario de Filadelfia en 1876, y a partir de entonces los avances en telefonía han sido extensos e impactantes hasta lo que hoy llamamos teléfonos celulares.

La implantación del teléfono, la llegada de los ferrocarriles, del telégrafo, de la industria del gas, de los coches y otros avances, transformó y modificó los espacios locales, regionales y nacionales. Las innovaciones tecnológicas tuvieron un papel fundamental para la industrialización y el comercio, pues permitieron la disminución de las distancias existentes entre los diferentes puntos de un territorio.

Las innovaciones tecnológicas organizadas en redes no pueden ser analizadas de manera aislada; hay que vincularlas con las estructuras económicas, políticas y sociales. El desarrollo comercial e industrial de los países se hizo patente en los centros urbanos de Brasil, la necesidad de un gran número de personas para trabajar en las industrias y un mercado consumidor emergente influyeron en su rápido crecimiento. Con el crecimiento de las ciudades, los agentes locales necesitaron de un medio de comunicación eficiente y el teléfono pasó a ser fundamental para los hombres de negocios.

La central telefónica. El concepto de central telefónica, por cuyo medio un teléfono pudiese conectarse con otro teléfono, fue propuesta por Edwin T. Holmes, quien dirigió una central de esta clase en 1877, en vínculo con su sistema de alarma contra ladrones en Boston. En este sistema, el par de hilos que sale de nuestro teléfono van sobre postes, al aire libre o subterráneos, recubiertos de aislante, a un edificio donde cientos de cables semejantes concurren para la interconexión.

En el campo de las telecomunicaciones, en un sentido amplio, una central telefónica es el lugar (puede ser un edificio, un local o un contenedor), utilizado por una empresa operadora de telefonía, donde se albergan el equipo de conmutación y los demás equipos necesarios, para la operación de llamadas telefónicas en el sentido de hacer conexiones y retransmisiones de información de voz. En este lugar terminan las líneas de abonado, los enlaces con otras centrales y, en su caso, los circuitos interurbanos necesarios para la conexión con otras poblaciones.

Uno de los motivos de la existencia de las centrales telefónicas, es el de ahorrar en el número de conexiones que se deben efectuar desde los aparatos telefónicos, uno de los primeros tipos fue la central con operadoras, que estableció el adelanto tecnológico posterior, había muchas empleadas, sentadas una al lado de las otras, delante de un cuadro de distribución telefónico. Cada una de estas empleadas estaba provista de un receptor y un emisor, ubicados delante de ellas en un panel, quedando así las manos libres. El frente del cuadro estaba formado

por un gran número de orificios pequeños llamados “jacks” y al lado de cada agujero estaba colocada una pequeña lámpara eléctrica. Cada uno de estos orificios representaba el final de una línea telefónica. Entre el operador y la cara vertical del cuadro había un estante angosto, de donde sobresalían cientos de terminales con la extremidad de metal. Estos se llamaban “clavijas”, e iban unidas a los cabos de cordones flexibles.

Cuando un abonado desmontaba su receptor del gancho, se prendía una de las diminutas lámparas del cuadro, y la operadora más próxima tomaba una de las clavijas y la insertaba en el jack adyacente a la bombilla encendida. La lámpara se apagaba, pero al mismo tiempo se encendía otra en el banco al lado del cordón flexible. La telefonista entonces cerraba un conmutador situado en el banco o estante que conectaba su teléfono con el del abonado y decía: “¡Central!” Al recibir el número que se deseaba, la telefonista tomaba otra clavija, la conectaba bajo el banco a la primera, la insertaba en el jack que pertenecía al número pedido y apretaba un botón, que hacía sonar el teléfono de la persona a quien se llamaba. Tan pronto como la persona, al contestar a la llamada, descolgaba el receptor de su teléfono, la lámpara adyacente al primer flexible se apagaba, indicando a la telefonista que había sido hecha la conexión pedida. Como el teléfono de aquélla era desconectado de la línea después de recibir el número deseado, quedaba la telefonista libre para establecer otras conexiones. Cuando el abonado en una línea volvía a colgar el receptor de su teléfono, la lámpara adyacente al flexible correspondiente se encendía, la telefonista retiraba la clavija, apagándose la lámpara, y se volvía a colocar la pieza en el estante. En una central telefónica activa las lámparas del cuadro estaban continuamente encendiéndose y apagándose, acompañadas de las llamadas, ” ¡central! “, y el tictac de las clavijas.

El otro tipo de medio, cuyo empleo se incrementó luego, a medida que las automatizaciones fueron reemplazando progresivamente a las operadoras, fue aquella en que las conexiones que se hacían por medio una máquina automática, que era dirigida por la persona que hacía la llamada. En lugar de esperar a que la telefonista pregunte el número que se desea, el abonado, de un modo automático, conectaba su teléfono con el de cualquier otro abonado haciendo girar una esfera numerada con las cifras sucesivas del número del teléfono deseado. La máquina automática conecta los dos teléfonos, y el abonado que llama puede entonces hacer sonar directamente el timbre del teléfono del otro abonado.

Para atender la demanda de los abonados se inventaron muchos modelos de centrales telefónicas por las diversas compañías. Hubo centrales que utilizaban el sistema inglés que consistía en un conmutador, un aparato que permite a cada abonado de la red telefónica llamar a la central y comunicarse con ella, y a ésta poner en comunicación a los abonados de una forma rápida y segura. Por cada conmutador de cien agujeros hay dos empleados, fijándose los indicadores respectivos, divididos en dos grupos, a cada uno de los lados del conmutador.

Cada empleado tenía a su disposición un teléfono para comunicarse con los abonados, habían además otros teléfonos que se emplean para enviar y recibir los recados de los despachos telefónicos.

Hoy en día existen algunas compañías que ofrecen la más amplia gama de servicios avanzados de telecomunicaciones, que incluyen transmisión de voz, datos y video, acceso a Internet y soluciones integrales para todos los segmentos del mercado de las telecomunicaciones; desde telefonía pública, rural y residencial, hasta la atención de clientes de la pequeña y mediana empresa, así como para grandes corporativos nacionales e internacionales, gracias a la gran capacidad técnica y de cobertura que brindan sus redes de acceso y transporte, que le han permitido un constante nivel de crecimiento en los productos y servicios que ofrece al mercado.

La Seguridad. Podemos entender como **seguridad** una característica de cualquier sistema (informático o no) que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible. Como esta característica, particularizando para el caso de sistemas operativos o redes de computadores, es muy difícil de conseguir, se suaviza la definición de seguridad y se pasa a hablar de **fiabilidad** (probabilidad de que un sistema se comporte tal y como se espera de él) más que de seguridad. A grandes rasgos se entiende que mantener un sistema seguro (o fiable) consiste básicamente en garantizar tres aspectos: confidencialidad, integridad y disponibilidad.

La **confiabilidad**, entendida como el nivel de calidad del servicio ofrecido. Consideran la disponibilidad como un aspecto al mismo nivel que la seguridad y no como parte de ella, por lo que dividen esta última en sólo las dos facetas restantes, confidencialidad e integridad.

a) **Confidencialidad:** nos dice que los objetos de un sistema han de ser accedidos únicamente por elementos autorizados a ello, y que esos elementos autorizados no van a convertir esa información en disponible para otras entidades.
b) **Integridad** significa que los objetos sólo pueden ser modificado por elementos autorizados, y de una manera controlada.
c) **Disponibilidad** indica que los objetos del sistema tienen que permanecer accesibles a elementos autorizados; es el contrario de la negación de servicio.

Generalmente tienen que existir los tres aspectos descritos para que haya seguridad: un sistema Unix puede conseguir confidencialidad para un determinado fichero haciendo que ningún usuario (ni siquiera el root) pueda leerlo, pero este mecanismo no proporciona disponibilidad alguna.

Las centrales telefónicas, se refuerzan ahora con una seguridad lógica ante la conectividad completamente abierta que proveen los puertos Ethernet y el protocolo TCP/IP. Estos puertos se han implementado en las centrales telefónicas y con ellos estos equipos se interconectan íntegramente a una red global con alcance mundial, proporcionando accesos, de los cuales una gran cantidad son accesos no controlados.

Esta facilidad y flexibilidad de acceso a las centrales telefónicas tiene un punto frágil, al ser un sistema abierto por su naturaleza, deja a estos equipos corporativos en un alto grado de vulnerabilidad para los accesos no autorizados, provocando una fragilidad para la corrupción del funcionamiento, alteración y destrucción de datos, fraudes, etc., y es que los elementos que conforman las redes de telecomunicaciones actuales, en particular las centrales telefónicas, continúan siendo un punto neurálgico central del negocio y prestación del servicio de las telecomunicaciones, y dada su arquitectura son elementos altamente sensitivos y delicados que incluyen sistemas integrados abarcando desde la facturación hasta la entrega de servicios al cliente.

La red de Telecomunicaciones y sus centrales telefónicas, son instalaciones de importancia que hoy en día puede ser ocupada como estrategia en cualquier país, ya que provee los medios necesarios para la comunicación continua a un nivel nacional e inclusive a un nivel internacional; por lo tanto, su seguridad operativa es un factor prioritario para cumplir la misión de continuidad del negocio y servicio de comunicación, tanto en situaciones normales de operación y más aun en situaciones de desastre donde la comunicación se hace vital para cualquier nación.

Introducción

Inicio mis actividades como profesionista en la empresa de Telefonía conocida en nuestro país como Telmex; casi inmediatamente cuando acabo el servicio social en Inttelmex (Instituto y dependencia de la empresa). Ahí entro a una área de sistemas la cual es la encargada de analizar, instalar y monitorear diferentes sistemas de gestión para dicha empresa es decir realizando soporte técnico (analista y consultor de sistemas) a toda la comunidad de Telmex la cual se encuentra hoy en día a nivel nacional.

Dicho lo anterior podemos definir como **soporte técnico** al órgano encargado de efectuar la evaluación, instalación, implementación, mantenimiento y adecuación de los diferentes sistemas de gestión y hardware que se tienen para monitoreo y buen funcionamiento de la red en Telmex, así como para prestar un óptimo y eficiente servicio y brindar la asistencia que se requiera.

El Área de Soporte Técnico se encuentra involucrada en el diseño y la implementación de Redes de Datos en las diferentes Centro Operativos (COPES), centros de Administración de la red (CAR), CAP, así como diversas áreas que se tienen en la organización. Es una de nuestras labores el implementar estos sistemas de acuerdo a las necesidades que se tengan en la empresa y con los usuarios, ya sea con personal netamente de nuestra área o en cooperación con personal de otras empresas dependiendo de la magnitud del proyecto.

