



**UNIVERSIDAD NACIONAL
PEDRO RUIZ GALLO**



**FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
ESCUELA PROFESIONAL DE INGENIERÍA
ELECTRÓNICA**

TESIS

**Diseño de un prototipo de seguridad para las redes industriales
medianas utilizando filtros ACL.**

**PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO
ELECTRÓNICO**

ELABORADO POR:

Del Pino Hernández Genady Acmed

Villanueva Bazán Henry Josué

LAMBAYEQUE - PERU

2014



**UNIVERSIDAD NACIONAL
PEDRO RUIZ GALLO**



**FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
ESCUELA PROFESIONAL DE INGENIERÍA
ELECTRÓNICA**

TESIS

**Diseño de un prototipo de seguridad para las redes industriales medianas
utilizando filtros ACL**

**PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO
ELECTRONICO ELABORADO POR:**

Del Pino Hernández Genady Acmed

Villanueva Bazán Henry Josué

**LAMBAYEQUE – PERÚ
2014**

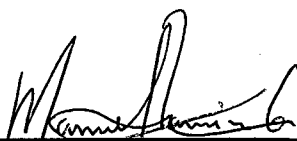
DISEÑO DE UN PROTOTIPO DE SEGURIDAD PARA LAS REDES INDUSTRIALES MEDIANAS UTILIZANDO FILTROS ACL

ELABORADO POR LOS BACHILLERES

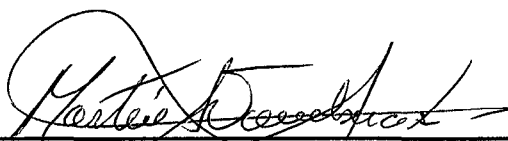
Br. Del Pino Hernández Genady Acmed

Br. Villanueva Bazán Henry Josué

Aprobado por los miembros del jurado:



Ing. Manuel Javier Ramírez Castro
Presidente del Jurado



Ing. Martin Augusto Nombera Lossio
Secretario del Jurado



Ing. Lucia Isabel Chaman Cabrera
Vocal del Jurado



Ing. Romero Cortez Oscar Uchelly
Asesor

DEDICATORIA

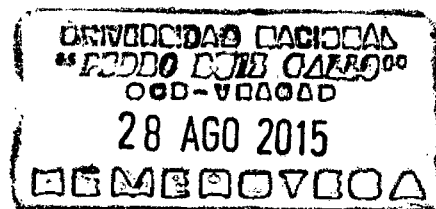
A mis padres por su amor, trabajo y sacrificio en todos estos años, gracias a ustedes he logrado llegar hasta aquí y convertirme en lo que soy. Ha sido un privilegio ser su hijo. Son los mejores padres.

Villanueva Bazán Henry Josué

DEDICATORIA

A mi abuela Blanca que me mira desde los cielos, mi abuelo Moisés que fue mi segundo padre quien ahora es un ángel quien me cuida aun no estando en vida y a mi querida madre Eva que siendo mi motor y motivo en esta vida siendo el tesoro máspreciado que tengo a quien agradezco por su sacrificio en todas las instancias de mi vida.

**Del Pino Hernández Genady
Acmed**



INDICE

CARATULA.....	1
DEDICATORIA	3
1. Aspectos informativos.....	10
1.1. Título del proyecto.	10
1.2. Autor(es)	10
1.2.1. Asesor.	10
1.3. Área de Investigación	10
1.4. Lugar de Ejecución	10
1.5. Duración Estimada.....	11
2. ASPECTO DE LA INVESTIGACIÓN	11
2.1. Planteamiento del Problema Científico	11
2.2. Revisión Bibliográfica	11
2.2.1. Antecedentes.....	11
2.2.2. Marco Teórico.....	12
2.3. Formulación del problema científico.....	14
2.4. Objetivos	14
2.4.1. Objetivo General.....	14
2.4.2. Objetivo Específico	14
2.5. Justificación e Importancia.....	14
2.5.1. Justificación Teórica.....	15
2.5.2. Justificación Práctica.....	15
2.5.3. Justificación Metodológica.....	15
2.6. Hipótesis	16
2.7. Definición de Términos y Conceptos	16
2.8. Operacionalización de Variables (Definición de las variables)	18
2.9. Tipo de Investigación.....	19
2.10. Diseño y Contrastación de la Hipótesis.....	19

2.11.	Población y Muestra de Estudio.....	19
2.12.	Técnicas de Muestreo.....	20
2.13.	Análisis estadístico de datos	20
3.	Sistema SCADA.....	20
3.1.	Descripción.....	20
3.2.	Objetivos.....	22
3.3.	Lo que puede ofrecer.....	23
3.4.	Prioridades de un sistema SCADA.	24
3.5.	Entorno.....	26
3.6.	Gestión de la Producción, MES (Manufacturing Execution System).....	26
3.6.1.	Pautas para la elección y diseño de un sistema SCADA.....	27
3.6.2.	Arquitectura de un sistema SCADA.....	29
3.6.3.	Interface Hombre-Máquina (HMI, MMI).	29
3.7.	Utilización de componentes físicos y software para el desarrollo. 30	
3.7.1.	Tipos de conexión e interfaz para la comunicación.....	30
3.7.2.	Modelo OSI.....	30
3.7.3.	RS-232.....	33
3.7.4.	RS-485.....	34
3.7.5.	Aspectos para la comunicación.....	35
3.7.6.	Protocolo OPC.....	38
3.8.	PLC's	42
3.8.1.	Conceptos básicos de PLC's	42
3.8.2.	Especificaciones técnicas de la familia PLC S7-300.....	46
3.9.	Software Step7 Lite.....	51
3.9.1.	Conceptos básicos de LabVIEW.....	52
3.10.	Instrumentación de planta de nivel de líquido.....	56
4.	Diseño del control y monitoreo.....	59
4.1.	Interfaz para comunicación.....	59

4.2. Desarrollo de diagrama en escalera STEP 7 Lite.....	60
4.3. Desarrollo para declarar variables en OPC.....	63
4.3.1. OPC Servidor de National Instruments (NI).....	63
4.3.2. OPC Servidor IBH Softec.....	66
4.4. Configuración para interactuar con LabVIEW.	68
4.5. Conexión PLC S7-300 CPU 313C con componentes de la planta hidráulica.	71
4.6. Programación y Desarrollo.....	74
5. Amenazas Lógicas	79
5.1. Acceso - Uso – Autorización	79
5.2. Detección de Intrusos	80
5.3. Identificación de las Amenazas	81
5.4. Tipos de Ataques.....	85
5.5. Errores de Diseño, Implementación y Operación.....	85
5.6. Implementación de las Técnicas.....	86
5.7. ¿Cómo defenderse de estos Ataques?	87
5.7.1. Amenazas lógicas – Tipo de ataques	88
5.7.2. Ingeniería Social.....	89
5.7.3. Ingeniería Social Inversa	90
5.7.4. Trashing (Cartoneo)	91
5.7.5. Ataques de Monitorización	91
5.7.6. Ataques de Autenticación	92
5.7.7. Denial of Service (DoS).....	92
5.7.8. Ataques de Modificación - Daño	92
5.8. Amenazas Lógicas Tipo de Ataques Motorizados	92
5.9. Amenazas lógicas de autenticación	99
5.9.1. Utilización de BackDoors	103
5.9.2. Utilización de Exploits	104
5.9.3. Obtención de Passwords.....	104
5.9.4. Uso de Diccionarios.....	105

5.10. Amenazas Logicas -Tipos de Ataques - Denial of Service (DoS).....	106
5.11. Amenazas Lógicas - Tipos de Ataques - Ataques de Modificación (Daño) 113	
5.12. Firewall – Cortafuegos	118
5.13. Routers y Bridges.....	120
5.14. Tipos de Firewall	120
5.14.1. Políticas de Diseño de Firewalls	121
5.14.2. Restricciones en el Firewall.....	122
5.14.3. Beneficios de un Firewall.....	123
5.14.4. Limitaciones de un Firewall.....	123
5.14.5. Firewall - Filtrado de Paquetes.....	124
5.14.6. Firewall - Dual-Homed Host.....	125
5.14.7. Firewall - Screened Host.....	126
5.14.8. Firewall - Screened Subnet.....	127
5.15. Protección.....	128
5.15.1. Vulnerar Para Proteger.	129
5.15.2. Firewalls	130
5.15.3. Access Control Lists (ACL)	130
5.15.4. Wrappers	131
5.15.5. Detección de Intrusos en Tiempo Real.....	132
5.15.6. Call Back	133
5.15.7. Sistemas Anti-Sniffers	133
5.15.8. Gestion de Claves "Seguras".....	134
5.15.9. Seguridad en Protocolos y Servicios	134
5.15.10. Criptología.....	134
5.15.11. Inversión.....	135
5.15.12. Vulnerar para Proteger.....	136
5.16. Administración de la Seguridad.....	136
5.17. Penetration Test, Ethical Hacking o Prueba de Vulnerabilidad. 138	
5.18. HoneyPots-HoneyNets.....	139

5.19.	Detección de Intrusos en Tiempo Real.....	141
5.19.1.	Intrusión Detection Systems (IDS).....	141
5.19.2.	Características de IDS.....	142
5.19.3.	Fortalezas de IDS.....	143
5.19.4.	Debilidades de IDS	144
5.19.5.	Inconvenientes de IDS	144
5.19.6.	Gestión de Claves Seguras	144
5.20.	Normas de Elección de Claves	146
5.20.1.	Normas para Proteger una Clave	147
5.20.2.	Contraseñas de un Sólo Uso.....	148
6.	Prueba de Captura de Datos, Contraseñas y Login.	150
6.1.	Wireshark.....	150
6.2.	Configuración de filtros.....	151
6.3.	Configuración de filtros.....	152
7.	Planteamiento de la solución.....	156
7.1.	Prueba de captura de contraseña e inserción de nuevos programas a través de la red (PLC).....	158
7.2.	Posibilidades que nos presenta el cisco asa 5110.....	159
7.3.	Configuración de equipos	161
7.3.1.	Configuración de SWITCH.....	161
7.3.2.	Configuración de Router	164
7.3.3.	Configuración del cisco asa 5-XXX.....	167
	167
8.	Conclusiones	171
9.	Referencia Bibliográfica	173
10.	Cronograma de actividades.	174
11.	Presupuesto.	175
12.	Financiación.....	175



1. Aspectos informativos

1.1. Título del proyecto.

"Diseño de un prototipo de seguridad para las redes industriales medianas utilizando configuración de filtros ACL".

1.2. Autor(es)

Del Pino Hernández Genady Acmed

Código: 062265-I

E-mail: genady3@hotmail.com

Villanueva Bazan Henry Josue

Código: 082291-E

E-mail: henryxd@live.com

1.2.1. Asesor.

Ing. Oscar Uchelly Romero Cortez – Ing. Electrónico de la Universidad Nacional Pedro Ruiz Gallo.

1.3. Área de Investigación

Ingeniería Electrónica

1.4. Lugar de Ejecución

El proyecto se llevara a cabo en los ambientes del Laboratorio de Control Industrial de la Escuela de Ingeniería Electrónica.



1.5. Duración Estimada

Dos meses y medio

2. ASPECTO DE LA INVESTIGACIÓN

2.1. Planteamiento del Problema Científico

Los Sistemas de control industrial son construcciones flexibles que se traducen en una mayor eficiencia y rentabilidad, al mismo tiempo para su crecimiento están las redes industriales medianas no contemplan la seguridad en el acceso interno o externo y con esto también vienen la vulnerabilidades que puede opacar o malograr el proceso industrial. En los últimos años, la seguridad informática industrial ha sido ignorada en su mayoría debido a los costos, la falta de comprensión y una tasa de incidencia baja. Estos sistemas se basan en un software comercial que aumenta la facilidad y la probabilidad de un ataque. Hoy, nos enfrentamos a la creciente amenaza de gente extranjera, los gobiernos y las empresas competidoras, cuyos riesgos se incrementan en órdenes de magnitud creciente. En la presente investigación se provee una visión general de los componentes de control común, comunicados a una red industrial mediana, para poder entender cómo funciona una industria, cuáles son sus vulnerabilidades más comunes y la situación actual de las redes industriales medianas.

2.2. Revisión Bibliográfica

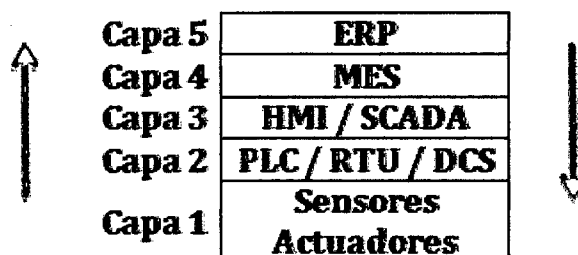
2.2.1. Antecedentes

Ataque de stuxnet en el 2010, un gusano para sabotear plantas industriales medianas y grandes en Irak.

