Seguridad y Competencias Profesionales
Curso 2010/2011

Rafael, Ledia, Leopoldo, Jesus, Luis

10 de noviembre de 2010

1. Seguridad Comunicaciones

1.1. Visión general

La seguridad en la red es uno de los aspectos más importantes dentro de la política de seguridad de una organización que se disponga de dispositivos conectados entre sí y más si se encuentran conectados a internet. Se establecerán medidas de seguridad para asegurar el acceso a la información desde el exterior de la entidad así como restringir los accesos mediante los medios de red por parte de los dispositivos conectados a la red de la empresa.

Se redactarán normas para asegurar el acceso desde el exterior estableciendo un nivel de seguridad perimetral, definición del protocolo escogido para la disposición del servidor web, medidas de seguridad ligadas a conexiones inalámbricas e implantación de VPN.

1.2. Objetivos

Esta política está diseñada para proteger los datos de la empresa. Permite asegurar que el acceso a los datos se realice siempre mediante los mecanismos de red establecidos, impidiendo el acceso de posibles intrusos que puedan realizar actividades que atenten contra la privacidad e integridad de los datos de la empresa.

1.3. Alcance

Esta política se aplica a todos los medios y dispositivos de red, y por tanto, a todos los empleados que los utilizan. De la misma forma, afectará a los usuarios que accedan de forma remota al las bases de datos.

1.4. Arquitectura

La empresa está dividida en tres edificios geográficamente separados entre sí. Estando estos edificios conectados por la red con topología de estrella y mallados a través de una conexión Macrolan de Telefónica como línea de backup. El edificio principal, edificio de oficinas, es el núcleo principal de la estrella, este conecta con los otros dos edificios, almacén/ventas y bodega a través de F.O. SM propietaria de la empresa.

La seguridad perimetral se establecerá a través de un servidor proxy. Este será la única puerta de entrada/salida con el exterior.

En el interior, la red estará dividida en las siguientes subredes lógicas (vlan): gestión de red, gestión directivos, gestión administrativa, red de respaldo (macrolan), servicio (máquinas embotellado, etc...) y WIFI. El acceso de una vlan a otra estará restringido así como el acceso a los servidores.

La red WIFI estará cifrada mediante el protocolo WPA2, y los roles de acceso y direccionamiento de cada usuario estará definido en el servidor Radius.

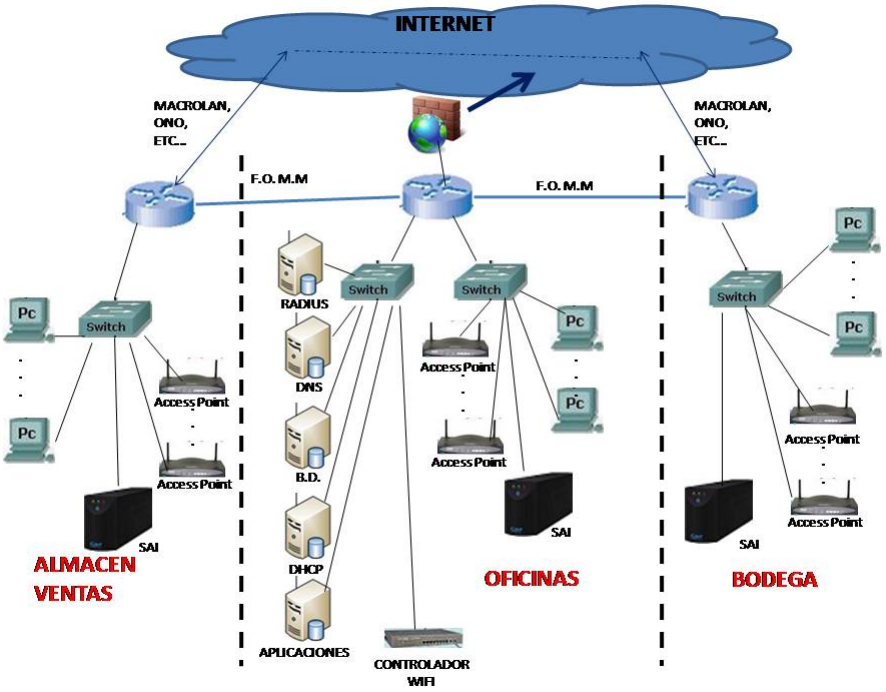

Figura 1: Arquitectura de la red.

La línea de respaldo, que une los edificios satélites (Almacen/Ventas y Bodega) sólo estará activa en caso de que se detecte que la línea principal este cortada. Los router de las distintas sedes usarán para tal fin el protocolo OSPF y solo estarán definidos el enlace primario y el de backup. A sí mismo, solo de definirán en lo router las vlan antes mencionadas.

El servidor Web de la empresa estará situado en la sede central y será propiedad de la misma. Este estará tras el firewall, dentro de la red interna.

Tanto los router como los switch estarán protegidos con contraseñas alfanuméricas y solo serán accesibles mediante SSH o consola. El conocimiento de estas contraseñas será exclusivo del personal que defina el responsable de la Unidad de Informática, máximo responsable de dicho conocimiento.

Las contraseñas serán modificadas una vez al mes, pudiéndose modificar con más frecuencia si el responsable de la Unidad de Informática lo estimara preciso. Este cambio quedará reflejado por escrito indicando la fecha, personal implicado y firma del responsable.

El cableado de red será estructurado, UTP CAT 5 ó superior. No se habilitará ninguna roseta sin cumplir con el protocolo establecido y solo se permitirá una conexión por toma de red, es decir, queda totalmente prohibido conectar hub, switch ó cualquier otro elemento que extienda la red sin consentimiento previo.

Ninguna roseta se cambiara de vlan sin el correspondiente visto bueno del responsable de la unidad, debiendo quedar reflejado por escrito en dicha solicitud la fecha, motivo y firma del responsable.

1.5. Habilitación de rosetas

Para la habilitación de una roseta es obligatorio informe del responsable de la unidad indicando el propósito de uso, fecha y firma.

Si una roseta quedara sin uso es responsabilidad del responsable de la unidad el informar al departamento de comunicaciones la rehabilitación de dicha roseta. Esto se realizará por escrito indicando la fecha, motivo y firma del responsable.

1.6. Conexiones desde el exterior

Todas conexión que se haga desde el exterior de la empresa a cualquier servidor se realizarán mediante VPN (red privada virtual), para los que se usarán los certificados clase 1 emitidos por la empresa