Es así que me involucro en uno de los tantos proyectos y sistemas que tiene la empresa (y en los cuales en algunos he participado) llamado SACET. En el momento que yo ingreso este sistema se encontraba en pruebas en conjunto con las diferentes aéreas ya mencionadas. SACET es un sistema institucional de Telmex, el cual esta constituido funcionalmente por dos elementos que son: security-gateway: agente de seguridad local y el SACET-gestor que posteriormente se explicaran y el cual sirve para brindar seguridad a las centrales contra cualquier ataque, así como para prevenir cualquier mal uso de algún servicio; antes que nada tratare de explicar un poco lo siguiente:

Ataques en una Central Telefónica*.* En una central telefónica, se centran los ataques sobre su “mal uso” provocando “desvío de recursos” en actividades ilícitas. Para realizarlo, hace falta por una parte personal altamente calificado y por la otra una entidad dispuesta a pagar un precio por su anonimato. El fraude es un ejemplo de esto. Otro tipo de situaciones que se presentan en las centrales telefónicas son los malos manejos de información “por desconocimiento” provocando afectación al servicio del cliente, interrupción, mal funcionamiento, pérdida total o parcial de servicios, etc.; Por lo tanto, el manejo por desconocimiento se tiene cuando un usuario ejecuta sobre la central algunas funciones para las cuales no está autorizado, no capacitado o que por la razón de “probar“, trata de verificar un funcionamiento cuyas consecuencias desconoce.

Si a lo anterior aunamos el empleo de “malas prácticas”, como el manejo clonado de las cuentas de acceso donde el uso de una cuenta se multiplica prácticamente para cualquier usuario. También el uso de cuentas bien conocidas y nunca mantenidas que permiten acceso prácticamente a cualquier central. El uso de cuentas para acceder a todos los recursos de las centrales ó bien conocidas con la misma cuenta, se puede ejecutar cualquier acción prácticamente sobre cualquier central.

Por último agregamos que en su generalidad estas cuentas de acceso proveen un acceso al total de la funcionalidad en la central, desde su facturación, hasta el aprovisionamiento de servicios a clientes personales, empresariales, gobierno, etc.

Es por eso que con un equipo integrado por tres personas realizando funciones de soporte (en el cual soy una de ellos), un coordinador y con la ayuda del sistema SACET se trata de mantener seguras las centrales y asi brindar un mejor servicio a nuestros usuarios.

Definición del Problema

Evitar ataques a centrales, mal uso de información provocando desvío de recursos en ciertas actividades, malos manejos por desconocimiento provocando afectación al servicio del cliente, interrupciones o mal funcionamientos llegando a la perdida total o parcial de ciertos servicios, mal uso de accesos a dichas centrales llegando hasta el manejo clonado de cuentas de acceso provocando malas prácticas, pérdidas de servicios, problemas de facturación y operación con la ayuda del sistema SACET.

Así como cada día mejorar el monitoreo, optimización y recuperación de procesos del sistema, realizar un servicio de helpdesk (proporcionar asistencia a los usuarios). Implementar y ejecutar políticas de seguridad de datos (Backups y Restore). Evaluar, diseñar y administrar los recursos del sistema y base de datos, Establecer normas y estándares para el uso de software (instalación) y desarrollar procedimientos automatizados que conlleven a incrementar la productividad de la empresa. Evaluar, instalar y mantener equipos de emergencia, para cuando se requieran; todo esto con las diferentes aéreas involucradas y con el grupo de trabajo ya mencionado.

DESARROLLO

Arquitectura.

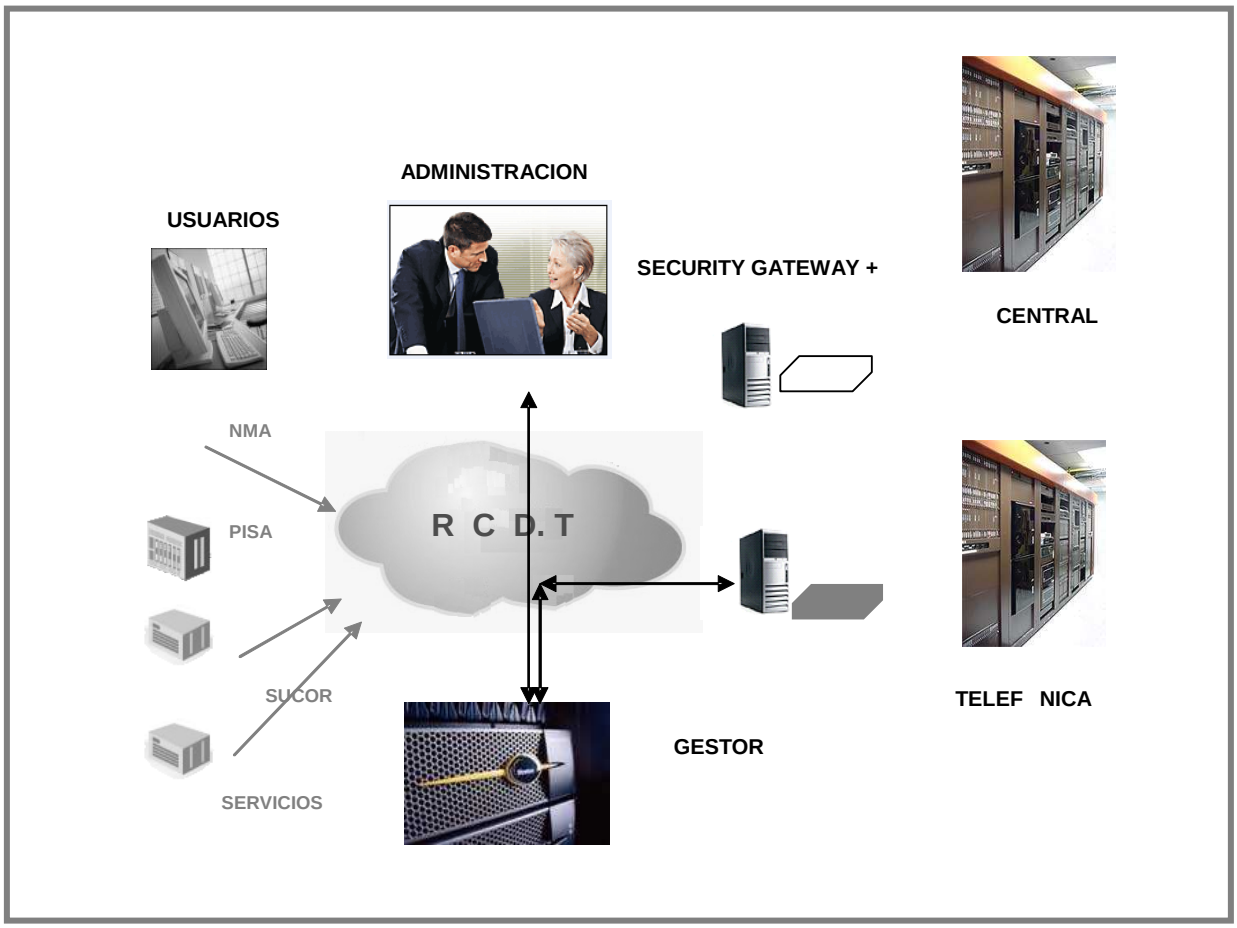


Figura. 1.1 Arquitectura del sistema SACET.

SACET utiliza una arquitectura administrador/agente como se muestra en la figura 1.1. El administrador constituye el sistema denominado “SACET-GESTOR” el cual reside en un servidor stratus modelo FtServer 5600 “tolerante a fallas”. Todas las funciones comunes como la administración de usuarios, control de la seguridad, recopilación de alarmas, etc., son desarrolladas por el sistema SACET-GESTOR. La administración de todos los recursos de la seguridad se realiza desde el SACET-GESTOR, el cual controla a todos los agentes.

Los agentes están constituidos por los sistemas de seguridad local denominados “security-gateway”, los cuales son “sistemas” independientes que radican y se ejecutan en una computadora PC ubicada físicamente a un lado de cada central telefónica Alcatel sistema 12.

Funcionalmente para cualquier aplicación o usuario que requiera acceder a la central telefónica, su acceso es filtrado por el sistema “security-gateway”, de tal manera que este sistema autentica a los equipos, aplicaciones y usuarios, permitiéndoles ejercer sobre la central únicamente los comandos que le son autorizados.

El grupo de comandos autorizados conforma “perfiles de comandos por usuario” y actúan de tal forma que un usuario solo podrá ejecutar sobre la central aquellos comandos que tenga definidos en su perfil, aquellos comandos que no le estén permitidos, le serán negados en su ejecución a la central. Los administradores del SACET- GESTOR se encargan de asignar los perfiles de comandos a los usuarios e incluso a las aplicaciones las cuales son vistas también como usuarios por el SACET.

En conjunto, los elementos tecnológicos SACET-GESTOR y security-gateway proporcionan seguridad en las centrales telefónicas y dan la flexibilidad de ser un sistema escalable en cobertura a nuevos elementos de red como son: equipos de transmisión, equipos de datos, conmutación de paquetes (conocidos como equipos “softswitch”), etc.

Instalación

La instalación básicamente consiste en la puesta a punto del security-gateway (PC), ubicándolo físicamente en la sala de control de la central telefónica dentro del gabinete del equipo DMCS. Adicionalmente se ubica dentro del mismo gabinete, arriba de la computadora, un switch electrónico. El sistema SACET opera para equipos que accedan a las centrales como tipo “terminal” y que cuenten con cualquier sistema operativo, por ejemplo Windows o UNIX, FTX, etc., estas pruebas se han desarrollado en ambientes Windows y/o UNIX y FTX. Esta actividad en un principio la realice, actualmente gente del área de administración y del proveedor lo realizan

Aprovisionamiento de centrales aseguradas en SACET. Las centrales que quedan aseguradas por medio de SACET son las que contienen un security-gateway y un switch electrónico instalados y listos para la operación.

Cuando un security-gateway ha quedado instalado, ejecutó un procedimiento setup independiente e individual para cada central, por medio del cual se activan las funciones de seguridad propias. El setup activa el software de seguridad propio del security-gateway, el cual es independiente para cada central y por lo tanto para cada security-gateway. Esta configuración independiente se distingue por medio del nombre CLLI de la central y su dirección IP del puerto de administración del security-gateway local para dicha central.

Es importante considerar que SACET considera a una central dada de alta, como una central lista para su operación, por lo tanto al darse de alta, SACET genera las áreas de trabajo y espacios necesarios e independientes para dicha Central asegurada por el security-gateway.

Adicionalmente SACET inicia un proceso persistente de comunicación con el security-gateway correspondiente a la central dada de alta. Por estas razones es recomendable dar de alta cada una de las centrales en cuanto se haya instalado el security-gateway, el cual debe encontrarse en condiciones operativas normales.
Los usuarios de SACET pueden utilizar Windows 98, Windows 2000 y Windows XP. Los usuarios cuya PC cuente con Windows XP, deberán:

1. Deshabilitar el Firewall de Windows XP (SP2).
2. Reiniciar el equipo
3. Deshabilite el manejador de energía del equipo, hibernación, etc.