Ataque de Duqu en el 2011, un virus que afecta los sistemas SCADA en redes industriales medias y grandes.

2.2.2. Marco Teórico

La necesidad de proteger las redes industriales en estos niveles nos muestran la necesidad de asegurar seguridad.



Empezando por la capa inferior (1), la capa de los Sensores y Actuadores (equipos que regulan las variables y ejecutan los controles), sería algo así como la capa física, donde lo que importa es el medio o los dispositivos de campo. Básicamente, aquí se concentran a nivel de dispositivos de campo, los sensores de movimiento, sensores de temperatura (termopar o termocuplas), sensores de niveles, sensores magnéticos, etc. y por otro lado, a este nivel lo que se transmiten son señales.

En la capa siguiente (2), se encuentran:

Los famosos PLC (Programmable Logic Controller o Controlador Lógico Programable)

Las RTU (Remote Terminal Unit o Unidad Terminal Remota) que básicamente son un microprocesador capaz de adquirir señales de campo y actuar en consecuencia en base a una programación existente.

DCS (Distributed Control System). Son un Sistema de Control Distribuido (se comunica con los dispositivos de campo y presenta los datos a un HMI o interfaz para humanos), que obtiene información de los PLC o de las RTU. Por lo general la forma antigua más común de interconexión era RS232 o Ethernet utilizando protocolos específicos como MODBUS o DNP3, entre otros (existen más protocolos y más



medios de interconexión). Los términos y conceptos de DCS y SCADA son muy similares entre sí, y en ocasiones se utilizan indistintamente, dependiendo del sector en el que se esté trabajando.

Subiendo un poco más en el modelo hasta la capa (3), nos encontramos con el nivel de los HMI/SCADA donde, fundamentalmente, se recolecta toda la información de los PLC y/o RTU distribuidos de manera automática, y donde empezamos a encontrarnos con un protocolo conocido como TCP/IP.

En la capa superior siguiente (4) aparece un nuevo jugador pocas veces mencionado, el MES (Manufacturing Execution System) cuyo objetivo no es la evaluación del proceso en sí mismo, sino la de su eficiencia a partir de la información recibida. Por ejemplo, si determinada máquina no tuvo el mantenimiento necesario en fecha y tiene disponible otro equipo que sí lo tuvo como para asegurar la calidad; el cumplimiento de un determinado proceso; o si el turno de tarde produce más que el turno de mañana, etc.

Y finalmente, en la última capa (5) se encuentra el también conocido ERP, donde básicamente se decide qué tipo de controles se ejecutarán, con qué frecuencia y con qué esfuerzo, con el objetivo de disponer de una planificación coherente.

No todas las plantas industriales o las fábricas disponen de la totalidad de estos componentes aplicados en sistemas. Si estos niveles no son protegidos o no tienen un mínimo nivel de seguridad, están siendo propensas a un ataque interno o externo.



2.3. Formulación del problema científico

¿De qué manera ayudará a mitigar riesgos en la seguridad de las redes industriales medianas, utilizando la configuración de filtros ACL?

2.4. Objetivos

2.4.1. Objetivo General

Diseñar un prototipo de seguridad para las redes industriales medianas.

2.4.2. Objetivo Específico

Diseñar e implementar un prototipo de plataformas de control industrial para redes industriales medianas.

Establecer los dispositivos y equipos adecuados para la implementación de la seguridad en las redes industriales medianas.

Utilizar la configuración de filtros ACL para mitigación de riesgos en las redes industriales medianas.

2.5. Justificación e Importancia

El estudiante de ingeniería electrónica, durante su formación profesional desarrolla diversos prototipos electrónicos y sistemas embebidos, pero para poder desarrollar este tipo de aplicaciones necesitan un elevado conocimiento de programación en equipos electrónicos, configuración de equipos y diseño de niveles de seguridad, es por eso que muchos de los estudiantes utilizan prototipos existentes en el mercado de la tecnología con ciertos límites, en esta oportunidad se ha probado existencia de conexión



externa de manera remota a redes industriales de acceso restringido provocando fallas de las ordenes de los controladores como datos falsos a la estación

Base concadenando una serie de problemas tanto en la administración y economía de cualquier empresa.

Con esta perspectiva hemos puesto interés en diseñar un prototipo de infraestructura que sea capaz de detener riesgos de lo anteriormente mencionado usando tecnología en estas empresas medianas.

2.5.1. Justificación Teórica

Desde el punto de vista el avance vertiginoso de la tecnología abre un mundo de posibilidades para el desarrollo de prototipos electrónicos, pues facilita la interacción y programación de controladores físicos y virtuales en forma eficiente y rápida maximizando la eficiencia que estos dispositivos nos brinda.

2.5.2. Justificación Práctica.

Al diseñar este prototipo se le agrega un nivel de seguridad a las redes industriales medianas para mitigar riesgos internos como externos en el menor tiempo posible y a su vez ser capaces de interpretar, porque una red industrial puede fallar y ocasionar mal funcionamientos de equipos.

2.5.3. Justificación Metodológica.

La metodología es interdisciplinaria, tanto en el ámbito de Control Industrial, Redes, Seguridad Informática y Optimización de procesos.



2.6. Hipótesis

Si se diseña un mecanismo de protección para una red industrial entonces se mejorará el nivel de seguridad

2.7. Definición de Términos y Conceptos

RED INDUSTRIAL: Protocolo de comunicación para la medición y el control de procesos donde todos los instrumentos puedan comunicarse en una misma plataforma.

SCADA: Acrónimo de Supervisory Control And Data Acquisition, Supervisión, Control y Adquisición de Datos) es un software para ordenadores que permite controlar y supervisar procesos industriales a distancia.

Router: También conocido como enrutador o en caminador, es un dispositivo que proporciona conectividad a nivel de red

PLC: Un controlador lógico programable, más conocido por sus siglas en inglés PLC (programmable logic controller), es una computadora utilizada en la ingeniería automática o automatización industrial, para automatizar procesos electromecánicos

ERP: Los sistemas de planificación de recursos empresariales('ERP, por sus siglas en inglés, enterprise resource planning) son sistemas de información gerenciales que integran y manejan muchos de los negocios asociados con las operaciones de producción y de los aspectos de distribución de una compañía en la producción de bienes o servicios.



Switch: Es un dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos.

Sistema operativo Linux: LINUX es un sistema operativo, compatible Unix. Dos características muy peculiares lo diferencian del resto de los sistemas que podemos encontrar en el mercado, la primera, es que es libre.

Niveles de seguridad: Agregar seguridad a cada nivel, para evitar intrusos.

ACL: Una lista de control de acceso o ACL (del inglés, access control list) es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.



2.8. Operacionalización de Variables (Definición de las variables)

VARIABLE	DEFINICIÓN OPERACIONAL	INDICADOR
Independiente		
Equipos de control	Dispositivos electrónicos diseñados para el control de procesos industriales	Monitoreo a través de un panel.
Red industrial	Arquitectura diseñada para interconectar equipos.	Panel de tráfico de datos.
VARIABLE	DEFINICIÓN OPERACIONAL	INDICADOR
Dependiente		
Sistema de control	Sistema automatizado que permita un control de la red industrial	Control a través de interfaces por panel o laptop.
Paquetes y datos	Sistema automatizado que permita sensar y controlar la cantidad de paquetes y datos que están entrando y saliendo.	Supervisión y control de tráfico.
Flujo	Sistema automatizado que permita un flujo de información segura dentro y fuera de la red	Supervisión de flujo en la red a través de las ACLs.



2.9. Tipo de Investigación

Tecnológica Experimental.

2.10. Diseño y Contrastación de la Hipótesis

Teniendo en cuenta los huecos de seguridad en las redes industriales medianas actuales, es necesario diseñar un medio de protección para agentes internos como externos, dados los procesos de alto riesgo que constantemente son monitoreados para evitar sus fallas, estos periféricos conectados a la red como el PLC sin seguridad, abren una vulnerabilidad para degradar el funcionamiento del proceso.

Dada la hipótesis, al vulnerar un periférico se ve en riesgo parcialmente o totalmente el proceso afectando la productividad de la empresa, teniendo consecuencias económicas, es necesario diseñar una infraestructura que protegerá a la red en los distintos niveles de su arquitectura utilizando tecnología ACL, para dar respuestas a estos riesgos existentes.

2.11. Población y Muestra de Estudio.

El crecimiento en las plantas industriales en Chiclayo, como en otras partes del Perú no es ajeno a esta investigación ya que son medianas industrias emergentes y si son pequeñas en algún momento tendrán que acoplar esta tecnología, actualmente están saliendo empresas peruanas de industria media como andino, apu, pinturas peru, etc. Que ya ven la necesidad de implementar o ya se a implementado una red industrial para mejorar su eficiencia y productividad.



2.12. Técnicas de Muestreo

A través de los correos de las empresas enviamos a múltiples empresas y recibimos respuesta de ellas.

2.13. Análisis estadístico de datos

A través de los datos recolectados se podrá diseñar un prototipo estándar para demostrar la necesidad de la seguridad en una red industrial y poner establecer cuáles serán las reglas claras para el ACL, como que equipos vamos a usar y en qué tipo de proceso a si podremos hacer una demostración.

3. Sistema SCADA.

3.1. Descripción.

Cuando cada fabricante se encontraba ante un problema de automatización desarrollaba un elemento electrónico específico para solventarlo. Una memoria reducida era lo normal en estos elementos, por lo cual necesitaban comunicarse constantemente con sus sistemas de control centrales para enviar los datos. Incluían una serie de entradas y salidas fijas y utilizaban generalmente lenguajes de programación poco conocidos.

Por lo que en los años setenta ven aparecer una nueva generación de autómatas de la mano de fabricantes de equipos eléctricos como Schneider Electric, Siemens, SquareD, o Allen-Bradley, que implementaron autómatas capaces de controlar grandes cantidades de entradas y salidas, ideales para industrias tales como la automotriz. Resultado de esto fue la introducción del micro PLC, en los años ochenta que permitan anexar controles modulares que se adaptaban a las necesidades del momento y venían provistos de sistemas de programación genéricos (ladder o escalera), lo que les deparó un éxito inmediato en todo el ámbito industrial.



Varios fabricantes desarrollaron entonces paquetes de software capaces de comunicarse con los sistemas de control existentes y permitieron así una flexibilidad de uso no imaginada hasta el momento. La evolución de los sistemas operativos ha incrementado también las posibilidades de estos sistemas, permitiendo las estructuras multipuesto gracias a los sistemas de red informáticos.

En el mundo de Internet de las comunicaciones industriales ahora es posible Conectarse con un sistema de control situado en cualquier lugar del mundo gracias a la tecnología Web-Server: un ordenador dotado de un explorador y la dirección IP (Internet Protocol), del sistema que queremos visualizar serán suficientes.

Refiriéndonos a la definición del sistema SCADA, observamos que no se trata de un sistema de control, sino de una utilidad software de supervisión o monitorización, que realiza la tarea de interface entre los niveles de control (PLC) y los de gestión a un nivel superior.

Las características para que su uso sea perfectamente aprovechado son los siguientes:

- Completa funcionalidad de manejo y la visualización en sistema operativo sobre cualquier computadora estándar.
- Arquitectura abierta donde permita combinaciones con aplicaciones estándar y de usuario, y deje a los integradores crear soluciones de mando y supervisión optimizadas
- Instalación sencilla, hardware de fácil manejo y con interfaces amigables con el usuario.
- Integración con las herramientas ofimáticas y de producción.
- Capaz de crecer o adaptarse según las necesidades cambiantes de la empresa, es decir fácilmente escalable y configurable
- Ser independiente del sector y la tecnología.
- Funciones de mando y supervisión integradas.
- Comunicaciones flexibles para poder comunicarse con total facilidad y de forma transparente al usuario con el equipo de planta y con el resto de la empresa (redes locales y de gestión).

La topología (su distribución física) de un sistema SCADA variará adecuándose a las características de cada aplicación. Unos sistemas



funcionarán bien en configuraciones de bus, otros en configuraciones de anillo, otros necesitarán equipos redundantes debido a las características del proceso, etc. para comunicación con bases de datos, lenguaje estándar integrado como VB (Visual Basic) o C, acceso a funciones y datos mediante API (Application Programming Interface; Interfaz de Programación de Aplicaciones.)

3.2. Objetivos.

Los sistemas SCADA y todas las que hayan reemplazar, se conciben principalmente como una herramienta de supervisión y mando. Entre sus objetivos podemos destacar:

Economía (ahorro), accesibilidad, mantenimiento, ergonomía, gestión, flexibilidad y conectividad.

