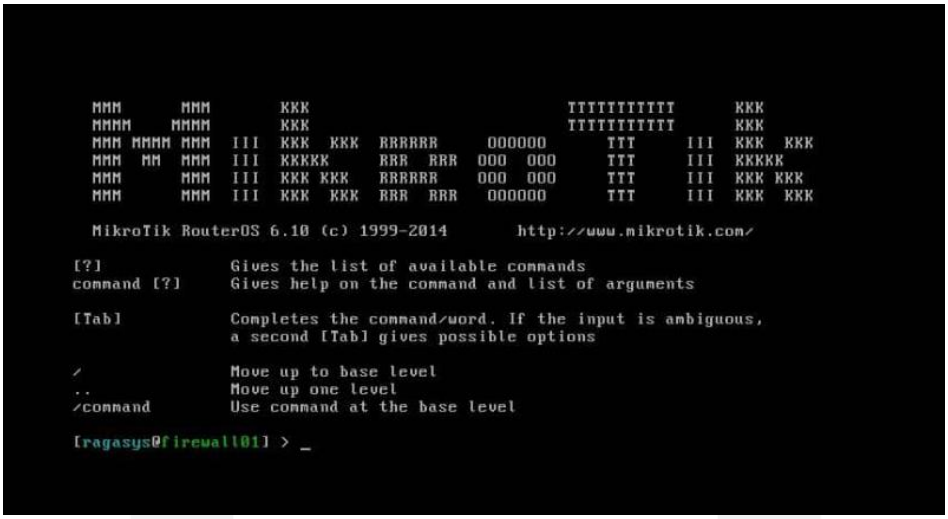
SISTEMA INTERNO DE SEGURIDAD



CONVERGENCIA DIGITAL

Ingeniería Aplicada
Conectando el futuro

INTRODUCCIÓN

Las informaciones en las redes inalámbricas presentan un alto índice de vulnerabilidades respecto al cableado estructurado o redes cableadas, ya que por este medio la información se ve fácilmente interceptada por equipos de alta gama. De tal manera el atacante ingrese al punto de acceso inalámbrico y puede dar beneficios al usuario y permisos no asignados dentro de la red que proviene del atacante hacia el proveedor o usuario. Para convergencia Digital es prioridad establecer políticas de seguridad altamente confiables, fácilmente administrables, que puedan contrarrestar amenazas que pongan en peligro la información y servicios.

Este documento proporciona y da a conocer mecanismos de seguridad que buscan contrarrestar la integridad de los servicios tecnológicos.

OBJETIVOS

- Seleccionar método para que el usuario pueda ingresar a la red por medio de la autenticación.
- Crear base de datos de acceso para administrar conexiones del equipo de red.
- Implementar mecanismos de seguridad donde se pueda utilizar de forma adecuada los equipos de trabajo.
- Elaborar políticas de seguridad para el uso correcto de los equipos mikrotik

1. Seguridad Física y Entorno

Esta política tiene diferentes sistemas de información como lo son instalaciones, equipamiento, cableado y medios de almacenamiento.
El personal encargado debe tomar medidas de seguridad tanto físicas como de entorno y debe realizar mantenimiento respectivo en los equipos de trabajo.
La persona encargada debe tener un control y evitar el acceso no autorizado al sitio de trabajo como a la información que maneja la empresa, mediante diferentes medidas de seguridad estipuladas por la entidad.
También se debe contar con un perímetro de seguridad para proteger el área donde se encuentre la información, es decir que no permita el acceso a terceros y personal que no esté autorizado a estar en la zona de trabajo.
Se debe tener en cuenta las amenazas que puedan afectar la operación del sistema, disponer de controles para poder minimizar un riesgo potencial como perdida de información, daños eléctricos, fuego entre otros.
La ubicación de equipos de procesamiento y almacenamiento de información deben estar en sitios donde se puedan proteger y no sufran ningún tipo de daño en el entorno, evitar el acceso no autorizado, fuera y dentro de las instalaciones.
Tenemos que tener mayor cuidado en los cableados de energía eléctrica tanto como el de comunicaciones el cual deben estar regidas bajo una norma de seguridad donde se pueda dar protección y prevenir cualquier eventualidad que se presente.
El mantenimiento de los equipos deber ser constante para garantizar que todo el tiempo este en óptimas condiciones.
La seguridad de los equipos fuera debe ser la misma protección que la interna, y tomando conciencia de los riesgos que se pueden ver en este entorno.
Se debe tener un control de equipos que ya no estén en condiciones de uso y desecharlos por completo ya que la reutilización puede afectar el buen funcionamiento de nuestra red.
Todas estas políticas de seguridad físicas son usadas por convergencia digital tanto en los nodos con en el ámbito del cliente para evitar cualquier tipo de problema que se presente en nuestro entorno de trabajo.

2. Seguridad en las Estaciones o Pc de trabajo

Convergencia Digital tiene como objetivo dar a conocer la importancia que se debe tomar en un control de acceso a la red y tener una medida de prevención a faltas que se presenten tanto interno como externamente. De igual forma restringir el acceso a personal no autorizado a nuestra información y servicios, implementar una autenticación y autorización, dar a conocer al personal que labora en nuestra entidad del uso correcto de las contraseñas y equipos de trabajo, garantizar que los nodos y conexiones en diferentes puntos sea optima, así asegurar el acceso remoto en nuestro entorno laboral.

Es importante recalcar el acceso a los usuarios, desde el momento que se ingresa el usuario hasta la fase final del registro, con este registro se trata de asegurar el acceso autorizado al usuario a nuestro sistema de información. Otro punto clave seria controlar los derechos de acceso del sistema y servicio.