Administración. En el sistema SACET manejo dos tipos de administradores: un súper-administrador y un conjunto de administradores regionales. El súper-administrador, en conjunto con los administradores regionales, se encarga de administrar el sistema SACET.

Súper-Administrador: Manejo solo un agente súper-administrador, quien cuenta con todos los permisos y privilegios. Con ayuda de este perfil realizo lo siguiente:

- ✓ Doy de alta a los administradores regionales.
- ✓ Defino regiones a los administradores.
- ✓ Asigno las centrales telefónicas por cada región.
- ✓ Doy de alta y baja centrales de SACET.
- ✓ Respaldo y restore de las centrales

Administradores Regionales: Son un grupo de administradores que se encargan se administrar la seguridad en las centrales que conforman su región. El alcance de un administrador regional está limitado al total de centrales que conforman su región de administración Con ayuda de este érfil realizo lo siguiente.

- ✓ Doy de alta usuarios
- ✓ Doy de alta comandos limitados y permitidos
- ✓ Reviso log's y reportes de las centrales de la región.

Nota: el administrador regional deberá recibir del súper administrador la central ya configurada con las IP asignadas por RCDT. Ya que dentro del sistema operativo "NO" cuenta con privilegios para levantar tareas que son parte del manejo de la seguridad de la central.

Operación del SACET-GESTOR

Para iniciar la sesión en el SACET-GESTOR ingreso al servidor y se presiona el icono 

ubicado en el escritorio, este acceso lo controlo yo y casi siempre soy el único que entra al menos que se tenga que ver cosas con el proveedor le otorgó dicho acceso. Al invocarse se activará la pantalla de bienvenida, se tendrá que indicar el nombre de usuario y contraseña para así poder acceder al listado de centrales; este usuario y password es proporcionado de acuerdo a su región y con la autorización correspondiente de alguno de mi grupo de trabajo o del líder usuario, cabe mencionar que solo lo podrán operar administradores de cada región (administradores regionales) y gente de soporte (administrador) así como gente que autoricé el líder usuario.

Sesión de SACET-GESTOR permanentemente activa. Es importante mencionar que siempre tengo una sesión de SACET-GESTOR permanentemente activada. Esta sesión me sirve y me ayuda para la visualización de alarmas, pero más para complementar procesos que se llevan a cabo en tiempo real, por ejemplo: paso automático a directo en alguna central. Cambio de dirección IPs para los reportes de RANT SUCORT comandada por un comando 5826 para cambio de direcciones de reportes a una central, etc.

Listado General de Centrales.

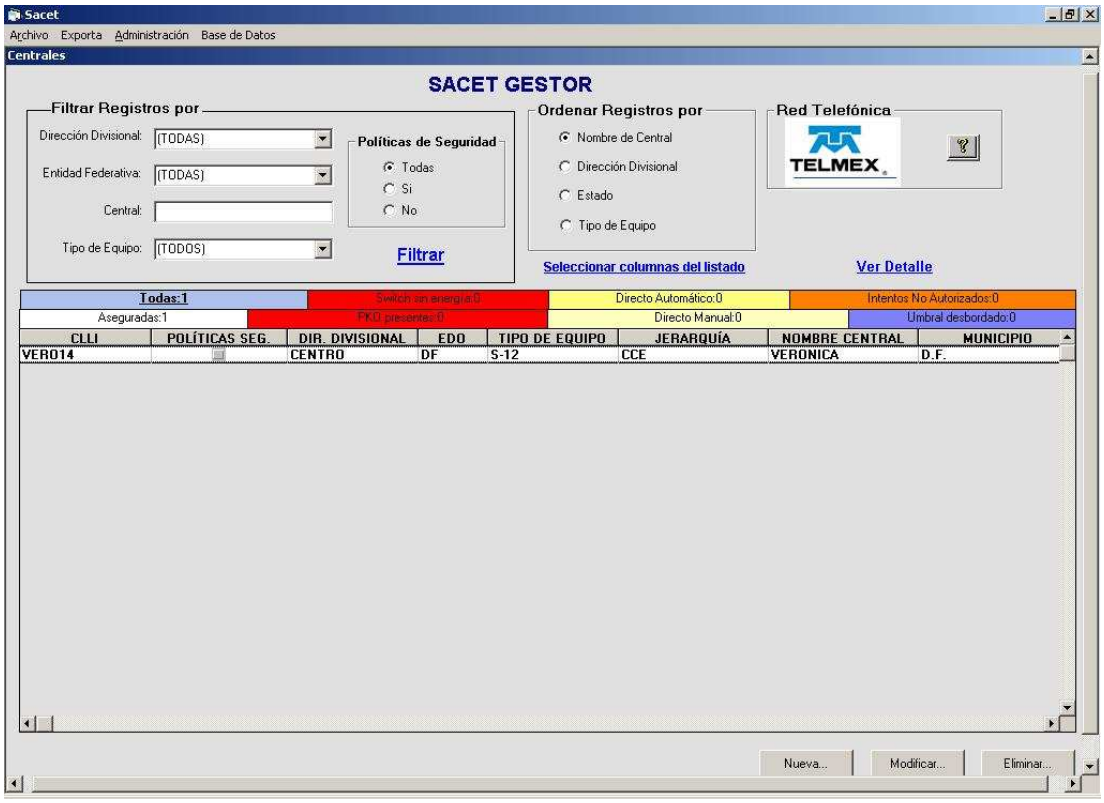


Figura 1.2 Listado General de Centrales

El listado general de centrales cuenta con un menú principal en la parte superior en el que se tiene acceso a los siguientes sub-menús:

Archivo: Este menú cuenta con la función “salir”, la cual permite abandonar el programa.
Exporta: Este menú me permite exportar el listado de centrales a documento de Word y a hoja de calculo Excel en caso de que sea necesario.
Administración: Únicamente yo como super-administrador tengo acceso a este menú en el cual define los parámetros para la administración de SACET, contando con las siguientes opciones:

Administradores Regionales: En esta opción solo yo como administrador puedo dar de alta a los administradores regionales, tal y como se ilustra en la siguiente pantalla.

Figura 1.3 Catálogo de Administradores

En esta pantalla realizo altas, bajas y cambios con los administradores regionales ingresando los datos correspondientes tales como: Nombre, login, contraseña, etc. El botón de liberar, sesión me ayuda a eliminar sesiones de usuarios que hayan dejado abierta su sesión o por error de sistema se haya quedado abierta.

Regiones: Al elegir esta opción dentro del menú de administración, aparece el catálogo de regiones, que incluye todas las posibles regiones que pueden ser administradas por SACET. En catálogo es donde me permite administrador del sistema crear, modificar o borrar una región.

Figura 1.4 Catálogo de Regiones

Centrales: Al seleccionar esta opción dentro del menú de administración, me sirva para realizar un despliegue del listado total de centrales aseguradas por SACET y así realizar un mejor monitoreo del servicio.

Base de datos: Este menú cuenta con las siguientes opciones y lo ocupo para realizar respaldos y/o restauración de datos:
Respaldar estructura: La estructura se refiere a todas las tablas que se manejan en la base de datos y se muestran en formato texto. Al seleccionar la opción "respaldar estructura" aparece la ventana para guardar dicho respaldo en la que debe indicarse el nombre del archivo con extensión (*.sql), aunque el archivo se podrá abrir en cualquier editor de texto.

Respaldar datos: El respaldo de los datos se refiere a todos los datos que se cargan en las tablas como son centrales, usuarios, equipos, así como las carpetas del sistema referentes a las centrales. Al seleccionar la opción "respaldar datos" aparece la ventana para guardar dicho respaldo en la que debe indicarse la ubicación donde se desea guardar el respaldo.

Restaurar datos La restauración de los datos se refiere a todos los datos que se cargan en dichas tablas como son centrales, usuarios, equipos, así como las carpetas del sistema referentes a las centrales. Al seleccionar esta opción aparecerá una pantalla para seleccionar la ruta y el nombre del respaldo que se va a restaurar y en la parte superior de la pantalla una barra de avance del proceso que indica el término de la restauración. Una vez que hago esto se necesita reiniciar el gestor por lo que tengo que coordinar con la diferentes áreas involucradas para realizar esto así en caso de que no se restaure bien algunas centrales volver a darlas de alta.

Estatus de la central: A través de este Listado, tengo una visibilidad del estatus general de cada una de las centrales telefónicas, existiendo dos tipos de alarmas

para indicar que es necesaria la intervención ya sea de parte de nosotros o de alguna otra área para su atención. Este estatus se actualiza cada 30 segundos.

En el Listado General de centrales, las centrales pueden aparecer en cinco tonalidades distintas.

Alarmas en color rojo: En color Rojo se muestran las Centrales que presentan alguna de las siguientes fallas:

- Alguno de los puertos está fallando (**Pko**)
- El Switch no cuenta con energía.

Alarmas en color amarillo: En color amarillo se muestran las centrales que se encuentran en modo directo, pudiendo haberse realizado la conmutación en forma manual o automática.

Estado “directo”: El switch electrónico conmuta ya sea por causas atribuibles al usuario (manual, es decir, que el usuario concientemente mando el comando para realizar el paso) o por fallas en el sistema (automático, es decir, por alguna perdida de comunicación el sistema ordeno el paso), y hay un acceso directo a la central. En este momento se sigue teniendo acceso a la central pero no se cuenta con seguridad, únicamente se cuenta con un log de eventos en el que se puede evaluar qué usuarios entraron y qué hicieron sobre la central telefónica en el periodo de tiempo en el que se estuvo en estado directo.

Alarmas en color naranja: En color naranja se muestran las centrales a las que se intenta entrar de modo no autorizado. Esta alarma aparece cuando en un lapso de 1 minuto un usuario no autorizado ha intentado acceder a la central a través de un mismo puerto como mínimo 3 veces. La alarma permanece por un periodo de 3 minutos en el listado general de centrales. Si se desea observar el detalle de la alarma, es necesario tomar la hora en que se presenta la alarma y abrir la bitácora de accesos no autorizados.

Alarmas en color morado: En color morado se muestran las centrales que se encuentran con desbordamiento de umbral, esto quiere decir que algún usuario de la central ha sobrepasado el número tope de envío de comandos no permitidos, que fue definido por el administrador en el panel de resumen general de la central.

Centrales en color blanco: En color blanco se muestran las centrales que se encuentran en estado asegurado y no presentan ninguna falla. El número de centrales de este tipo es contabilizado en el contador correspondiente.