La IEEE define como sistema abierto todo aquel que proporciona los medios para poder funcionar correctamente con otros sistemas que operen bajo las mismas especificaciones de éste, siendo estas especificaciones de dominio público.

Todos los sistemas, de mayor o menor complejidad, orientados a lo anteriormente dicho, aparecen bajo uno de los nombres más habituales para definir esta relación:

MMI: Man Machine Interface, Interfase Hombre-Máquina.

HMI: Human Machine Interface, Interfase Humano-Máquina.

Que se definen como el aparato que presenta los datos a un operador (humano) y a través del cual éste controla el proceso.



3.3. Lo que puede ofrecer.

- Monitorización

Representación de datos en tiempo real a los operadores de planta.

Se leen los datos de los autómatas (temperaturas, velocidades, detectores...etc.).

Una máquina simple, una instalación hidroeléctrica, un parque eólico, pueden ser vigilados desde muchos kilómetros de distancia.

- Supervisión

Mando, observación y adquisición de datos de un proceso y herramientas de gestión para la toma de decisiones (mantenimiento predictivo, por ejemplo). Además tendrá la capacidad de ejecutar programas que puedan supervisar y modificar el control establecido y, bajo ciertas condiciones, anular o modificar tareas asociadas a los autómatas.

Evita una continua supervisión humana.

- Observación del proceso mediante la adquisición de datos. La visualización de los estados de las señales del sistema (alarmas y eventos). Reconocimiento de eventos excepcionales acaecidos en la planta y su inmediata puesta en conocimiento a los operarios para efectuar las acciones correctoras pertinentes. Además, los paneles de alarma pueden exigir alguna acción de reconocimiento por parte del operario, de forma que queden registradas las incidencias.

- Mando, que los operadores tengan la posibilidad de poder cambiar consignas u otros datos claves del proceso directamente desde la computadora (marcha, paro, modificación de parámetros...). Se escriben datos sobre los elementos de control.

Registro y grabación de acciones o recetas. En varios procesos se utilizan combinaciones de variables que son siempre las mismas. Este sistema de recetas permite configurar toda una planta de producción ejecutando un solo comando.

- Garantizar la seguridad de los datos, el envío y la recepción de datos, debe de estar suficientemente protegido de inserciones no



deseadas, intencionadas o no intencionadas (fallos en la programación, intrusos, situaciones inesperadas, etc.).

- Garantizar la seguridad en los accesos, registrando todos los accesos y acciones llevadas a cabo por cualquier operador, restringiendo zonas de programa comprometidas a usuarios no autorizados
- Viabilidad para programación numérica, esto permite realizar cálculos aritméticos de elevada resolución sobre la CPU del ordenador (lenguajes de alto nivel, C y Visual Basic, generalmente).

3.4. Prioridades de un sistema SCADA.

Hablando de un sistema SCADA no se debe olvidar que hay algo más que la información desplegada en pantalla o de cómo se observa dicha información de nuestra instalación. Entre éstas se encuentran multitud de elementos de regulación y control, sistemas de comunicaciones y múltiples utilidades de software que pretenden que el sistema funcione de forma eficiente y segura.

Las más evidentes ventajas de los sistemas de control automatizado y supervisado (SCADA) se enuncian a continuación:

- Un nivel actual de desarrollo de los paquetes de visualización permite la creación de aplicaciones funcionales sin necesidad de ser un experto en la materia.
- Un PLC en conjunto, está concebido para trabajar en condiciones adversas, proporcionando robustez y fiabilidad al sistema que controla.
- La accesibilidad y modularidad de los autómatas permite adaptarlos a las necesidades actuales y ampliarlos posteriormente si se desea.
- En un programa de PLC, cualquier tipo de sensores y actuadores puede integrarse mediante las múltiples tarjetas de adquisición disponibles (tensión, corriente, sondas de temperatura, etc.).
- Debido a las herramientas de evaluación, se consigue una localización más rápida de errores. Dado esto, se permite minimizar



los periodos de paro en las instalaciones y repercute en la reducción de costes de mantenimiento.

-Un sistema de control remoto (RTU "Remote Terminal Unit") se concibe de modo que pueda funcionar de forma automática, aún sin comunicaciones con la estación maestra.

-El sistema de telemetría permite realizar modificaciones de software en las estaciones remotas (RTU) desde el centro de control.

- Los programas de control pueden documentarse convenientemente de manera que puedan ser fácilmente interpretados por los técnicos de mantenimiento así como un conjunto de manuales de usuario y documentación técnica adecuada que permita el manejo satisfactorio por terceras personas.

-Los sistemas de diagnóstico implementados en los elementos de control informan continuamente de cualquier incidencia en los equipos.

-Los programas de visualización pueden presentar todo tipo de ayuda al usuario, desde la aparición de una alarma hasta la localización de la causa o la parte de esquema eléctrico implicada en la misma. Esto permite reducir los tiempos de localización de averías al proporcionarse información sobre el origen y las causas de los fallos.

-Generación y distribución automática de documentación. El sistema de visualización puede recoger los datos del automático y presentarlos en formatos fácilmente exportables a otras aplicaciones de uso común, tales como hojas de cálculo.

-La integración de sistemas es rápida gracias a los sistemas de comunicación estandarizados.

-La tecnología Web permite el acceso desde cualquier punto geográfico a nuestro sistema de control.

-Los protocolos de seguridad permiten una gestión segura y eficiente de los datos, limitando el acceso a personas no autorizadas.

-Aumento de calidad del producto mediante las herramientas de diagnóstico.

El operador es notificado en el momento en que se detecta una incidencia.



- Reducción de personal permite menor número de equipos de mantenimiento, más reducidos y mejor coordinados gracias a la información proveniente de las estaciones remotas, evaluada en el centro de control.
- Posibilidad de mantenimiento por parte de suministradores locales de servicios.
- Distribución de recursos y control sobre la red permite una mejor coordinación entre las estaciones remotas en caso de fallos en una de ellas.
- Mediante las redes de comunicación, el sistema SCADA se integra en la red corporativa, permite la integración entre los niveles de Campo y Gestión y completa así la estructura CIM (Computer Integrated Manufacturing; Equipo Integrado de Fabricación).

3.5. Entorno.

La automatización de sistemas ha pasado a formar parte del ámbito corporativo y se incluye dentro del contexto empresarial con el objetivo de mejorar la calidad y optimizar la productividad.

La jerarquía en cómo se distribuye el flujo de información dentro de la empresa, es parecida a la conocida pirámide de la automatización CIM.

Planificación de Recursos Empresariales, ERP (Enterprise Resource Planning).

Abarca la parte de gestión: finanzas, compras, ventas, logística. Esto es para conocer los requerimientos previos para planificar la producción a corto, medio y largo plazo, y coordinar compras y logística.

3.6. Gestión de la Producción, MES (Manufacturing Execution System).

Comprende la gestión de calidad, documentación, gestión de producción,

mantenimiento y optimización. Con la finalidad de conocer las existencias de material disponibles para aplicar en el proceso productivo y decidir si hay que planificar nuevas compras y coordinar los ciclos de Mantenimiento Preventivo para conocer la disponibilidad de maquinaria y la capacidad operativa durante el tiempo de producción previsto Control: abarca toda la parte de automatización y control de procesos. Para así conocer el estado operativo de planta Estos se complementan para el flujo de información entre sí mismos (comunicación horizontal) y los otros niveles (comunicación vertical).

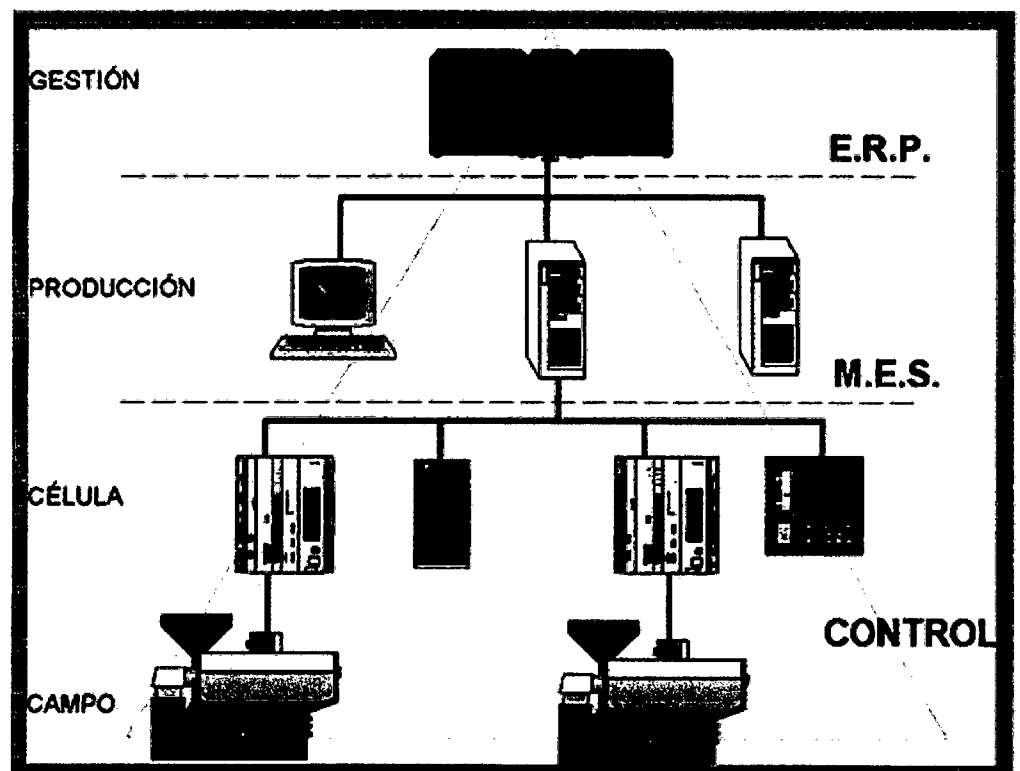


Figura 3.1 Esquema de flujos de información

3.6.1. Pautas para la elección y diseño de un sistema SCADA.

Un sistema de control cualquiera es útil, evidentemente, mientras funcione correctamente. En caso contrario puede crear problemas de forma directa o indirecta La reacción de un sistema ante situaciones



inesperadas determinará su grado de fiabilidad, es decir, el tiempo de operación del mismo, y puede mejorarse mediante el uso de técnicas de diseño adecuadas.

Los parámetros que influyen en las posibilidades de supervivencia se pueden englobar bajo los siguientes denominadores:

- Disponibilidad

Por disponibilidad de un sistema informático se entiende la medida en la que sus parámetros de funcionamiento se mantienen dentro de las especificaciones de diseño. Se basará en dos pilares fundamentales: hardware y software.

- Robustez.

Esto se refiere a un sistema eficiente donde responde ante un fallo de diseño, un accidente o una intrusión, para poder mantener un nivel mínimo requerido de operatividad en el servicio.

- Seguridad.

Sobre estas situaciones el sistema debe permitir establecer estrategias para prevenir, detectar y defenderse de acciones no deseadas (intencionadas o no).

- Prestaciones.

Se refieren primordialmente al tiempo de respuesta del sistema. Esto es, comprende toda una serie de funciones y utilidades encaminadas a establecer una comunicación lo más clara posible entre el proceso y el operador.

- Mantenimiento.

Reducir al mínimo los tiempos de mantenimiento siempre y cuando el sistema esté provisto de unas buenas herramientas de diagnóstico que permitan realizar tareas de mantenimiento preventivo, modificaciones y pruebas de forma simultánea al funcionamiento normal del sistema.

- Escalabilidad.

Relacionado con la posibilidad de ampliar el sistema con nuevas herramientas o

Prestaciones y los requerimientos de tiempo necesarios para implementar dichas coberturas.



3.6.2. Arquitectura de un sistema SCADA.

Con el desarrollo de la computadora todo el control de la automatización del proceso se encuentra ahí mismo. De esta manera, el sistema queda dividido en tres bloques principales:

*Software de adquisición de datos y control (SCADA).

*Sistemas de adquisición y mando (sensores y actuadores). *Sistema de interconexión (comunicaciones).

Un sistema SCADA es una aplicación de software especialmente diseñada para funcionar sobre ordenadores en el control de producción que proporciona comunicación entre los dispositivos de campo, llamados también RTU (Remote Terminal Unit o Unidades Remotas), donde se pueden encontrar elementos tales como controladores autónomos o autómatas programables, y un centro de control o Unidad Central (MTU, Master Terminal Unit), donde se controla el proceso de forma automática desde la pantalla de uno o varios ordenadores.

La estructura funcional de un sistema de visualización y adquisición de datos obedece generalmente a la estructura Maestro-Esclavo. La estación central se comunica con el resto de estaciones, requiriendo de éstas una serie de acciones o datos.