También es muy importante controlar la asignación de privilegios que se le dan al usuario, ya que si les dan un uso inadecuado a estos privilegios podrían afectar el buen funcionamiento de la entidad.

La entidad debe contar con buenas prácticas de seguridad en el momento de seleccionar y usar las contraseñas.

La autenticación de nodos es la alternativa para el acceso remoto de usuarios, el cual están conectados a un sistema compartido seguro.

Se implementa protección de puertos de diagnóstico el cual impide el acceso a personal no autorizado. Sera protegido por un mecanismo de seguridad asignado.

3. Seguridad en Conexiones Inalámbricas

La conexión a las redes inalámbricas de Convergencia Digital, se suministrarán para temas relacionados con el buen desarrollo de las actividades de los funcionarios y deben solicitarse al Administrador general de la Red.

Por ningún motivo se permitirán conexiones a internet inalámbrico corporativo a terceros a menos que se requiera para temas de soporte sobre la infraestructura tecnológica. Para conexiones inalámbricas a terceros se contará con una red específica para proporcionar conectividad a internet.

4. Seguridad Equipos de Red}

Lo más importante para Convergencia Digital es la Red, el cual crea un usuarios y contraseñas en los equipos para que no sean vulnerables a atacantes, que puedan acceder a él o borrar información.

También se actualiza el firmware ya que trae mejoras y un mejor funcionamiento de los equipos

Para el acceso a los equipos de red, se aplican listas de acceso en cada uno por medio de protocolo SSH versión 2, en los equipos que no se soporte el protocolo SSH, se utilizará el acceso vía TELNET con su respectiva lista de acceso.

5. Acceso a Clientes

Para el acceso a internet de los clientes, debido a que la red es inalámbrica en su totalidad, se implementó el sistema de seguridad WPA2-PSK en los puntos de acceso, esto permite que solo los equipos CPE con la contraseña correcta obtengan su acceso a internet. La siguiente ilustración, muestra de manera simplificada de la solución implementada.

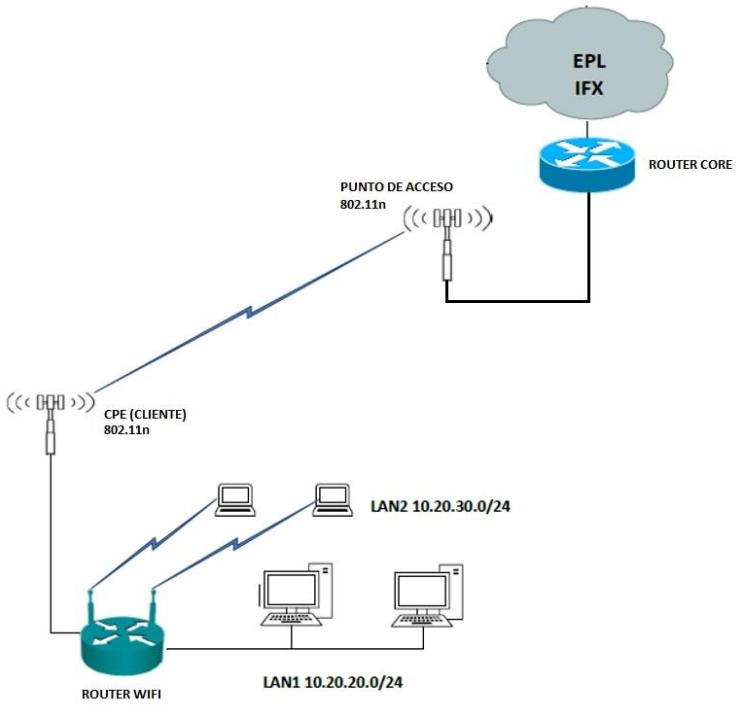
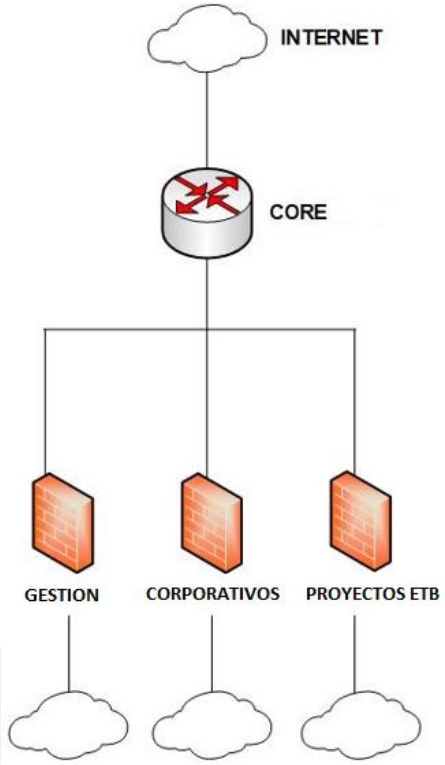


Figura 1. Acceso clientes a Internet

Para bloquear el acceso a los usuarios a los equipos de red, se implementan listas de acceso. Adicionalmente, se segmenta las redes a través de VLAN, lo que permite controlar la gestión de los equipos y usuarios.

6. Seguridad de Aplicaciones

Las aplicaciones y páginas web, se protegen por medio de contextos (firewall virtual), lo que permite separar los usuarios de las distintas aplicaciones con las que cuenta Convergencia Digital. El siguiente diagrama muestra de manera simplificada los contextos de firewall.


INTERNET
CORE
GESTION
CORPORATIVOS
PROYECTOS ETB