Layout del archivo bitácora de cambio a asegurado: El archivo **SG_ScriptBita.txt**, contiene 4 campos separados por coma los campos son.
Fecha y hora del cambio de dirección IP,

SCROXaY.TXT.- Indica cambio de dirección IP de X a la Y.
True/False.- Indica si que el cambio fue Exitoso.
True,False.- Indica si apareció un mensaje de cambio No exitoso.

Cuando se realiza un cambio de dirección exitoso se debe mostrar la Fecha y Hora, SCROXaY.TXT, True, False.
Ejemplo: **04/05/2006 11:19:44,SCRO8a23.TXT,True,False**

Cuando se realiza un cambio de dirección No exitoso se debe mostrar la Fecha y Hora, SCROXaY.TXT, False, False.

O cualquier otra combinación diferente a la exitosa.

Criticidad de Fallas.

Cuando una central presente alguna situación por la que deba contar con dos tonalidades de alarma, se dará la siguiente prioridad:

Prioridad 1: Alarmas en color rojo
Prioridad 2: Alarmas en color amarillo
Prioridad 3: Alarmas en color naranja
Prioridad 4: Alarmas en color morado

Visualización de la información en el listado general

Filtrado de registros: El listado general cuenta con 4 tipos de combos que los utilizo para seleccionar una central y que me permita hacer una búsqueda eficiente de la misma. Estos combos son los siguientes: dirección divisional, entidad federativa, central, tipo de equipo, filtrado por políticas de seguridad.

Movimientos sobre Centrales. Alta de centrales

Prerrequisitos: Antes de declarar una nueva central en el SACET-GESTOR, es importante que el security-gateway y el switch electrónico se encuentren instalados y con conexión hacia la central telefónica. El estatus de security-gateway instalado debe ser:

1. El security-gateway local debe de estar instalado al igual que el switch electrónico, y conectado a la central telefónica.
2. EL security-gateway debe estar apagado.
3. El switch electrónico debe estar alimentado a la energía.
4. En este estado el security-gateway reconoce que la central se encuentra en formato de directo.
5. Una vez que se tiene acceso a la central, éste es en modo directo.

Para dar de alta una nueva central en el SACET-GESTOR, hago los siguientes pasos:

1) Acceso al SACET-GESTOR.
2) Acceso al “Listado general de centrales”.
3) Selecciono la opción de “nueva”: En esta plantilla, declaro todos los campos indicados. La plantilla contiene campos obligatorios y campos complementarios no obligatorios. El “campo obligatorio” en esta plantilla es el nombre de la Central. Este campo acepta un máximo de 20 caracteres alfanuméricos, excepto los siguientes: (/ : * ¿ “ > < |) y caracteres especiales. El resto de los campos en esta plantilla son campos complementarios no obligatorios.

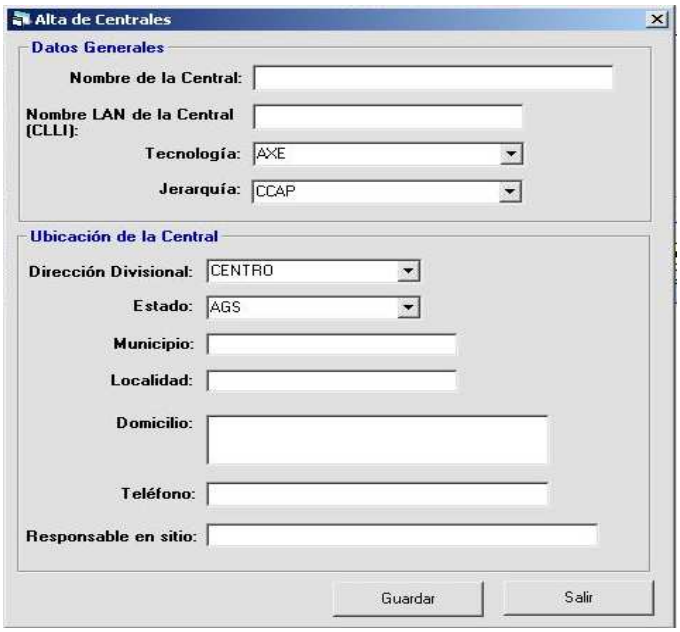


Figura 1.5 Plantilla de Alta de Centrales.

Configuración General de Central.

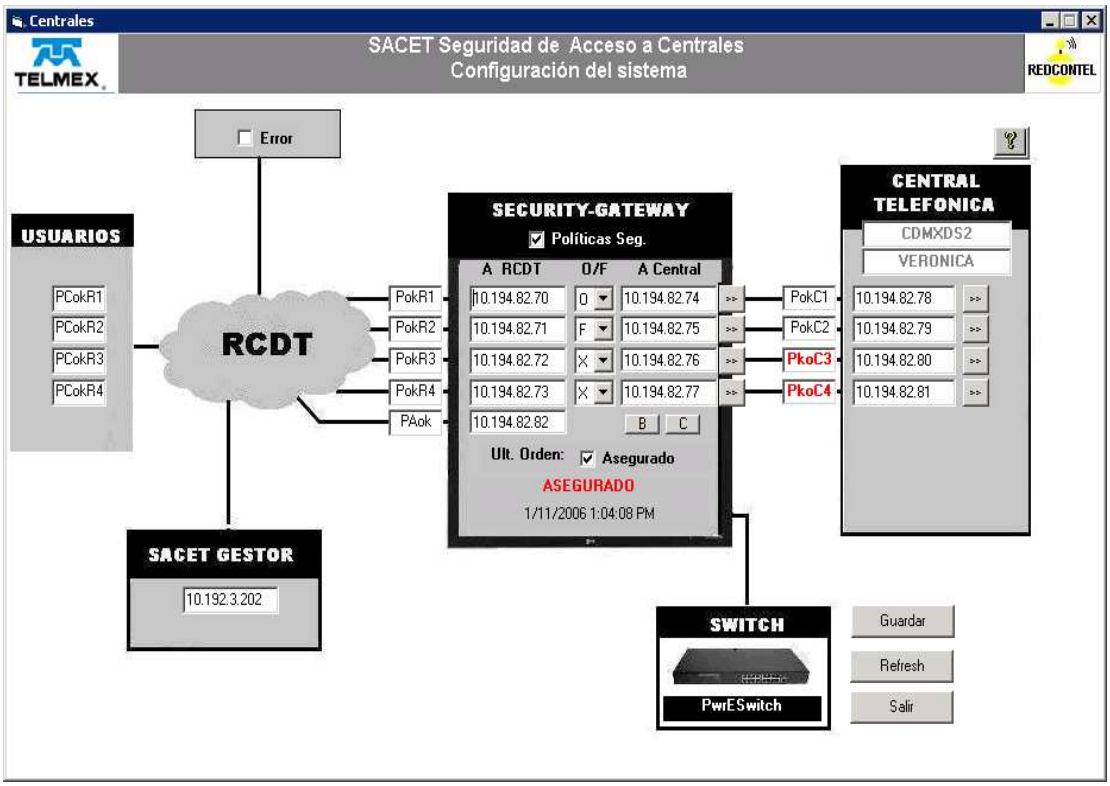


Figura 1.6 Pantalla de Configuración General

Direcciones a RCDT: Es un campo obligatorio, presenta un juego de 4 direcciones IP del security-gateway hacia RCDT, para cada uno de los puertos (4 puertos ethernet). Estas direcciones corresponden a las direcciones originales de la central a asegurar.

Direcciones A Central: Es un campo obligatorio, presenta un juego de 4 direcciones IP del security-gateway hacia la central, para cada uno de los puertos (4 puertos ethernet). Estas direcciones corresponden a las direcciones asignadas por la RCDT del security-gateway a la central telefónica.

Dirección IP del puerto de administración: Es un campo obligatorio y corresponde a la dirección IP designada por RCDT para el security-gateway. Si se requiere cambiar este campo, es necesario seguir el procedimiento correspondiente.

Puertos O/F: Es un conjunto de 4 campos obligatorios, los cuales tienen un valor por omisión que es “X”. Estos campos sirven para especificar el tipo de puerto de Central, siendo los tipos de Puerto los siguientes:
O: Puerto de Operación & Mantenimiento.
F: Puerto de Facturación.
X: Puerto fuera de servicio.

Direcciones de reportes: En el campo de direccionamiento de reportes, la dirección se especifica con "&", en lugar de ".", esto es debido a que SACET se ajusta al formato especificado en la central para el envío de tales campos a su dirección destino. Por ejemplo, para especificar la dirección 10.192.11.203 como dirección del servidor destino, se debe especificar el valor de: 10&192&11&203.

Direcciones de central: Son campos obligatorios. Presenta un juego de 4 direcciones IP de la central, para cada uno de los puertos (4 puertos ethernet), estas direcciones corresponden a las direcciones asignadas por la RCDT a la central, como direcciones aseguradas.

NA: Es un campo obligatorio y se declara presionando las flechas a la derecha del campo de dirección IP para los puertos de la central. Estos valores se declaran para cada uno de las direcciones o puertos IP de la central. Los valores típicos son:

Puerto Ethernet	Valor de NA	Valor a configurar en SACET
1	H'C	C
2	H'D	D
3	H'22C	22C
4	H'22D	22D

LCEID: Es un campo obligatorio y se declara presionando las flechas a la derecha del campo del campo NA para los puertos de central. Estos valores se declaran para cada una de las direcciones o puertos IP de la central. Los valores típicos son:

Puerto Ethernet	Valor de LCEID	Valor a configurar en SACET
1	H'0	0
2	H'10	10
3	H'80	80
4	H'90	90

Verificación de procesos al dar de alta una Central

Cuando se ha dado de alta una nueva Central y se han configurado sus parámetros obligatorios, es necesario revisar en el programador de tareas que se hayan dado de alta dos procesos (demonios). Estos procesos permitirán al SACET monitorear a los puertos ethernet del security-gateway y hacer una recuperación a modo directo cada vez que se requiera. Estos programas se encuentran en la carpeta C:\SISA-CCS\CCLI-CENTRAL\Exportacion\, estos programas son: 1-. MACC 2-. SyncPuertos

Datos de Seguridad de la Nueva Central

Con el alta de una central también doy de alta los datos administrativos de la seguridad del security-gateway. Los datos que se deben recabar son:

- Configuración de equipos.
- Configuración de usuarios.
- Configuración de perfiles de comandos permitidos.
- Configuración de perfiles de comandos limitados.