3.6.3. Interface Hombre-Máquina (HMI, MMI).

Comprende la función de un Panel Sinóptico (control y representación gráfica) que es la de representar, de forma simplificada el sistema en supervisión y control.

Los paneles sinópticos en principio eran de tipo estático, colocados en grandes paneles plagados de indicadores y luces. Posteriormente han ido evolucionando, junto con el software, en forma de representaciones gráficas en pantallas de visualización. En los sistemas complejos suelen aparecer los terminales múltiples, que

permiten la visualización, de forma simultánea, de varios sectores del sistema.

Lo importante es mantener la forma antigua del Panel Sinóptico, pues la representación del sistema completo es más clara para el usuario al tenerla presente y no le perjudique los eventuales fallos de controladores gráficos o alimentación de componentes.

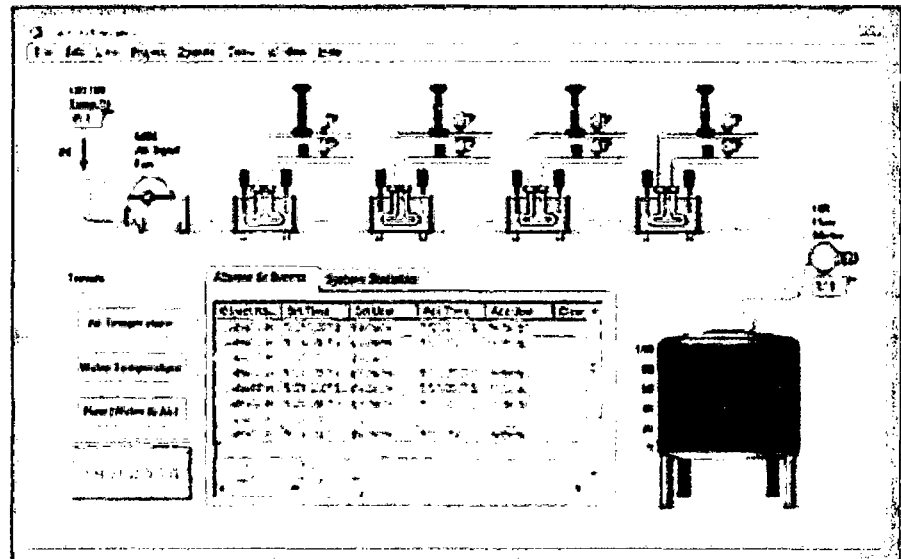


Figura 3.2. Visualización grafica de un sistema SCADA

3.7. Utilización de componentes físicos y software para el desarrollo.

3.7.1. Tipos de conexión e interfaz para la comunicación.

3.7.2. Modelo OSI.

Un primer aspecto a considerar es la transmisión de datos se efectúa por lo general en serie, por motivos de economía de conexiones (sólo algunos buses locales serán de tipo paralelo).

La normalización en un campo que se desarrolla tan rápidamente como el de las comunicaciones, es ciertamente difícil y no puede ser muy rígida si no se quiere que quede obsoleta a causa de la continua innovación.



ISO (Organización Internacional de Normalización). Ha desarrollado la norma marco más general, denominada Modelo OSI (Open Systems Interconnection), pensada para abarcar desde redes locales hasta las grandes redes de paquetes conmutados. Las reglas de protocolo consistirán, pues, en relaciones de tipo horizontal que deben ser compatibles entre cada par de terminales enlazados,

El modelo OSI pretende subdividir las tareas del proceso de diálogo a través de máquinas digitales.

Una parte de dichas tareas del sistema de comunicación va dirigida a dar soporte al usuario (niveles 7, 6 Y 5), Y otra parte va dirigida a facilitar el flujo de información digital entre terminales y/o máquinas (niveles 4, 3, 2 Y 1).

Tareas asignadas a cada uno de los niveles OSI

NIVEL 7: APLICACIÓN. Este nivel se encarga de proporcionar un entorno que facilite el entendimiento entre usuarios de distintas máquinas digitales a nivel temático, sin importarle medios ni protocolos de comunicación.

NIVEL 6: PRESENTACIÓN. Se encarga de facilitar la comunicación, a nivel de lenguaje y formato de presentación, entre el usuario y la máquina digital que le va a permitir el acceso a la red.

NIVEL 5: SESIÓN. En un diálogo interactivo, las tareas encargadas a este nivel consisten en controlar la comunicación, arbitrando en cada instante quién debe transmitir y quién debe recibir. En particular, se encarga también de señalar el inicio y el final de la comunicación.

NIVEL 4: TRANSPORTE. Este nivel es el responsable de establecer un medio de comunicación y garantizar la transferencia de información sin errores en ambos sentidos. Apoyándose en los niveles inferiores, actúa como un gestor capaz de interpretar las direcciones, fraccionar si es preciso los paquetes muy largos y llevar los mensajes a su destino correcto, sin precisar cuál va a ser la ruta o los medios utilizados para ello.

NIVEL 3: RED. Este nivel es el responsable real del encaminamiento de mensajes entre nodo y nodo, a través de un medio físico, sin

importarle cuál sea dicho medio ni el contenido del mensaje. En el caso de comunicaciones digitales el medio podrá ser por ejemplo, cable, radio, fibra óptica, etc.

NIVEL 2: ENLACE. El nivel de enlace es el responsable de mantener la comunicación entre cada par de nodos de la red, apoyándose para ello en un medio físico de conexión.

NIVEL 1: FÍSICO. El nivel físico se encarga de disponer de los medios materiales que garantizan el enlace entre nodos (cables, fibra óptica, modems, etc.) y de que ambos se entiendan a nivel de interpretar los unos y ceros de la comunicación digital (codificación de bits por niveles de tensión, por tonos de frecuencia, etc.). El nivel físico sólo entiende de unos y ceros, sin importarle qué representan.

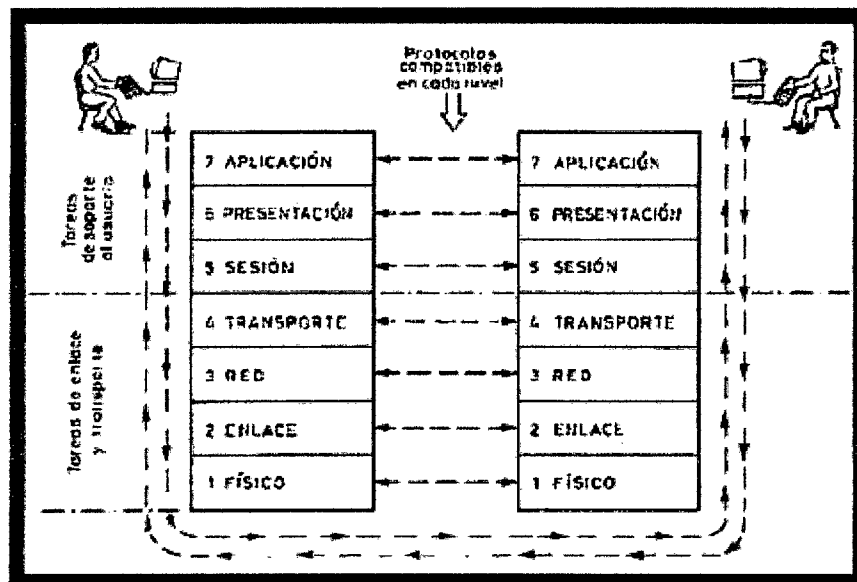


Figura 3.3 Niveles OSI

Las redes de comunicación industriales y más particularmente las redes de autómatas a nivel de planta, se estructuran habitualmente como redes de tipo local de bajo nivel, denominadas también buses de campo y suelen utilizar sólo los niveles 1, 2, 3 Y 7 de modelo OSI, pero pueden enlazarse con redes superiores LAN (Local Area Network: Red local que comunica varios terminales, por lo general a corta distancia del orden de 1 km). y WAN (Wide Area Network: Red de Área Amplia cubriendo de 100 hasta unos 1000 km).



3.7.3. RS-232.

El enlace RS-232C, recibe su nombre de la norma americana de EIA (Electrical Industries Association), equivalente al estándar europeo V.24 de CCITT. Este estándar fue previsto en un principio para la comunicación entre un terminal (DTE) y un modem (DCE) pero, posteriormente, han surgido una multitud de variantes, aplicadas de forma generalizada a enlaces punto a punto entre terminales de datos (DTE ↔ DTE).

La norma se ocupa, esencialmente, del aspecto físico de la conexión, indicando los tipos de conectores, niveles de señal y las señales de protocolo a nivel de hardware (señales de «handshaking»). En concreto, el enlace definido por la norma básica utiliza 25 líneas (datos + control) y conectores tipo DB-25.

La denominación V.24 de la norma equivalente del CCITT viene del hecho de que los niveles de tensión utilizados son de +12 V Y -12 V (0 Y 1 lógicos, respectivamente). En realidad, existe una banda de tolerancia para estas tensiones.

Actualmente existe una gran diversidad de dispositivos digitales (ordenadores, aparatos de medida, controladores industriales, etc.) que disponen de un canal de comunicaciones serie que suele designarse como RS-232, aunque ciertamente utilizan sólo una mínima parte de las señales definidas en la norma original. Este hecho ha dado lugar a algún desconcierto y falta de compatibilidad entre terminales que teóricamente obedecen a la misma norma pero que, en muchas ocasiones, no utilizan las mismas señales de control «handshaking».

Así por ejemplo, los aspectos básicos de la norma han sido adoptados para los enlaces entre terminales industriales, autómatas y ordenadores personales (PC) pero, en dichas aplicaciones, no suelen emplearse todas las señales previstas por la norma original y, por ello, muchos utilizan un conector de 9 patillas, tipo DB-9, en lugar de conector DB-



3.7.4. RS-485.

RS-485 o también conocido como EIA-485, que lleva el nombre del comité que lo convirtió en estándar en 1983. Es un protocolo de comunicaciones en bus de la capa física del Modelo OSI.

Está definido como un sistema en bus de transmisión multipunto diferencial, es ideal para transmitir a altas velocidades sobre largas distancias y a través de canales ruidosos, ya que reduce los ruidos que aparecen en los voltajes producidos en la línea de transmisión. El medio físico de transmisión es un par entrelazado que admite hasta 32 estaciones en 1 solo hilo, con una longitud máxima de 1.200 metros operando entre 300 y 19200 bps y la comunicación half-duplex (semiduplex). Soporta 32 transmisiones y 32 receptores. La transmisión diferencial permite múltiples drivers dando la posibilidad de una configuración multipunto. Al tratarse de un estándar bastante abierto permite muchas y muy diferentes configuraciones y utilizaciones.

Desde 2003 está siendo administrado por la Telecommunications Industry Association (TIA) y titulado como TIA-485-A.222

ESPECIFICACIONES REQUERIDAS.

- Interfaz diferencial
- Conexión multipunto
- Alimentación única de +5V
- Hasta 32 estaciones (ya existen interfaces que permiten conectar 128 estaciones)
- Velocidad máxima de 10 Mbps (a 12 metros)
- Longitud máxima de alcance de 1.200 metros (a 100 Kbps)
- Rango de bus de -7V a +12

Cabe señalar que algunos ordenadores portátiles como de escritorio - actuales-, no disponen de entradas para RS-232 o RS-485, solo para entradas USB, Universal Serial Bus (bus universal en serie), por lo

que existen convertidores exclusivos para cada tipo de norma. Estos al utilizarse necesitarían para su manejo drivers (software o programa que sirve de intermediario entre un dispositivo de hardware y el sistema operativo), que hacen el mismo papel que si tuviera el puerto RS-232.

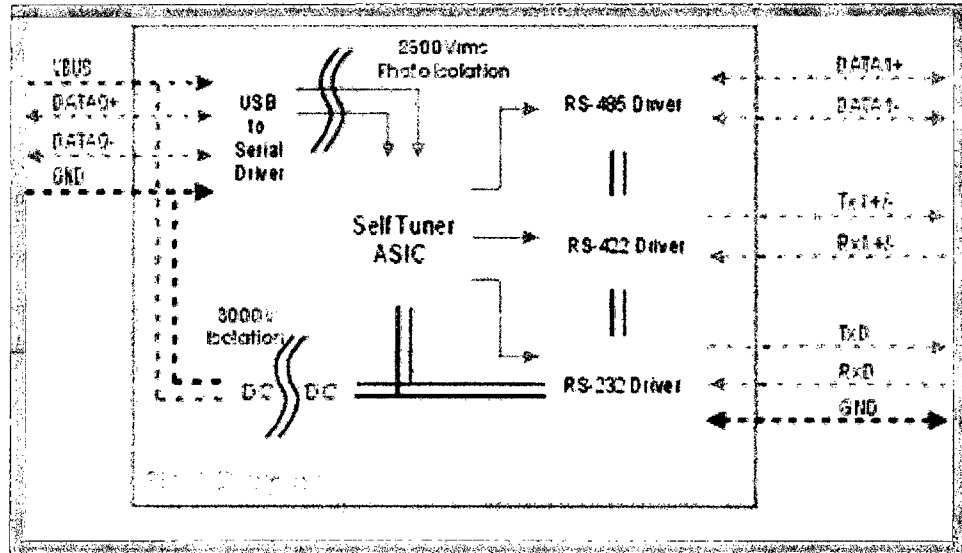


Figura 3.4. Diagrama básico convertidor USB a RS232/RS485

3.7.5. Aspectos para la comunicación.

Las comunicaciones en el entorno industrial suelen basarse en redes más reducidas del tipo LAN y aun manteniendo la compatibilidad con el modelo, se pueden soslayar las funciones de alguno de los niveles OSI o agrupar otras de niveles distintos en uno sólo para simplificar el sistema.

En cualquier red de comunicación dentro de los niveles más bajos, debemos distinguir dos aspectos: Entendiendo por topología de red a la disposición física de las distintas terminales que la componen y la forma en que se encuentran enlazados por el medio físico.

Dentro de la estructura de una red industrial se encuentra el enlace físico Nivel 1 OSI (cables, fibra óptica, enlace radio) y el nivel lógico Nivel 2 OSI (reglas para dialogo, reglas para transito).

La elección de la topología tiene una fuerte influencia sobre las prestaciones de la red y condiciona muchas veces sus posibilidades de ampliación, de cambio y el compartir de los recursos.

Las topologías básicas en redes locales son tres: Estrella, Anillo y Bus. Lo que entendemos por medio físico es el conjunto de elementos de hardware destinados a transmitir las señales eléctricas u ópticas entre los diversos nodos de una red. En el caso de redes LAN, el medio físico lo forman esencialmente dos grupos de componentes: interfaces y medios físicos.

Una de las características esenciales del medio físico, independientemente de cual sea el número de canales que es capaz de transmitir con el mismo medio físico, es el tipo de enlace: banda base y banda ancha.

Para transmisión de señales de proceso a distancias muy grandes se pueden conectar estaciones a la red a través de modems unidos a líneas telefónicas o mediante estaciones de radio.

Desde el punto de vista físico, estos sistemas representan sólo una interfaz en la vía de comunicación.

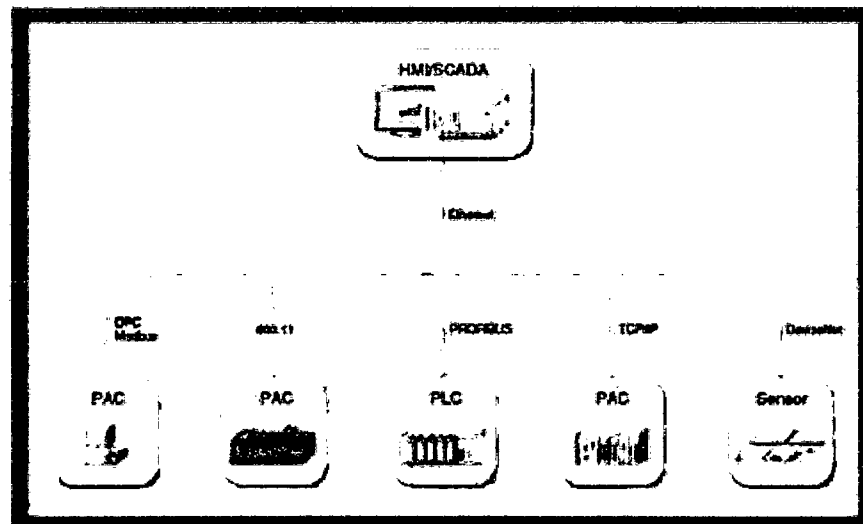


Figura 3.5. Protocolos de comunicación para interfaz

La estructura lógica de una red consiste en la forma en que se asignan y cumplen las tareas del nivel de enlace del modelo OSI



(nivel 2). Estas tareas pueden dividirse básicamente en dos grandes grupos:

- a) Control de acceso al medio (MAC, Media Access Control).
- b) Enlace lógico entre terminales (LLC, Logic Link Control).

El conjunto de todas estas tareas es lo que muchas veces se conoce en las redes locales como «protocolo», aunque hay quien prefiere decir que el protocolo es esto más algunas funciones desarrolladas a nivel de hardware, donde ciertas señales de hardware implicaban el bloqueo de la transmisión o de la recepción.

- Control de acceso al medio (MAC)

El medio físico más frecuente en las redes locales es un bus compartido por las distintas estaciones que la forman. Esto hace que deba resolverse el uso del mismo para transmitir una u otra estación sin que aparezcan conflictos por intentos de ocupación simultánea. Son dos las estrategias más generales de control de asignación de dicho medio físico:

- Control centralizado (maestro fijo).
- Control descentralizado (maestro flotante).
- Control lógico de enlace (LLC)

En el caso de una red local, el subnivel LLC controla el enlace desde el punto de vista lógico, es decir, establece el protocolo para que la estación transmisora pueda identificarse, establece el formato de mensaje para que la estación o estaciones destinatarias puedan reconocer que el mensaje va dirigido a ellas, permite identificar el inicio de mensaje y su final y añade caracteres para control de errores. Por lo que el nivel de protocolo LLC controla «quién habla y con quién» y «cuándo empieza y cuándo termina el enlace». Nótese que para redes WAN algunas de estas funciones corresponderían al nivel OSI 3 (red), pero a nivel local este papel lo ejerce totalmente el nivel OSI 2.

En cuanto a los tipos de enlace posibles podemos distinguir:

- 1) Enlace punto a punto. Implica direccionamiento de una estación única por parte de la estación transmisora.



- 2) Enlace con un grupo. Un transmisor puede emitir un mensaje dirigido a un grupo concreto de destinatarios.
- 3) Enlace difundido. Un transmisor puede emitir un mensaje dirigido a todas las estaciones de la red.

3.7.6. Protocolo OPC.

La tecnología OPC surge como una necesidad de establecer un mecanismo estándar que permita la comunicación entre numerosas fuentes de datos, ya sea desde dispositivos montados en campo o desde bases de datos instaladas en equipos del cuarto de control.

Cabe hacer mención que la tecnología OPC es el resultado de la evolución de herramientas que en un principio patentó Microsoft, conocida como OLE (Object Linking and Embedding; Incorporación y Vinculación de Objetos), la cual hace posible el intercambio de componentes entre diversas aplicaciones y es posible generar un solo documento donde se integre texto, gráficas resultantes de hojas de cálculo, esquemas o dibujos, etc. además de estar sometidos a un ambiente similar y compartir herramientas como un revisor ortográfico o un generador de ecuaciones: □ OPC (Incorporación y Vinculación de Objetos para el Control de Procesos.)

Esta tecnología se extrapoló al uso de herramientas de productos de fabricantes diferentes a Microsoft, como AutoCad, Matlab etc. Finalmente esta tecnología es expuesta a aplicaciones de control y administración de los procesos de producción logrando ahora la "compatibilidad" de sus herramientas con una aplicación comercial como Word, Excel, Power Point, Visual Basic etc.

La tecnología OPC en los medios de producción

Las comunicaciones entre los diversos equipos de campo se pueden esquematizar a través de los siguientes niveles:

Administración de los dispositivos de campo. Con el surgimiento de los dispositivos de campo "inteligentes", ahora es posible tener una

gran cantidad de información, como el valor de una o más variables de proceso, parámetros de configuración, estado del dispositivo etc. Y la cual debe ser almacenada o presentada al usuario o alguna otra aplicación de una manera consistente.

Administración del proceso. El manejo de sistemas de control distribuido o sistemas SCADA para el control, monitoreo, control de supervisión, y gestión de la información de un proceso completo permite manejar electrónicamente datos que anteriormente eran recopilados manualmente.

Administración empresarial. La integración, gestión y análisis de la información obtenida desde las etapas anteriores permite tomar decisiones adecuadas que impactan directamente en la calidad y cantidad de producción.

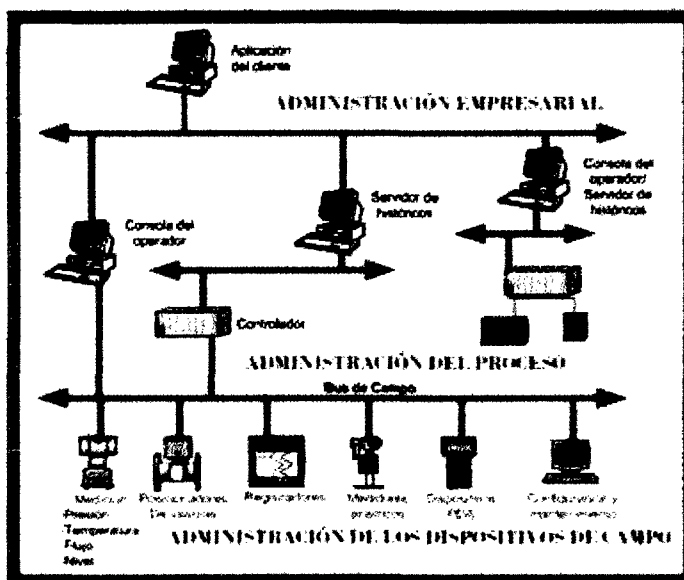


Figura 3.6. Esquematización de comunicación para los niveles de flujo de información

Para lograr que estos niveles se interconecten eficientemente, es necesario que los diversos fabricantes sean capaces de acceder a los datos generados desde los dispositivos de campo desde múltiples medios empleando herramientas como los sistemas SCADA, bases de datos, hojas de cálculos, etc. La clave está en generar una arquitectura de comunicaciones efectiva y abierta concentrándose en el acceso a datos y no el valor o contenido de los datos.

Lo que se necesita es una forma común para que las aplicaciones puedan acceder a los datos desde diversos medios como un dispositivo o una base de datos.

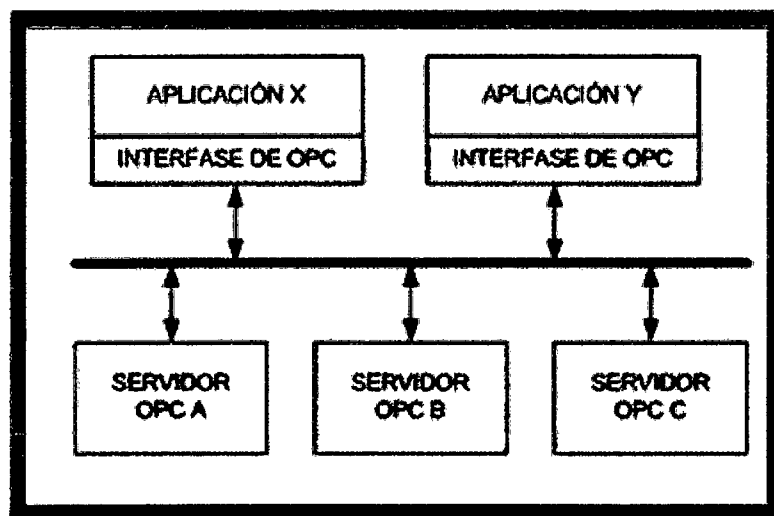


Figura 3.7. Esquema servidor OPC.

OLE for Process Control, traza una línea entre los proveedores del hardware y desarrolladores de software. La tecnología OPC es un mecanismo que permite traer datos desde una fuente (servidor) y ponerlos a disposición de cualquier aplicación cliente de forma estándar. Un fabricante puede ahora desarrollar un servidor optimizado para comunicarse continuamente con la fuente (cliente)/dispositivo de datos.

Suministrando el servidor con la interfase OPC permitirá a cualquier cliente acceder a estos dispositivos.

OPC está diseñado para la ejecución de aplicaciones cliente que permita el acceso a datos obtenidos desde los dispositivos de campo de una manera consistente. Con esto hace que:

- * Los fabricantes de software únicamente tienen que diseñar un conjunto de componentes de software para que los clientes lo utilicen en sus aplicaciones.
- * Los clientes tendrán más opciones con las cuales desarrollar un sistema integrado de manufactura de clase mundial.
- * Con OPC, la integración de sistemas en un ambiente de cómputo heterogéneo se tornará en una tarea simple y se lograrán arquitecturas a gran escala.

Un objetivo primario para OPC es generar especificaciones que permitan prestaciones como: Manejo de eventos y alarmas, acceso de datos en línea e históricos.