Baja de Central: Para dar de baja la central, selecciono la opción eliminar en el listado general de centrales. Cuando se realiza el proceso de baja de central, se pierde la configuración de conectividad y la configuración de seguridad (usuarios, equipos, perfiles, etc.), por tanto existe un procedimiento para respaldar dicha información para utilizarla como apoyo en el alta de la nueva central.
El procedimiento es el siguiente:

1. Hago un respaldo de la carpeta correspondiente a la central que desea eliminar. Este respaldo consiste en hacer un “copy” de la carpeta en cualquier localidad del disco duro.
2. Una vez realizado el respaldo se puede proceder a eliminar la central.
3. Dentro de la carpeta de central (que tiene asociado el CLLI como nombre), se encuentran siete sub-directorios que contienen la siguiente información:
    a. Accesos no autorizados
    b. Histórico de accesos
    c. Log de eventos
    d. Estatus: Esta carpeta contiene la última configuración en la que se encontraba el security-gateway.
    e. Importación
    f. Exportación: En esta carpeta se concentran los archivos con la información del security-gateway, siendo estos archivos los siguientes:
        SISA_usuarios
        SISA_perfiles
        SISA_perfilescomlimitados
        SISA_direcciones
        SISA_configuracion
4. Para cargar estos datos a la nueva Central con el nuevo CLLI, abro dichos archivos y cargo cada uno de sus datos de forma manual.

Cambio de CLLI de una central: Para cambiar el CLLI de una Central en el SACET-GESTOR**,** realizo lo siguiente:

1. Accedo al SACET-GESTOR
2. Accedo al “listado general de centrales”.
3. Selecciono la central a la que va a cambiar el CLLI.
4. Doy clic en la opción de “Modificar”.

A continuación se abrirá la plantilla de alta de centrales y solo deberá cambiar el por el nuevo nombre. Una vez que se hace este cambio se abrirá una pantalla negra indicando los pasos que se están ejecutando, sigo las indicaciones y continuo con el proceso, al final realizo una exportación para que tome bien los cambios.

Análisis y Metodología

Soporte técnico SACET incluye de manera general lo siguiente:

1. Contesto llamadas de usuarios de **SACET** a nivel nacional.
2. Solicito información básica al usuario relacionada al problema reportado.

- Registro la llamada en el sistema de soporte técnico de seguimiento de incidentes.
- Doy seguimiento y resuelvo problemas del sistema y/o el usuario tenga.
- Para problemas relacionados a la WAN, soy responsable y tengo la obligación de dar seguimiento hasta su solución con la RCDT documentando su solución.

3. De acuerdo a la severidad o impacto del problema, tengo la obligación de notificar y escalar el problema a las entidades correspondientes (internas y externas) así como enviar en caso de que aplique la notificación de no atención cada cierto tiempo.
4. Género y envío a través del correo, el reporte de operación semanal del proyecto.
5. Junto con el proveedor damos seguimiento a aquellos casos que no estén identificados en las tipificaciones de SACET y para los cuales no exista una instrucción previamente documentada hasta encontrar e identificar el origen del problema y solución.

Solución ante contingencia. De acuerdo con los problemas que se han tenido he llegado a clasificar soluciones cuando se tiene alguna contingencia las cuales tratare de explicar en lo que sigue:

Contingencias en el security-gateway.
Falla en puertos del lado de central: Bajo operación normal del security-gateway (modo asegurado), algunos de los puertos de seguridad son desconectados o hay alguna falla momentánea de la RCDT; bajo este escenario ocurrirán varias respuestas del sistema de acuerdo a las políticas de conmutación del lado de central definidas por Telmex, dichas políticas definen bajo qué escenarios la central se quedará en estado directo o en estado asegurado según sea el caso. Estas políticas son:

1) Cuando alguno de los puertos denotados como P&L (operación y mantenimiento) falle, debe conmutar a estado directo.
2) Cuando ambos puertos de facturación falle, debe conmutar a estado directo.
3) Si se pierde el puerto de administración debe mantenerse el estado Asegurado.

Bajo ninguna otra circunstancia imprevista el sistema debe conmutar, o en todo caso, que esta conmutación sea comandada por el SACET-GESTOR por orden del administrador a cargo (conmutación manual).

Respuestas del sistema ante las eventualidades ya mencionadas

	PROBLEMA	a) RESPUESTAS DEL SISTEMA
1	Puertos de operación (al menos uno)	**1.** El sistema conmutara y el gestor dará aviso de ello mediante una alarma en el listado general de centrales, (central en color rojo por Pko). **2.** En el listado general de centrales se actualizará el contador de puertos Pko. **3.** En el panel de configuración, el puerto que se encuentra fuera de servicio es mostrado en color rojo **PCko**. **4.** En el panel de configuración, se mostrará la leyenda de acceso directo, en color rojo.
2	Un Puerto de facturación falla.	**1.** El sistema no hace ninguna conmutación. **2.** El sistema notificará de ello, mostrando una alarma en color rojo en el listado general de centrales (central en color rojo por Pko). **3.** En el listado general de centrales se actualizará el contador de puertos Pko. **4.** En el panel de configuración, el puerto que se encuentra fuera de servicio es mostrado en color rojo **PCko**. **5.** En el panel de configuración, se mostrará la leyenda de acceso asegurado, en color rojo.
3	Todos los puertos de facturación fallan.	**1.** El sistema conmutara y el gestor dará aviso de ello mediante una alarma en el listado general de centrales, (central en color rojo por Pko). **2.** En el listado general de centrales se actualizará el contador de puertos Pko. **3.** En el panel de configuración, los puertos que se encuentran fuera de servicio son mostrados en color rojo **PCko**. **4.** En el panel de configuración, se mostrará la leyenda de acceso directo, en color rojo.
4	El puerto de administración falla.	**1.** El sistema no hace ninguna conmutación. **2.** El sistema notificará de ello, mostrando una alarma en color rojo en el listado general de centrales (central en color rojo por Pko). **3.** En el listado general de centrales se actualizará el contador de puertos Pko. **4.** En el panel de configuración, el puerto de administración es mostrado en color rojo **PAko**. **5.** En el panel de configuración, se mostrará la leyenda de acceso asegurado, en color rojo.

Falla del lado de la RCDT:

1. Puerto del switch de RCDT.
2. Problemas de cableado.
3. Puerto del security-gateway.

Bajo estos escenarios la política de conmutación definida por Telmex es:

Cuando se presente una falla del lado de RCDT no se debe efectuar ninguna conmutación.
Excepción: Cuando SACET-GESTOR perciba que los puertos de acceso al security-gateway han quedado fuera de servicio y además haya perdido la comunicación con dicho security-gateway, es decir que haya perdido el contacto con su puerto de Administración, entonces el SACET-GESTOR sí comanda la conmutación a directo, esto se debe a que, bajo su perspectiva el security-gateway ha quedado fuera de servicio.

Cuando se presente la falla se mostrará en el listado general de centrales una alarma en color rojo para que ésta pueda ser atendida y dependiendo del tipo de falla, se podrá hacer una conmutación en forma manual.

Cuando se presente una falla momentánea de red o de comunicación en el extremo de la central, el sistema no se verá afectado y tampoco ningún proceso que estuviese corriendo. Esto se debe a que el sistema cuenta con reloj en cada uno de sus puertos en el que registra cuánto tiempo se ha estado sin conexión con la central y si este tiempo es superior a 5 minutos, entonces es cuando el sistema opera de forma emergente pasando a un estado directo siguiendo sus políticas de conmutación.

Falla en puerto de administración. Bajo operación normal del security-gateway (modo asegurado), el puerto de administración del security-gateway queda fuera. Cuando existe una falla de comunicación en RCDT o el puerto de administración del security-gateway esté dañado, el sistema no debe conmutar, pero si debe hacer un registro en alarmas de dicho suceso. Como este puerto va directamente al equipo (switch) de RCDT se puede detectar la falla rápidamente. Al realizar el gestor transferencias de información hacia el security-gateway, el gestor las pondrá en cola de espera, y se llevarán a cabo hasta el próximo restablecimiento del puerto. Mientras tanto el security-gateway sigue trabajando correctamente, es decir, no se pierde en ningún momento la seguridad de la central. Para poder detectar esto es necesario ingresar en el panel de configuración de central y comprobar que la etiqueta correspondiente al chequeo de su puerto se encuentre activa, esta etiqueta reporta la comunicación administrativa entre el gestor y el security-gateway. De otro modo significa que el gestor no tiene comunicación con security-gateway.

Reinicio de la PC

Contingencia en donde la PC se reinicia. Esta falla puede deberse a diferentes circunstancias tales como:

1) Problema de inestabilidad del Sistema Operativo.
2) Problema de Hardware.
3) Por causas de mantenimiento.

Falla del security-gateway: Falla de energía. Se apaga inesperadamente por una falla de energía. Cuando la central se encuentra en estado asegurado y todo el sistema se encuentra en estado operativo correcto, existe la posibilidad de que el security-gateway se quede sin energía eléctrica, cuando esto sucede el sistema realizará lo siguiente:

El gestor notificará la falla y se realizará una conmutación automática a modo directo y además muestra una alarma en el listado general de centrales en donde dicha central aparece en color rojo.

Acciones que tomo: Una vez que la PC esta en estado directo, procedo a su revisión y mantenimiento. En caso de que presentarse un corte de energía eléctrica en el equipo security-gateway, provocando un apagado repentino, SACET pasará a la central al modo directo. Una vez recuperada la energía en el security-gateway, y antes de regresar al estado asegurado, es importante que ejecute un procedimiento necesario para la verificación del estado funcional correcto del disco duro del equipo security-gateway, para detectar una corrupción de datos y afectación física en el disco provocada por el apagado.

Cuando el security-gateway esté en condiciones operativas satisfactorias, listo para ser reactivado después de haber revisado y darle su mantenimiento, entonces procedo a pasarlo a asegurado. Estas condiciones incluyen una comprobación de los puertos ethernet hacia la central, hacia la RCDT y el de administración los cuales deben estar operando correctamente.

No se puede efectuar la conmutación. Existen dos casos en los que el sistema puede no permitir una conmutación de modo directo a asegurado:

Cuando no haya puerto de administración. En este caso la respuesta del sistema será, “No existe puerto HBL, no se puede conmutar”.
Cuando la PC se encuentre apagada o con algún problema de energía, dará el mismo mensaje.

Para corregir el problema accedo de forma remota y levanto el puerto de administración. En caso de que el puerto de administración esté funcionando correctamente, es necesario ir a sitio para revisar la PC.

Falla en la red durante la conmutación. Para esta contingencia de comunicación no se verá afectado el proceso de conmutación, porque el sistema esta diseñado de forma cíclica, lo que permite que aunque en un determinado momento se presente un corte de comunicación y el proceso sea detenido, el sistema lo volverá a intentar en cuanto haya un restablecimiento del enlace.

Virus o inestabilidad de sistema operativo. Si por alguna circunstancia no prevista el sistema operativo queda inestable, el software security-gateway de igual manera también se hace inestable, por tanto el gestor lo identifica y realiza una conmutación automática.

Contingencias en el switch electrónico

Falla de energía en el switch electrónico en modo asegurado. Bajo este esquema de asegurado, se considera un caso no crítico y este problema es alarmado por SACET-GESTOR con una alarma en el listado de central en color amarillo y dentro de la configuración de central este es identificado por la etiqueta correspondiente a esta variable, denotada como (PwrESwitch), lo que indica que el switch electrónico no tiene problemas de energía y si la etiqueta es (switch sin energía), indica que el switch fue desconectado o hubo un daño en su fuente de alimentación. No sensando switch. Nos indica que el switch no manda señales de presencia puede deberse a que el PAD se desconecto o esta fallando.

Falla de energía en el switch electrónico en modo directo. Cuando ocurre esta situación es un caso grave, debido a que la central se encontraba en modo directo y se pierde la comunicación total con la central, el gestor se entera de ello por que se pierden sus 4 puertos monitoreados (PCok1, PCok2, PCok3, PCok4) y por tanto no hay accesos. La única solución a este problema es conmutar a asegurado.

Desconexión del puerto serial. Desconexión del puerto serial de sincronización con la pc. Ante esta situación si el sistema se encuentra en modo Asegurado, tras desconectarse el serial del switch, éste queda sin comunicación con el security-gateway, y de esta forma el switch conmuta, lo cual es un problema grave, por que RCDT se quedara sin comunicación con la central.

Antes de pasar a asegurado: es importarte verificar que se cumplan los requisitos funcionales del sistema, esto requisitos son:

- Los puertos del security-gateway hacia la central deben operar correctamente y estar habilitados.
- Los puertos del security-gateway hacia la RCDT deben operar correctamente y estar habilitados.
- Los puertos ethernet de la central deben estar operando correctamente.
- Los puertos ethernet de la RCDT deben estar operando correctamente.
- Todos estos puertos deben estar conectados correctamente en el switch electrónico SWE.

Puertos enmascarados, procedimiento de recuperación. Este problema se origina si estando en formato de operación directo, se usan cualquiera de los 4 puertos ethernet y a estos puertos se les declara en la central su dirección asegurada, por lo tanto se publicarán en la RCDT dichas direcciones aseguradas. Si estando en esta condición se solicita un cambio a asegurado al security-gateway, como resultado, se realizará el cambio de todas las direcciones aseguradas en la central, pero dejará enmascarados los puertos hacia la RCDT, quedando sin acceso dichos puertos.

Para resolver este problema acceso en forma remota a la pc del security-gateway, con la ayuda de la herramienta “conexión a escritorio remoto”, se selecciona dentro del “panel de control”, la opción “conexiones de red”. Para cada uno de los 4 puertos del security-gateway a la RCDT, se procede a cambiar la dirección 15.x.x.x a la dirección real correspondiente, por ejemplo a las direcciones 10.x.x.x. esto se repite para los 4 puertos denominados PR1, PR2, PR3 y PR4, como se muestra en la siguiente figura:

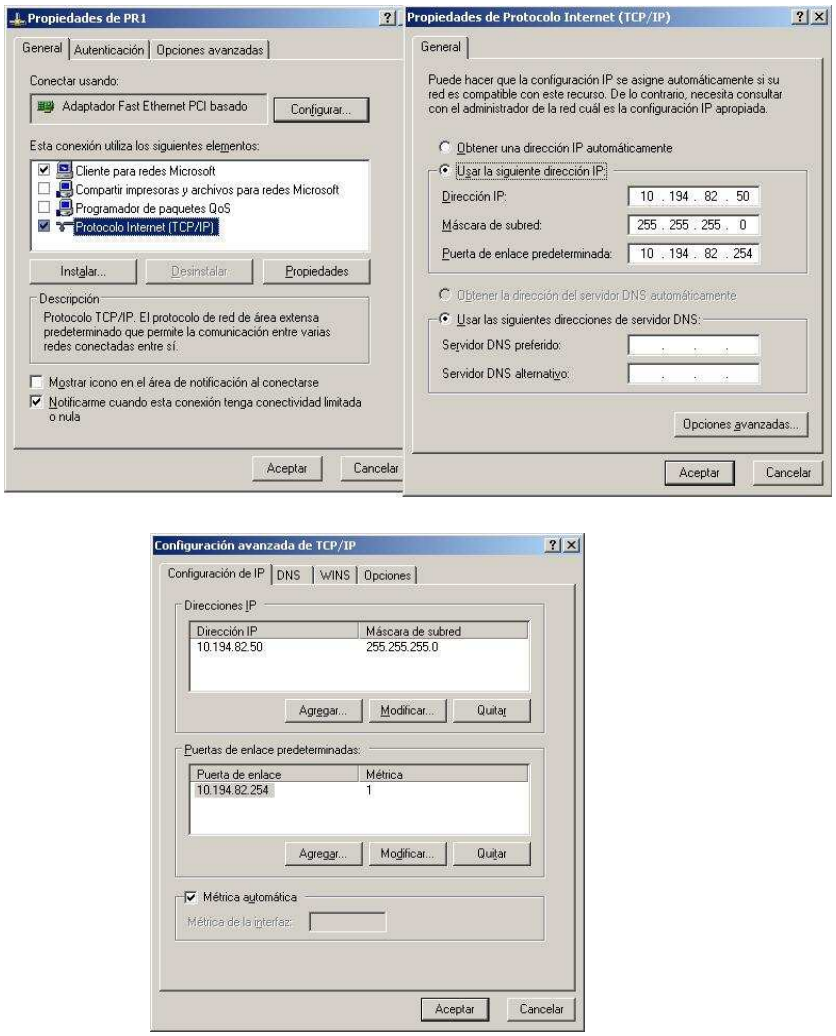


Figura 1.7 Ejemplo de Configuración de interfaz PR1. Proceso de desenmascaramiento de puertos.

Archivos corruptos. En caso de que algún o algunos archivos se corrompan por las situaciones de contingencia lo único que hago es copiar de la carpeta de instalación los archivos ejecutables o los archivos que se hayan dañado. Para copiar archivos *.txt o *.bat, solo se selecciona de la carpeta instalación y se copian a la carpeta de security-gateway, después realizo una exportación para que se actualicen.

Para restablecer archivos *.exe, primero detengo todas las tareas para que no se este ejecutando dicho archivo y se verifico que no este en uso en el administrador de tareas del security gateway, una vez hecho esto selecciono el archivo dañado y lo borro, copio de la carpeta instalación el archivo antes borrado, para terminar la restauración de dichos archivos reinicio la maquina y realizo una exportación.

Problemas en RCDT

Cuando ocurre una falla en un puerto del security-gateway a la RCDT, el security-gateway se percata del problema, pero no puede diagnosticar la causa del mismo, pudiendo ser el puerto del router que entrega la conexión al security-gateway, el puerto del security-gateway o el cableado. Para ello realizo lo siguiente:

- Realizo un acceso remoto al equipo security-gateway.
- Verifico las interfaces de los puertos, que se encuentren “Con conexión habilitada”.

Si por alguna causa se encontrara en estado “Sin conexión”, esto podría deberse a alguna de las siguientes tres causas:

Que la falla sea del puerto de la tarjeta del security-gateway.
1) Doy un reset a dicho puerto (Deshabilito – Habilito).
2) Doy un reset a nivel hardware (Deshabilito/Habilito en el administrador de dispositivos del sistema de Windows).

Que la falla sea del Cableado.
Que la falla sea del Switch de RCDT.

Para estos últimos casos podría requerirse ayuda del departamento de RCDT e ir directamente a Sitio a revisar los equipos, cualquiera de los casos contacto a la gente de dicha área y revisamos.

- Si las conexiones se encuentran en estado activo – habilitado, entonces se puede deber a un problema lógico por un problema del sistema operativo o por daño de la tarjeta. Por lo que ahora compruebo que la configuración del puerto sea la misma que la mostrada en la pantalla principal de configuración del security-gateway. Es decir:

La configuración del puerto debe tener Métrica 1, firewall únicamente con permisos de Telnet, FTP y eco entrante.
Verifico la transmisión y recepción de paquetes enviados (debe ser más paquetes enviados que recibidos).
Habilito y Deshabilito el puerto.
Si no se eliminó el problema Reinicio el Equipo.
Si ya que se ha reiniciado el equipo se presenta el mismo problema debo coordinarme con la gente correspondiente y dirigirnos a sitio a revisar el equipo.

Cuando se tienen problemas de comunicación entre los Heart-Bit, reinicio el o los programas de Heart- Bit. En el security gateway o en el gestor.

Reiniciando HBL. (Security Gateway): Para reiniciar este programa, es primero detengo en tareas programadas la que se llama SISA_Fija, esta tarea revisa y en caso de que haya alguna tarea detenida la volverá a levantar, en seguida detengo la tarea llamada HBL. Una vez que se haya detenido la tarea HBL, ahora detengo el programa ya que se esta ejecutando en background llamado SG-HB.exe. Ejecuto nuevamente del programador de tareas la tarea llamada HBL, o en caso de que se requiera dejo nuevamente en background y reinicio el equipo.

Reiniciando HBC (gestor): Para reiniciar este programa término la tarea HBC en el programador de tareas y a su vez se detendrá el Programa HBMC2.exe. Una vez hecho esto solo vuelvo a ejecutarla desde el programador de tareas.

CONCLUSIONES

SACET es un sistema gestor de seguridad para centrales telefónicas que asegura, en su primera fase, la conectividad a centrales S1240 por puertos ethernet. El proyecto SACET funcionalmente cuenta con las siguientes características para el acceso seguro a las centrales:

- Monitoreo de comando de acuerdo a perfiles de usuarios.
- Autentificación de usuarios
- Elaborar bitácoras de actividades (se guardará los comandos ejecutados y los rechazados)

La primera fase del proyecto SACET solo incluye a las centrales S1240 vía puertos ethernet, el acceso por conexiones sincronías y asíncronas no están contempladas dentro de este documento. Es importante mencionar que el proyecto SACET es una parte del proyecto global de seguridad a las centrales.

SACET está instalado en un servidor Stratus redundante, tolerante a fallas, que asegura en un 99.999 una disponibilidad continua. El modelo del servidor es ftServer 5600 y al ser redundante, cuenta con todos sus componentes duplexados trabajando en espejo, incluyendo al disco duro para garantizar el respaldo de datos. El Sistema está equipado con una unidad de cinta modelo SDLT600 para respaldo de la base de datos y sistema operativo.

El security-gateway corre en una PC HP Modelo DC 7100 y no cuenta con redundancia a nivel de HW. Sin embargo, cuenta con un proceso que permite no perder la funcionalidad operativa de acceso a la central en caso de falla, en el que detallo a continuación:

El security-gateway cuenta con un switch electrónico cuya misión es censar la funcionalidad correcta de la PC y en caso de falla, interconecta directamente los puertos ethernet de la RCDT a la central telefónica. Inmediatamente el SACET-GESTOR, al determinar la pérdida funcional del security-gateway ejecuta un “script” de comandos en la central para cambiar las direcciones IPs de acceso (por lo que las direcciones del security-gateway son asignadas a la central), actualizando las direcciones de entrega de reportes y alarmas y garantizando que las aplicaciones sigan teniendo conectividad con la central con las mismas direcciones IP. Con ello se logra que aun en caso de emergencia y fuera de servicio del security-gateway no se interrumpa el acceso funcional “desde y hacia” la central telefónica.