Un servidor OPC puede ser de diversos fabricantes, El vendedor debe facilitar el código para determinar el dato y dispositivo para el cual cada servidor tiene acceso, así como el nombre de los datos y los detalles acerca de cómo el servidor físicamente accede a los datos. Es decir una aplicación cliente debe tener la posibilidad de conectarse con una aplicación servidor OPC aunque sean de uno o más fabricantes.

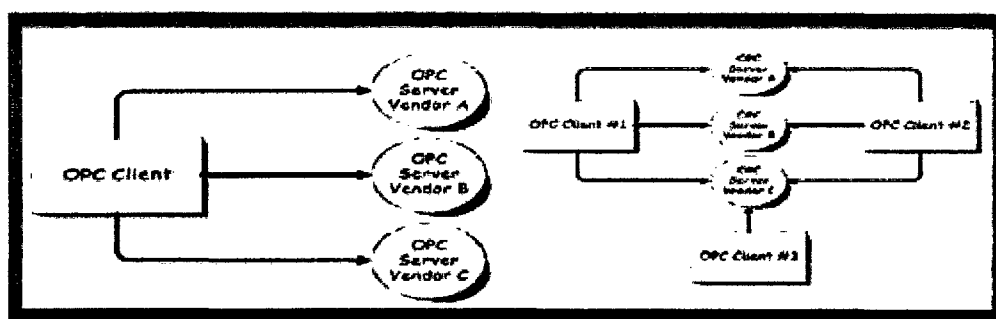


Figura 3.8. Esquema servidor-cliente OPC.

Las especificaciones de OPC implican propiamente dicho el manejo y caracterización de interfaces y no su implementación.



La principal es la frecuencia de transferencia de datos entre el servidor y los diversos dispositivos de campo o alguna base de datos.

Una aplicación cliente OPC se comunica con un servidor OPC a través de la interface de automatización desarrollada por el usuario.

El servidor OPC debe implementar la interface cliente y opcionalmente podría implementar la interface de automatización.

3.8. PLC's

3.8.1. Conceptos básicos de PLC's

De acuerdo con la definición de la "Nema" (National Electrical Manufacturers Association) un controlador de lógica programable es: "Un aparato electrónico operado digitalmente, que usa una memoria programable para el almacenamiento interno de instrucciones para implementar funciones específicas, tales como lógica, secuenciación, registro y control de tiempos, conteo y operaciones aritméticas para controlar, a través de módulos de entrada/salida digitales (ON/OFF) o analógicos (1 5 VDC, 4 20 mA, etc.), varios tipos de máquinas o procesos.

Secuencia de Operaciones en un PLC.

- a) Al encender el procesador, este efectúa un auto chequeo de encendido e inhabilita las salidas. Entra en modo de operación normal.
- b) Lee el estado de las entradas y las almacena en una zona especial de memoria llamada tabla de imagen de entradas
- c) En base a su programa de control, el PLC modifica una zona especial de memoria llamada tabla de imagen de salida.
- d) El procesador actualiza el estado de las salidas "copiando" hacia los módulos de salida el estado de la tabla de imagen de salidas (estas controlan el estado de los módulos de salida del PLC, relay, triacs, etc.).
- e) Vuelve paso b)

A cada ciclo de ejecución de esta lógica se le denomina ciclo de barrido (scan) que generalmente se divide en:

* I/O (entradas/salidas) scan

* Program Scan

El direccionamiento de entradas y salidas en la programación de un PLC consiste en informar a la CPU, de acuerdo al formato empleado por el fabricante, la dirección lógica de las diferentes entradas y salidas.

El direccionamiento de I/O varía de marca en marca, sin embargo, la mayoría adopta una nomenclatura dividida en campos que proporciona información sobre la ubicación física de la entrada o salida.

Como existen gran cantidad de I/O y estas pueden estar alojadas en diferentes módulos, nace la necesidad de indicarle a la CPU, mediante nuestro programa, la referencia exacta de la entrada o salida con la que queremos interactuar. Al mecanismo de identificación de I/O en los PLC se le denomina direccionamiento de entradas y salidas.

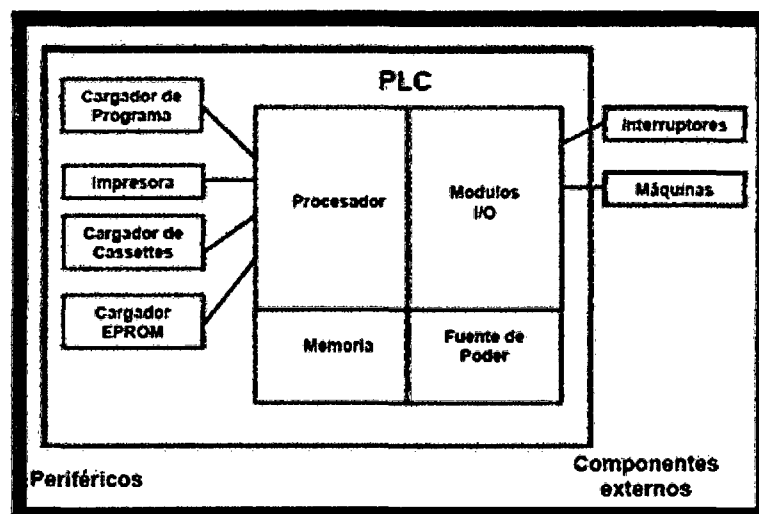


Figura 3.9. Arquitectura interna del PLC

Un esquema de escalera o de contactos está constituido por varias líneas horizontales que contienen símbolos gráficos de prueba ("Contactos") y de acción ("Bobinas"), que representan la secuencia lógica de operaciones que debe realizar el PLC. La programación en Ladder de alguna forma se ha ido normalizando y ya casi la mayoría



de los fabricantes presentan y programan sus PLC en formatos muy parecidos.

La IEC 1131-3 es una norma aprobada como estándar internacional para los lenguajes de programación de PLCs. Dicha norma recoge todos los tipos de operandos de uso común en PLCs. En su apartado 2.2 (Representación exterior de los datos) se establece que dicha representación deberá consistir en literales numéricos (enteros y reales),

literales de cadenas de caracteres y literales de tiempo. A partir de ello en el sistema ISaGRAF (IEC 1131-3 compatible) de CJ International se agrupan en cuatro tipos básicos: Booleano, Analógico, Temporizado y Mensaje. Además, tanto la norma como el ISaGRAF establecen como lenguajes de programación:

- ✦ LD: Diagrama a contactos o de escalera (Ladder Diagram).
- ✦ IL: Lista de Instrucciones (Instruction List).
- ✦ FBD: Diagrama de Bloques Funcionales (Function Block Diagram).
- ✦ ST: Texto Estructurado (Structured Text).
- ✦ SFC: Carta de Funciones Secuenciales (Sequential Function Chart).

Tendencias en PLCs:

- ✦ Sistemas abiertos.
- ✦ Comunicaciones.
- ✦ Desafío competitivo con las PCs.
- ✦ Incremento de las capacidades analógicas.

Estos son algunos símbolos básicos utilizados para el diagrama de escalera.

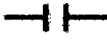
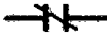




Contactos	Relevador	Normalmente Abierto	
		Normalmente Cerrado	
Bobinas	Relevadores		
	Solenooides		
Motor	Armadura DC		
Focos Piloto			

Figura 3.10. Simbología básica para diagrama de escalera

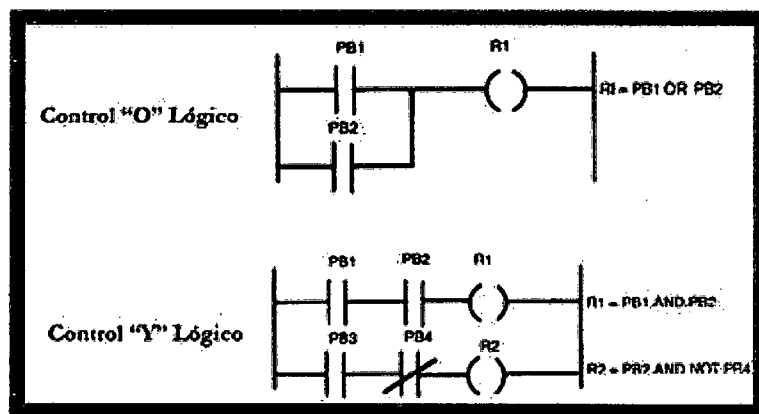


Figura 3.11. Secuencia lógica O, Y.

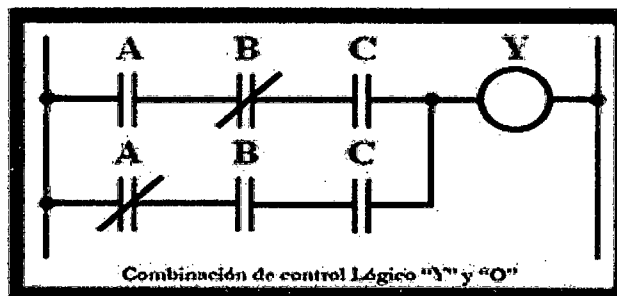


Figura 3.12. Combinación lógica O, Y

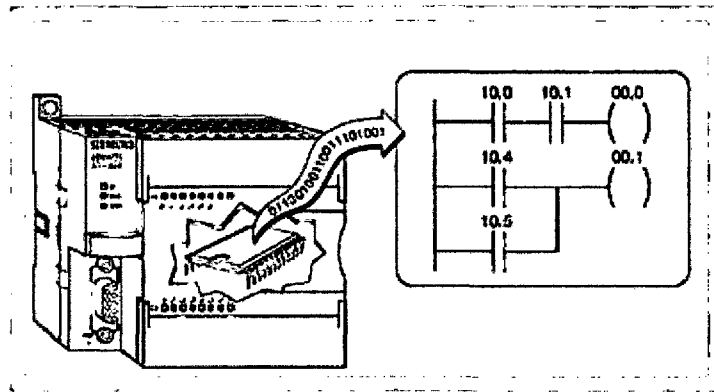


Figura 3.13. Visualización básica de cómo opera un PLC.

3.8.2. Especificaciones técnicas de la familia PLC S7-300.

Este es un mini autómatas de SIEMENS ideado especialmente para aumentar la cadencia y disminuir sensiblemente los tiempos ciclo y de respuesta y aumentar la calidad del proceso, opera más allá de los límites de prestaciones anteriores, asegurando la adquisición y tratamiento de señales (analógicas o digitales) a cualquier velocidad y en cualquier forma en que se presenten, de allí que es ideal para usarlo en maquinarias de embalaje y en máquinas herramientas, sector agroalimentario o en industria química o farmacéutica.

Posee una CPU cuya velocidad es 100 veces mayor a las convencionales (la más potente de sus 5 CPU no necesita más de 0,3 ms para ejecutar 1024 instrucciones binarias y no mucho más al procesar palabras), una Memoria de programa de 16K instrucciones de capacidad máxima, 1024 entradas/salidas digitales y 32 módulos, dentro de un solo sistema (para tareas especiales se ofrecen módulos específicos), alta potencia de cálculo con hasta aritmética de 32 bits en coma flotante e interfaces multipunto o puerto MPI.

Pequeño, extremadamente rápido y universal son las características más importantes de éste PLC, además de su modularidad, sus numerosos módulos de extensión, su comunicabilidad por bus, sus

funcionalidades integradas de visualización y operación así como su lenguaje de programación bajo entorno Windows 95 en adelante.

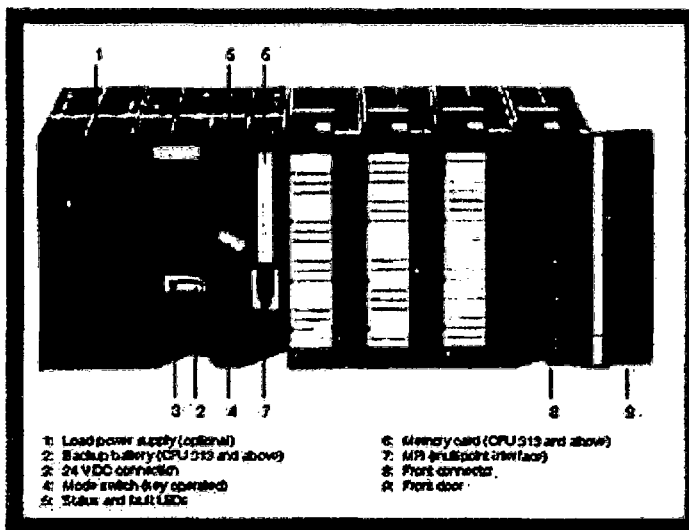


Figura 3.14. Principales Componentes del PLC

El autómata programable consta de los siguientes componentes:

- ✦ Unidad central de procesamiento (CPU), que constituye el "cerebro" del sistema y toma decisiones en base a la aplicación programada.
- ✦ Módulos para señales digitales y analógicas (I/O)
- ✦ Procesadores de comunicación (CP) para facilitar la comunicación entre el hombre y la máquina o entre máquinas. Se tiene procesadores de comunicación para conexión a redes y para conexión punto a punto.
- ✦ Módulos de función (FM) para operaciones de cálculo rápido.
- ✦ Existen otros componentes que se adaptan a los requerimientos de los usuarios:
- ✦ Módulos de suministro de energía
- ✦ Módulos de interfaces para conexión de racks múltiples en configuración multi-hilera
- ✦ En los módulos de entrada pueden ser conectados:
- ✦ Sensores inductivos, capacitivos, ópticos
- ✦ Interruptores



- ✚ Pulsadores
- ✚ Llaves
- ✚ Finales de carrera
- ✚ Detectores de proximidad.

En los módulos de salida pueden ser conectados:

- ✚ Contactares.
- ✚ Electroválvulas.
- ✚ Variadores de velocidad.
- ✚ Alarmas.

Descripción de los 5 Módulos Centrales

El sistema modular comprende de cinco CPU para distintas exigencias, módulos de entradas y salidas analógicas y digitales, módulos de función de conteo rápido, posicionamiento de lazo abierto y lazo cerrado, así como módulos de comunicación para el acoplamiento a redes en bus.

La CPU más potente puede tratar 1024 instrucciones binarias en menos de 0,3 ms. Pero como las instrucciones puramente binarias constituyen más bien la excepción, tenemos que mencionar los tiempos de ejecución de las instrucciones mixtas: 65% de instrucciones con bits y un 35% con palabras, el más rápido de los autómatas puede con 1K en sólo 0,8 ms.

Otro detalle es la simplicidad de diagnóstico. Los datos de diagnóstico de todo el autómata están fijamente almacenados en la CPU (hasta 100 avisos). Estos datos pueden consultarse centralizadamente en la CPU, ya que todos los módulos relevantes son accesibles vía interfaces MPI de ésta, lo que permite ahorrarse gastos suplementarios y evita molestas manipulaciones de conectores.

En una configuración de PLC en red, el puesto central de mando puede acceder directamente a cualquier CPU y a cualquier módulo de función, a cualquier panel de operador y a cualquier procesador de comunicaciones de la red, todo ello sin hardware ni software adicional.



El sistema de diagnóstico inteligente de la CPU se activa al reemplazar un módulo: se encarga de verificar si la configuración del autómata es aún compatible y evita así funcionamientos anómalos en la instalación, incluso la destrucción de módulos.

Además realiza automáticamente el registro de la hora y la memorización de los fallos, contribuyendo así a un diagnóstico rápido y puntual a posteriori cuando ya no se manifieste más el defecto o cuando éste sea de naturaleza esporádica.

- Tipos de Módulos Disponibles

Tanto si son analógicas o digitales como si son entradas o salidas, éste autómata trata las señales a medida que se van presentando.

- Módulos de entradas digitales

Los módulos de entradas digitales convierten las señales digitales externas del proceso al nivel interno del autómata.

Por ejemplo, si se va a utilizar detectores de proximidad o finales de carreras con una tensión de 24 VDC, se debe elegir el módulo de entrada de 24 V., que le ofrece 16/32 entradas y conecta los sensores con separación galvánica y en grupos de 8 entradas con contacto común.

Para señales de corriente alterna de 120 ó 230 V., existe un módulo de 8 canales que se encarga de traducir las señales para que las pueda leer el autómata.

- Módulos de salidas digitales

Los módulos de salidas digitales convierten las señales internas del S7-300 en señales externas adaptadas al proceso.

Por ejemplo, si desea conectar electroválvulas, contactores, pequeños motores, lámparas, etc., entonces necesitará un módulo de éste tipo. En lo que respecta a los actuadores de 24 VDC, como por ejemplo contactores y válvulas, el autómata ofrece varias alternativas como ser: desde módulos de 16/32 canales y 0,5 A. Con separación galvánica hasta módulos de relé de 8 a 16 canales.



- Módulos de entradas analógicas

Este convierte las señales analógicas en señales digitales que el autómata procesa internamente. Se puede conectar sensores y emisores de señal de tipo tensión o intensidad, resistencia, así como termopares y termoresistencias y se puede elegir entre módulos que van de los 2 a 8 canales.

- Módulos de salidas analógicas

Este módulo convierte las señales digitales del S7-300 en señales analógicas para el proceso. Es una herramienta indispensable para convertidores de frecuencias, regulaciones, etc. Además dispone de 2 ó 4 canales y tiene una resolución de 4 bits, con posibilidad de configuración para señales tipo tensión o corriente.

- Módulo de suministro de energía

Este módulo es la fuente de alimentación del autómata que transforma la tensión externa de suministro en la tensión operativa interna. Las tensiones de alimentación posibles para el S7-300 son: 24 VCC, 115 VCA o 230 VCA.

El SIMATIC S7-300 tiene varios mecanismos de comunicación:

Intercambio cíclico del conjunto de datos entre redes de CPU mediante la comunicación global de datos

Comunicación de resultados transmitidos por las redes utilizando bloques de comunicación. Mediante el servicio de comunicación global de datos, las redes de CPU pueden intercambiar datos cíclicamente con cada una de las otras unidades centrales de procesamiento. Esto permite a una CPU acceder a la memoria de datos de otra CPU. La comunicación global de datos solo puede ser enviada vía interfaces multipunto (MPI).

En particular el S7-300 de Siemens viene dotado con 3 interfaces para trabajar en equipo red, ellos son:

El M.P.I. (Interface Multi Punto) o El P.P.I. (Interface Punto por Punto)
o El Profibus-DP. Existen además a nivel industrial otras redes tales como la Profibus-FMS, Industrial Ethernet, etc., que también puede ser conectado a cualquiera de ellas.

3.9. Software Step7 Lite.

Para el desarrollo del programa de aplicación en escalera en este PLC se utilizará el software STEP 7 Lite de Siemens. Este software es para un entorno de desarrollo integrado exclusivo para la automatización industrial, el cual es de manejo amigable. Aquí se desarrollará dicho programa y se guardará en la CPU o en una memory card (tarjeta de memoria 64 kb) del propio PLC. Conteniendo las variables declaradas, se utilizarán más adelante para integrarlo al OPC y así interactuar con LabVIEW.

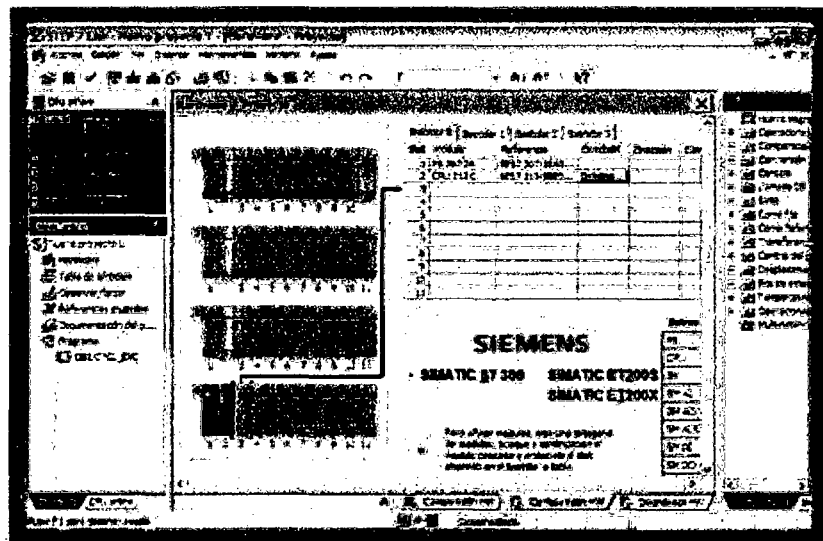


Figura 3.15. Software Step7 Lite.

3.9.1. Conceptos básicos de LabVIEW

El software LabVIEW es un revolucionario entorno de desarrollo gráfico con funciones integradas para realizar adquisición de datos, control de instrumentos, análisis de medida y presentaciones de datos. Este software da la flexibilidad de un potente ambiente de programación, pero mucho más sencillo que los entornos tradicionales. A diferencia de los lenguajes de propósito general, LabVIEW tiene funciones específicas para acelerar el desarrollo de aplicaciones de medida, control y automatización. Con LabVIEW se puede colocar objetos ya construidos para crear interfaces de usuario rápidamente. Además se puede conectar de manera transparente con todo tipo de hardware incluyendo instrumentos de escritorio, tarjetas insertables, controladores de movimiento y controladores lógicos programables (PLCs).

Para esta aplicación se utilizará LabVIEW versión 11.

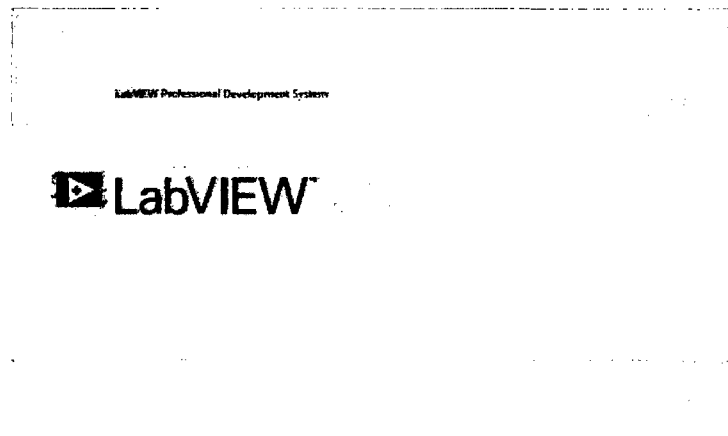


Figura 3.16. Software LabVIEW 11

Los programas creados con LabVIEW son usualmente denominados VI (Virtual Instruments) por la sencilla razón de que estos parecen y actúan como una copia de los instrumentos físicos, como por ejemplo, osciloscopios e instrumentos de medición.

El Panel frontal y el Diagrama de bloques son los componentes más importantes dentro de un VI.

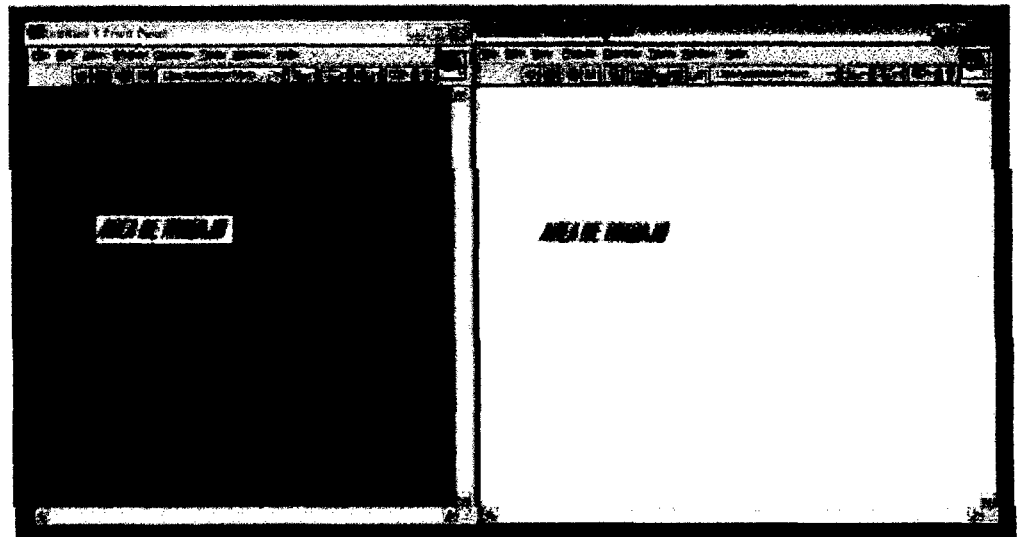


Figura 3.17. Área de trabajo en LabVIEW.

a) Panel Frontal (Front panel): Se utiliza como interfase entre usuario/VI y que es donde los datos son manipulados, controlados y monitoreados. Se construye a partir de controles (entradas) e indicadores (salidas).

Los controles simulan instrumentos de entrada y entregan los respectivos datos al diagrama de bloques del VI. Entre los controles tenemos perillas, botones pulsadores (pushbuttons) y otros dispositivos de entrada.