El servidor SACET-GESTOR no es un sistema de gestión ya que solo tiene comunicación con los security-gateway para la actualización de las políticas y del perfil de los Usuarios. De acuerdo al modelo de FCAPS se ocupa el rubro de Seguridad (Gestión de Elementos de Seguridad).

Configuración de los servidores:
La única diferencia es en cuanto a capacidad en disco:

Servidor de Pruebas:
1 Procesador Duplexado
2 GB en RAM Duplexados
2 Discos de 80GB Duplexados

Servidor de Producción:
1 Procesador Duplexado
2 GB en RAM Duplexados
1 Disco de 73GB Duplexado
1 Disco de 18GB duplexado

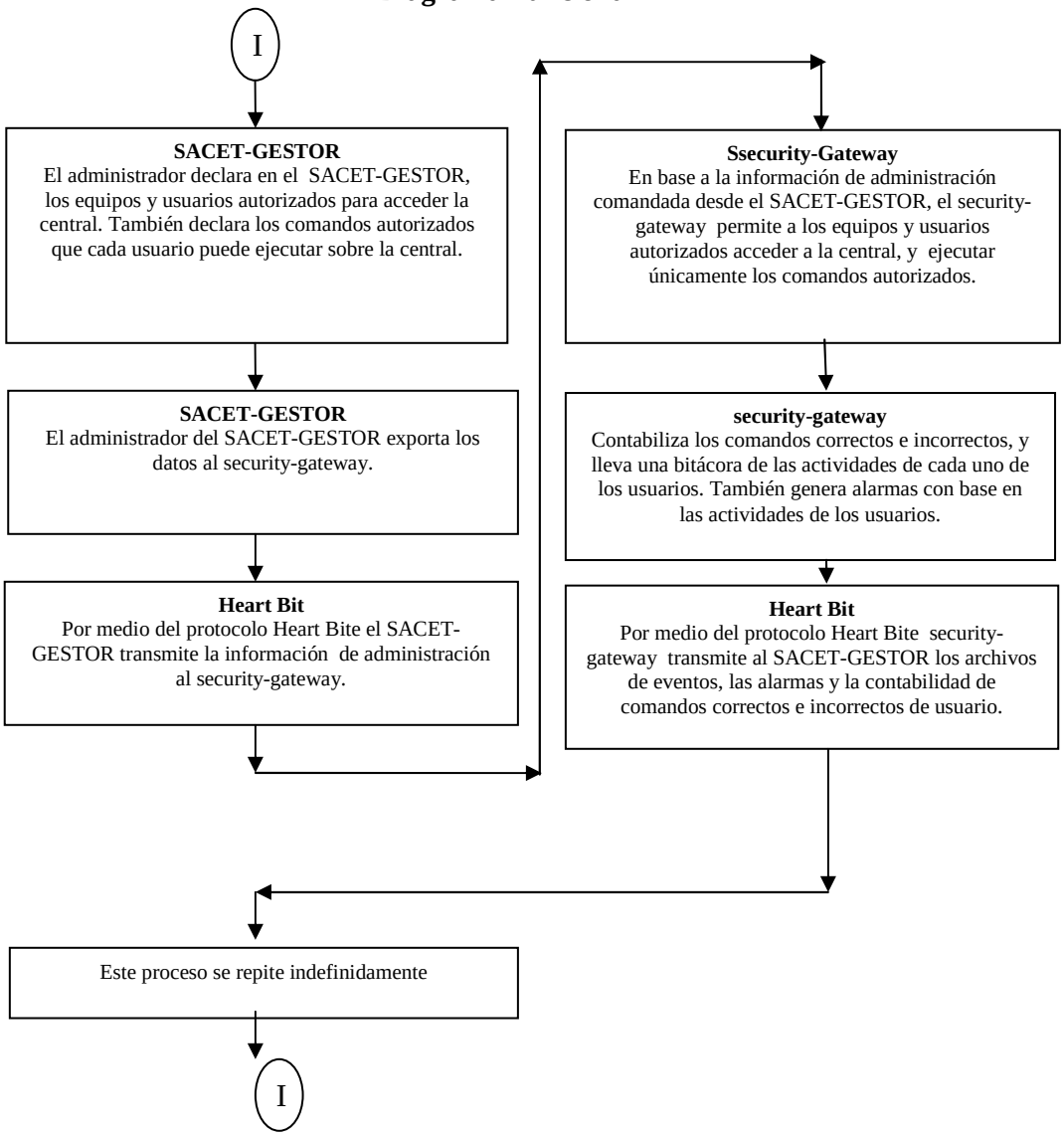
Flujo de tráfico de los usuarios:

- Los usuarios de la central sistema 1240 son las aplicaciones NMA, PISA, PISA QUEJAS, RANT SUCOR, auditoria de servicios y facturación, y algunos usuarios vía Telnet.
- El acceso de estos Usuarios se efectúa a través del security-gateway local, el cual es el elemento de red que autentifica la conexión y aplica las políticas de seguridad que se cargan en el SACET-GESTOR.
- El acceso a la central se restringe debido a que cada usuario solo tiene permitido ejecutar cierto número de comandos en la central, cada usuario que quiere conectarse a la central el security-gateway recibirá su petición y validara su usuario. Una vez en la central solo se permite ejecutar los comandos permitidos para el tipo de usuario y además se tendrá un registro de los comandos ejecutados y de sus respuestas, esto con el fin de saber las actividades realizadas sobre la central.

Flujo de Administración:

- La administración se realiza por medio de SACET-GESTOR, al cual se conectan los clientes de administración remota (administradores). El flujo de acceso de administración entre el administrador remoto y el SACET-GESTOR se realiza por el protocolo TCP/IP. Este flujo lo puedo sintetizar con el siguiente diagrama:

Diagrama Funcional



Podría sintetizar mis actividades como:

- Monitoreo y Mantenimiento del Sacet Gestor (servidor Startus FT 5600), Security-Gateway y centrales mediante la interfaz de Sacet, revisar que se encuentren funcionando correctamente.
- Monitoreo de las centrales y verificar su status con la interfaz Sacet.
- Agregar, mantenimiento y administración de usuarios en la aplicación.
- Agregar y administración de las centrales al Sacet Gestor.
- Monitoreo, optimización y recuperación de procesos.
- Servicio de Helpdesk. Ayuda a los usuarios. Realizar pruebas necesarias para que el sistema funcione correctamente. Resolución de problemas y en ocasiones se trabajo en conjunto con el proveedor debido a problemas con el desarrollo del sistema.
- Realice pruebas de conexión de central con la interfaz de Sacet para poder monitorear dicha central. Verificar que corran todos los procesos necesarios, configuración de puertos, revisión de logs y bitácoras.
- Monitoreo de centrales telefónicas de tecnología S12, FTP y Telnet, es decir, que cualquier usuario pueda realizarlos sin ningún problema estando asegurada la central, desbloqueo de usuarios y verificación de conexiones de los puertos de los Security Gateway.
- Capacitación Interna. Asistí a capacitación para poder dar un mejor servicio con el sistema Sacet.
- Configuración de Security-Gateway, puertos, agregar tareas, desactivar algunas opciones del perfil de seguridad en Windows para su buen funcionamiento.
- Conectar las centrales a la interfaz de Sacet junto con gente del proveedor y las áreas correspondientes de Telmex. Revisión de conexiones, asegurar centrales, revisión de switches, verificar accesos tanto en central como en el servidor antes y después de asegurarlas.
- Mandar los procesos correspondientes para asegurar las centrales así como cuando se requiera quitar dicha seguridad (coordinar con las áreas correspondientes para realizar dicho evento).
- Revisión y monitoreo de direcciones IP a la central, direcciones IP del puerto de Administración (del servidor Gestor), de los puertos de operación y facturación, direcciones de central, direcciones de reportes.
- Di reinicio de tareas y procesos cuando se requiere. Resolución de problemas dependiendo que es lo que el usuario reporta.
- Monitoreo de comando de acuerdo a perfiles de usuarios.

BIBLIOGRAFIA

- Manuales del usuario y soporte técnico del Sistema SACET.
- Documentación del sistema SACET.
- Curso del sistema SACET.

ANEXO

Ethernet: Tecnología popular para redes de área local, inventado por Xerox Corporation. Es un sistema de entrega en el mejor esfuerzo, emplea tecnología CSMA/CD. Xerox Corporation, Digital Equipment Corporation e Intel Corporation desarrollaron el estándar Ethernet de 10 Mbps con cable trenzado (10BaseT)

CSMA/CD: Características del hardware de red que al operar permite que varias estaciones compitan por el acceso a un medio de transmisión escuchando para saber si el medio está ocupado, así como también un mecanismo que permite al hardware detectar cuando dos estaciones intentan transmisiones simultáneas. Ethernet utiliza CDMA/CD.

TCP(Transmition Control Protocol): Protocolo de nivel de transporte TCP/IP estándar que proporciona el servicio de flujo confiable full duplex y del cual dependen muchas aplicaciones. El TCP/IP permite que el proceso en una máquina envíe un flujo de datos hacia el proceso de otra. El TCP está orientado a la conexión en el sentido de que, antes de transmitir datos, los participantes deben establecer la conexión. Todos los datos viajan en segmentos TCP, en donde cada viaje se conoce frecuentemente como TCP/IP debido a que el TCP y el IP son los dos protocolos más importantes.

Telnet: Protocolo estándar de TPC/IP para el servicio de terminal remota. Telnet permite al usuario en una localidad interactuar con un sistema de tiempo compartido remoto como si el teclado y el monitor del usuario estuvieran conectados a la máquina remota.

FTP (File Transfer Protocol): Es un programa que se utiliza para transferir información almacenada en archivos, de una máquina remota a otra local, o viceversa. Para poder realizar esta operación es necesario conocer la dirección IP (o el "nombre") de la máquina a la que nos queremos conectar para realizar algún tipo de transferencia. Es fundamental distinguir entre máquina local y máquina remota:

Registro de Equipo: El registro de equipo es el primer nivel de seguridad, basta con un simple registro o identificación del equipo en el SACET-GESTOR, para que dicho equipo quede reconocido y sea autenticado por el SACET.

Un punto importante a mencionar es que todo equipo que corresponda a cualquier “sistema” que pretenda acceder a la central telefónica, deberá estar registrado; en otras palabras, cada sistema se registra por el equipo de cómputo que lo contiene y por lo tanto por su dirección o en su caso por sus diversas direcciones de acceso, de tal manera que si un sistema se encuentra distribuido en varios equipos, se requiere el registro individual de cada equipo para el acceso global de dicho sistema.

Equipo Autenticado: Es cualquier equipo en la red de Telmex, que requiera acceso a las centrales telefónicas, para cualquier usuario que acceda por medio de dicho equipo y que dicho equipo esté marcado como “equipo autenticado” con lo cual, el sistema SACET solicitará a cualquier usuario (humano o automático) su contraseña individual de usuario al momento de pretender acceder a cualquier central en la red de Telmex, estas contraseñas o claves de acceso son individuales y particulares para cada usuario.

Equipo NO Autenticado: Equipo “no autenticado” es cualquier equipo en la red de Telmex que requiera acceso a las centrales telefónicas por cualquier usuario que acceda por medio de dicho equipo y que dicho equipo esté marcado como “equipo no autenticado”, por lo tanto el SACET no solicita a ningún usuario (humano o automático) su contraseña individual de usuario para acceder a cualquier central en la red de Telmex.

Es importante mencionar que los equipos marcados “sin autenticación” o equipo “no autenticado” al no requerir una autenticación para el acceso, para cualquier entidad que las emplee para acceder a las centrales, será “marcado sin autenticación”, será el responsable de todos los eventos que cualquiera de sus usuarios ejecuten sobre las centrales y las estadísticas buenas y estadísticas malas de los usuarios le serán acumulados a tales equipos. Por esta razón es muy recomendable asignarles a los equipos marcados “sin autenticación”, un perfil muy bajo de comandos permitidos a ejecutar. Esto es importante, ya que cualquier usuario que las acceda tomará por este perfil asignado al equipo, lo cual limita su actividad en las centrales, por razones de seguridad. Por lo tanto, cualquier usuario que acceda por un equipo marcado como “no autenticado” perderá las facultades que le confiere su perfil individual de usuario y tomará el perfil limitado del equipo “marcado sin autenticación” que está utilizando.

Registro y Configuración de Usuario: El registro de usuarios es el segundo nivel de seguridad del SACET de tal manera que solo aquellos usuarios que estén registrados en este sistema serán viables de acceder a la central telefónica.

SACET maneja en su operación un conjunto de parámetros que acompañan al registro del usuario y que determinan su estado operativo en la central por ejemplo: usuario habilitado, usuario no habilitado, perfil de comandos permitidos, etc. Una nota importante es que todo equipo registrado en el SACET adicionalmente debe estar registrado como un usuario, este a su vez con un “perfil de usuario” correspondiente. Un equipo al darse de alta o registrarse se genera automáticamente un registro de usuario correspondiente.

Perfil de Usuario: Una característica operativa de cada usuario es el “perfil de comandos permitidos” el cual determina su alcance operativo de comandos a ejecutar en la central telefónica. El perfil es por lo tanto un número indicador que asocia a un grupo de comandos permitidos a ejecutar en la central telefónica, este indicador se asigna a cada usuario en forma individual. Es típico que un perfil se asigne a un grupo de usuarios “tipo” de tal forma que se puede desarrollar perfiles

de comandos por ejemplo para el equipo de “operación y mantenimiento”, otro para “ingeniería”, otro para “soporte técnico”, etc. SACET tiene la facultad de manejar o asignar a los usuarios dos tipos de perfiles:

En el **“perfil de comandos permitidos”** se enlistan todos los comandos que le son permitidos a ejecutar al usuario.
En el **“perfil de comandos limitados”** se enuncian todos los comandos que le son limitados al usuario.

Estos manejos representan una gran facilidad operativa, por ejemplo cuando a un usuario solo se le permite ejecutar una lista pequeña de comandos, es muy fácil enunciar tal lista en el “perfil de comandos permitidos”, por otro lado, para otro tipo de usuarios es más fácil el enunciar solamente los comandos que le son negados, por ejemplo un personal de soporte técnico, se le pueden permitir prácticamente todos los comandos, pero se le limitan comandos de reinicio de central, entonces para este casos se facilita el emplear un “perfil de comandos limitados” donde se enliste únicamente la lista de comandos que le son limitados, permitiéndole la ejecución del resto de comandos.

Switch Electrónico.- Consiste en un dispositivo electrónico que proporciona la funcionalidad de conmutación de puertos ethernet. El security-gateway debe presentar ciertas condiciones en cuanto a sus características funcionales; en caso de no presentarlas, se comanda al switch electrónico efectuar una conmutación. Estas características funcionales son: correcto estado del hardware, correcto estado funcional del sistema y correcto estado funcional del sistema operativo.

Bajo una operación normal (asegurada), el security-gateway recibe el tráfico de 4 puertos ethernet desde la RCDT y entrega en forma asegurada el tráfico a la central telefónica. En caso de que el security-gateway quede fuera de funcionamiento, por falla del hardware de la computadora, falla de energía, falla de software o falla de sistema operativo, entonces se conmutan los 4 puertos ethernet directamente de la red RCDT a la central telefónica, preservando de esta manera la conexión de RCDT con la central.

Proceso de Conmutación.- El security-gateway, puede operar en forma directa o asegurada. La operación asegurada corresponde al estado funcional normal operativo del security-gateway asegurando a la central. En operación directa, las cuatro conexiones ethernet de la central se conectan directamente a la central telefónica por lo que el security-gateway queda fuera de su función de aseguramiento, sin embargo puede quedar conectado y en comunicación con el SACET. Para que el security-gateway pueda funcionar con ambas condiciones operativas Asegurado-Directo, es necesario que ocurra un conjunto de procesos denominados Procesos de conmutación. Los procesos de conmutación son automáticos y se generan al momento de ejecutar un cambio de directo a asegurado y viceversa.

Operación en Directo: La operación directa, corresponde al estado funcional cuando el hardware o el software del security-gateway han fallado o cuando el administrador del SACET ha decidido hacer una operación o onmutación a directo, provocando con ello que el switch electrónico conecte directamente los puertos ethernet de la red RCDT con la central telefónica. En este estado el SACET-GESTOR reconfigura a la central, para permitir que los usuarios y aplicaciones continúen accediendo a la central telefónica por las direcciones IP´s conocidas.

Indicadores de estatus de puertos.- Nos auxiliamos de la siguiente ilustración para mostrar el significado de los indicadores del estatus de los puertos que emplea SACET.

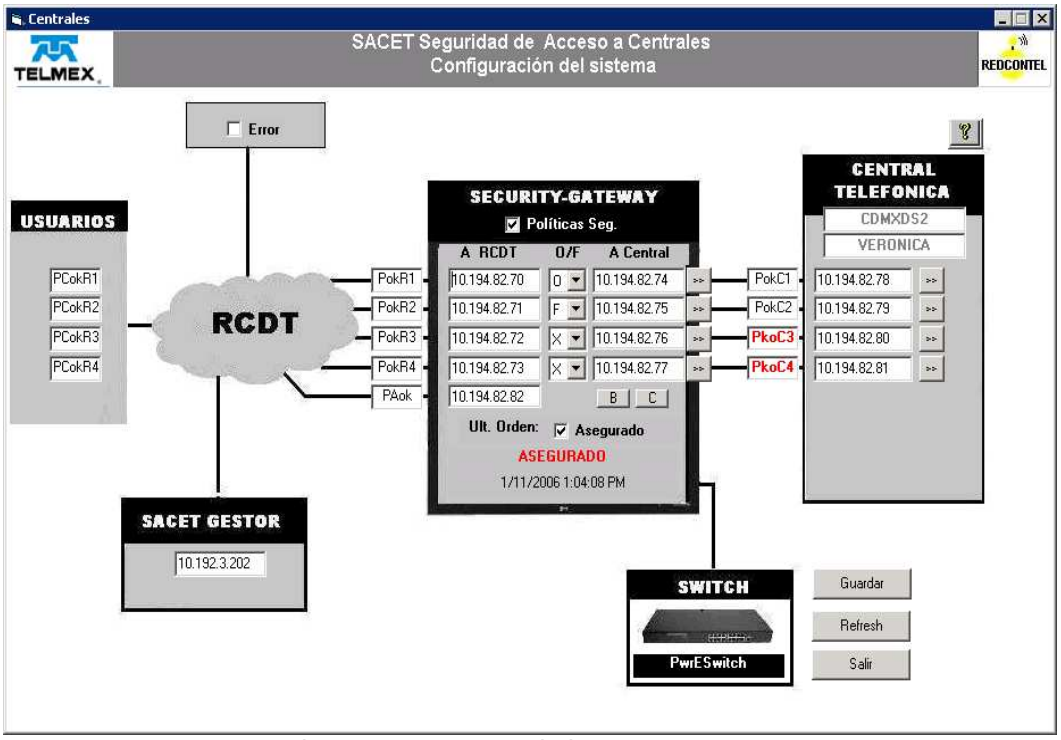


Figura. 1.12 Estatus de los puertos en SACET.

PAok, PAko.- Indicación en el SACET para denotar el estado funcional del puerto de administración del security-gateway:
PAok.- puerto de administración trabajando correctamente, conectado o security-gateway en comunicación con SACET.
PAko.- puerto de administración desconectado o security-gateway sin comunicación con SACET.

PCokR1, PCkoR1, PCokR2, PCkoR2, PCokR3, PCkoR3, PCokR4, PCkoR4.- Indicación en el SACET para denotar el estado funcional de los puertos hacia la central o al security-gateway, como la perciben los usuarios de la red. Los estados pueden ser correspondientemente ok o ko y su significado es el siguiente:
PCokXX.- Puerto de acceso operando correctamente.
PCkoXX.- Puerto de acceso con alguna falla.

PokR1, PkoR1, PokR2, PkoR2, PokR3, PkoR3, PokR4, PkoR4.- Indicación en el SACET para denotar el estado funcional del puertos hacia la RCDT como lo percibe el security-gateway. Los estados pueden ser ok o ko y su significado es:
PokXX.- Puerto de acceso operando correctamente.
PkoXX.- Puerto de acceso con alguna falla.

PokC1, PkoC1, PokC2, PkoC2, PokC3, PkoC3, PokC4, PkoC4.- Indicación en el SACET para denotar el estado funcional del puertos hacia la central como lo percibe el security-gateway. Los estados pueden ser ok o ko y su significado es:
PokCX.- Puerto de acceso operando correctamente.
PkoCX.- Puerto de acceso con alguna falla.

Tonalidades de Puertos: Para resaltar cuando un puerto está fallando o fuera de funcionamiento, SACET lo ilustra en color rojo, por ejemplo **PkoC1** pero cuando el puerto se encuentra operando correctamente se ilustra en tonalidad normal en color negro, por ejemplo **PokC1**.