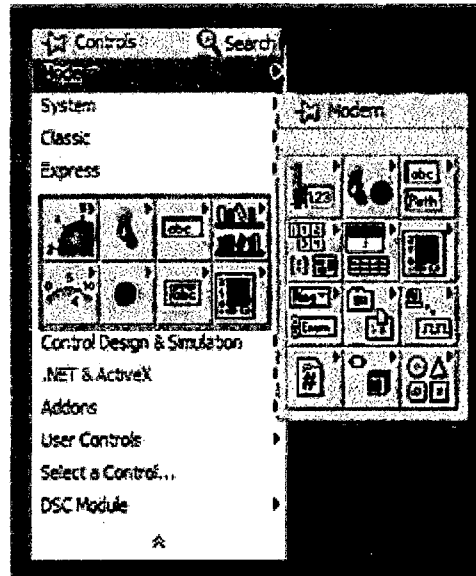


Figura 3.18. Componentes del Panel Frontal.

b) Diagrama de bloque (Block diagram): contiene el código gráfico G que define la funcionalidad del VI. Por ende, podemos ver la estructura del programa de una forma gráfica donde los datos fluyen a través de cables o líneas. Además contiene las librerías de LabVIEW como son las funciones y estructuras para conseguir nuestro programa. En resumen, una vez construido el panel frontal, se crea automáticamente el código gráfico en el diagrama de bloques, representando las funciones de los controles que fueron puestos en el panel frontal y sólo bastaría unir correctamente los terminales de los controles e indicadores para el funcionamiento del VI creado.

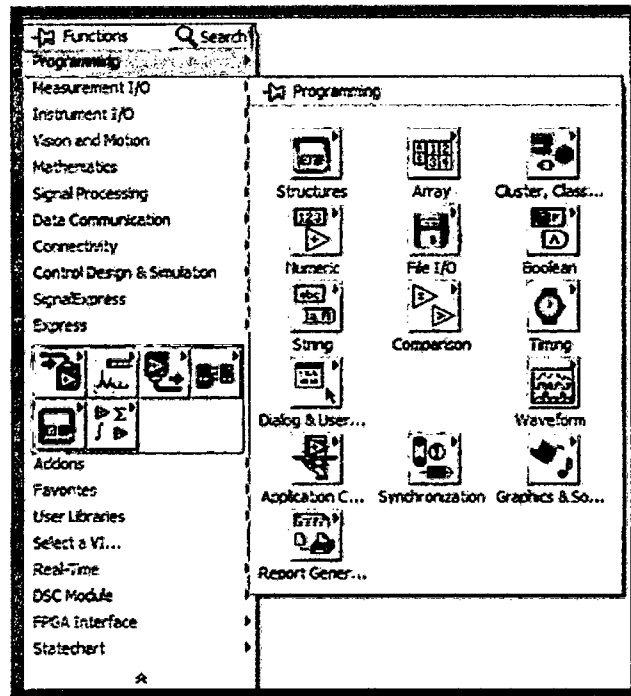


Figura 3.19. Componentes para el Diagrama de Bloques.

Para el desarrollo de nuestro sistema SCADA, se utilizará un módulo de LabVIEW llamado DSC (Datalogging and Supervisory Control; Registro de Datos de Vigilancia y Control), que a partir de la versión LabVIEW 8.5 solo lo contiene, ya que éste módulo ayuda a desarrollar una aplicación de registro de datos y alarmas de muchos canales sin programación, con características adicionales como configuración y administración de alarmas y eventos, visión de tendencias en tiempo real e históricas y configuración de seguridad en sus aplicaciones. Este módulo hace más accesible el protocolo OPC para dicha comunicación con el PLC.

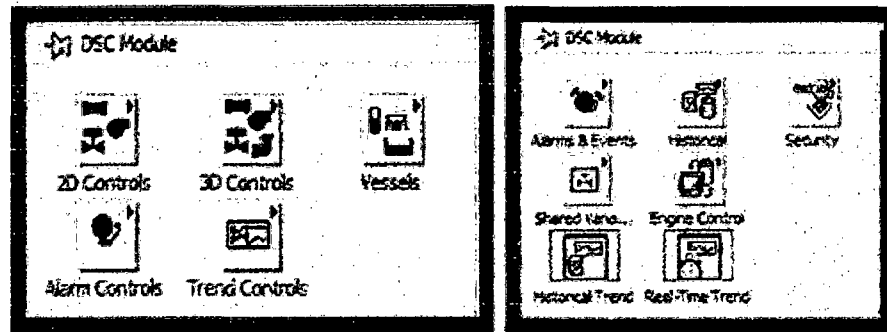


Figura 3.20. Componentes del DSC.

3.10. Instrumentación de planta de nivel de líquido.

Para el proceso experimental se utilizara una planta hidráulica, la cual dicha planta posee válvulas neumáticas de control, posicionadores e instrumentación electrónica compatible con los estándares de la industria.

Para gasto o flujo se utilizan 2 rotámetros y 2 placas de orificio; cada placa incluye un transmisor de presión diferencial, el flujo puede modificarse mediante 2 válvulas, solenoides, para los 2 actuadores que regulan el flujo en la planta se emplean, convertidores corriente-presión que los enlazan con sus respectivos controladores electrónicos.

Para nivel se utiliza un transmisor de presión diferencial en el tanque abierto, que determina el nivel del agua dentro del tanque midiendo la presión que produce el líquido. Para el tanque cerrado hay 2 interruptores, uno de nivel bajo y otro de nivel alto, que se activan cuando el agua alcanza uno de estos niveles.

Hay dos indicadores mano metritos, tipo tubo de Bourdon, que indican la presencia de flujo midiendo presión en las tuberías en la descarga de las bombas. Para el control del proceso se utilizan controladores electrónicos del tipo CAT (tipo ajuste de corriente).

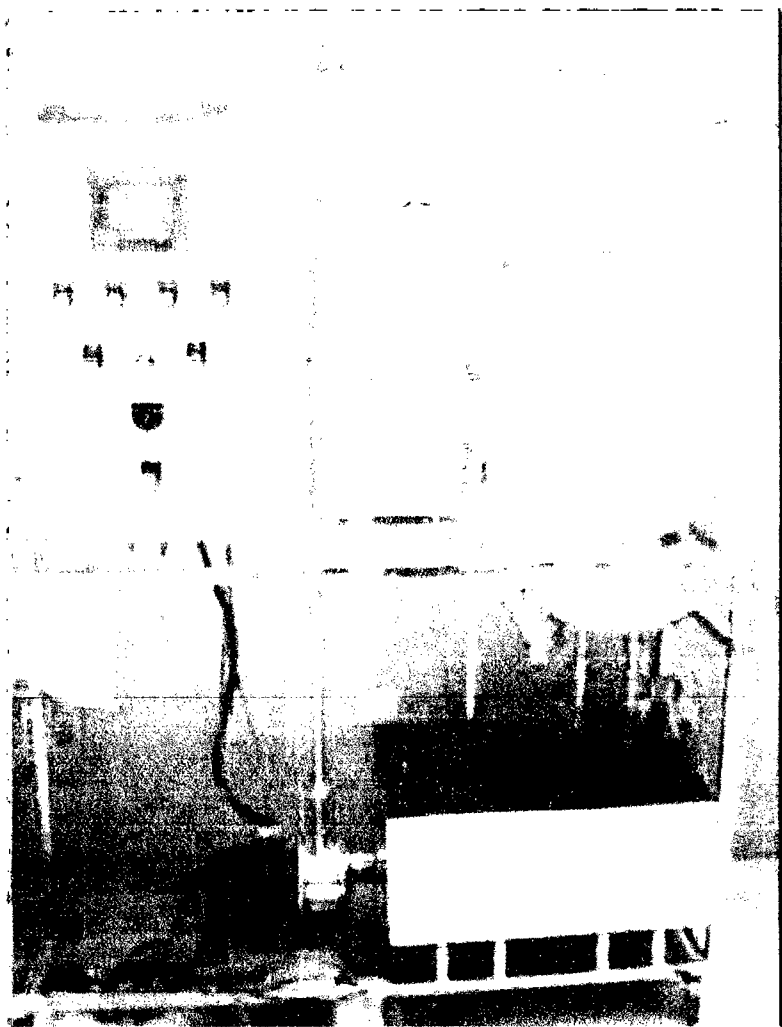


Figura 3.20. Foto de Planta Piloto.

4. Diseño del control y monitoreo.

4.1. Interfaz para comunicación.

Para la interfaz como medio físico entre PLC Siemens S7-300 CPU 313C y software STEP 7 Lite, se puede utilizar convertidor MPI-RS232 así como MPI-USB. Para la comunicación entre PLC Siemens S7-300 CPU 313C y OPC Servidor-Cliente NI (National Instruments) para desarrollo de entorno en LabVIEW, se utiliza un convertidor interfaz MPI-RS232.

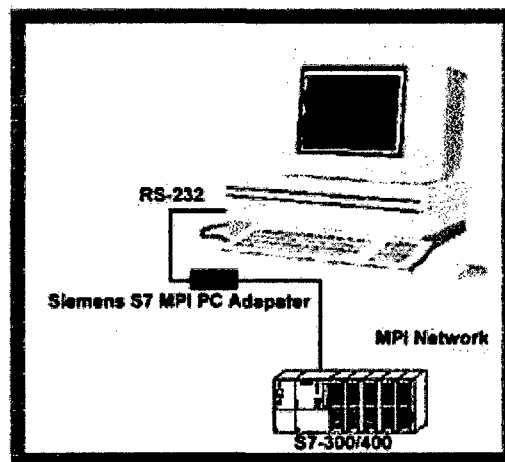


Figura 4.1. Adaptador MPI-RS232.

Para la comunicación entre PLC S7-300 CPU 313C y OPC Servidor IBH (exclusivo para adaptadores Siemens), se pueden utilizar cualquiera de los convertidores, en este caso usaremos un convertidor interfaz MPI-USB. Con la finalidad de hacer comunicación con OPC Cliente de NI.

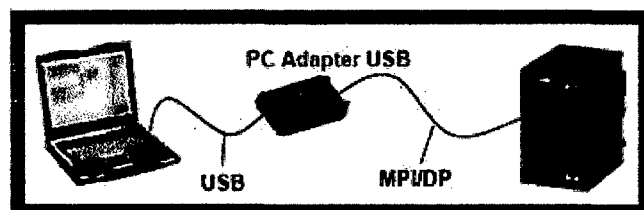


Figura 4.2. Adaptador MPI-USB.

Ambos convertidores utilizarán un driver exclusivo de Siemens. En Control Panel de Windows se encontrará como Set PG/PC Interface, ahí se hace la configuración correspondiente o a veces por defecto, así como también revisar puertos COM para direccionar correctamente la interfaz. Es necesario hacerlo ya que es para obtener un buen funcionamiento en la comunicación.

Como objetivo es leer y escribir entradas, salidas de operandos, la memoria, los datos, es decir, los contadores y las horas, etc.

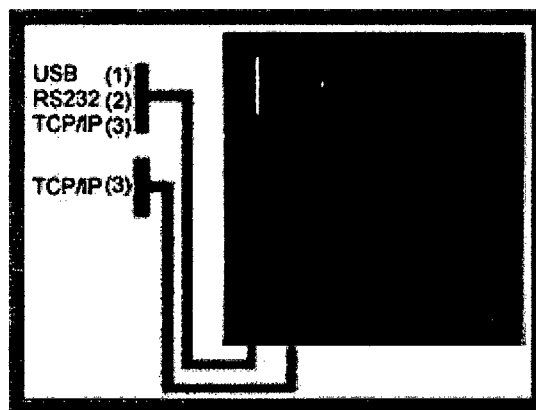


Figura 4.3. PLC Siemens S7-300 CPU 313C

4.2. Desarrollo de diagrama en escalera STEP 7 Lite.

Para el desarrollo del programa en escalera en Step7 Lite, nos desplazamos hacia donde dice Inicio de Windows para encontrar el programa, se abre el software STEP 7 Lite. Damos clic en Archivo/ Nuevo y aparece un recuadro abajo. Después pulsamos en Hardware.

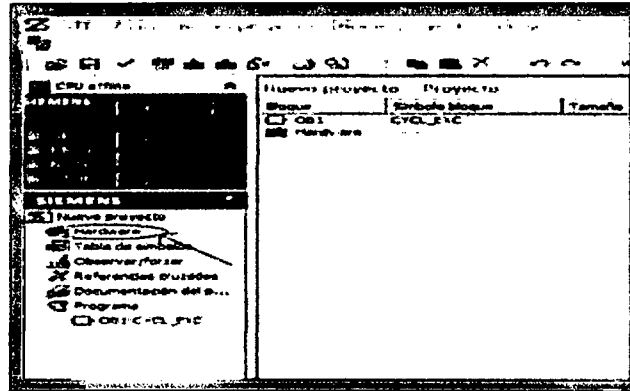


Figura 4.4. Desarrollo de programa en Step7 Lite

Se observa gráficamente al PLC y los módulos que añadiremos. Se escoge dependiendo de los módulos que ofrezca el PLC. En el recuadro derecho aparecen éstos y escogemos la fuente de alimentación (PS 307 2A), después el CPU (313C). En este caso solo escogeremos éstos.

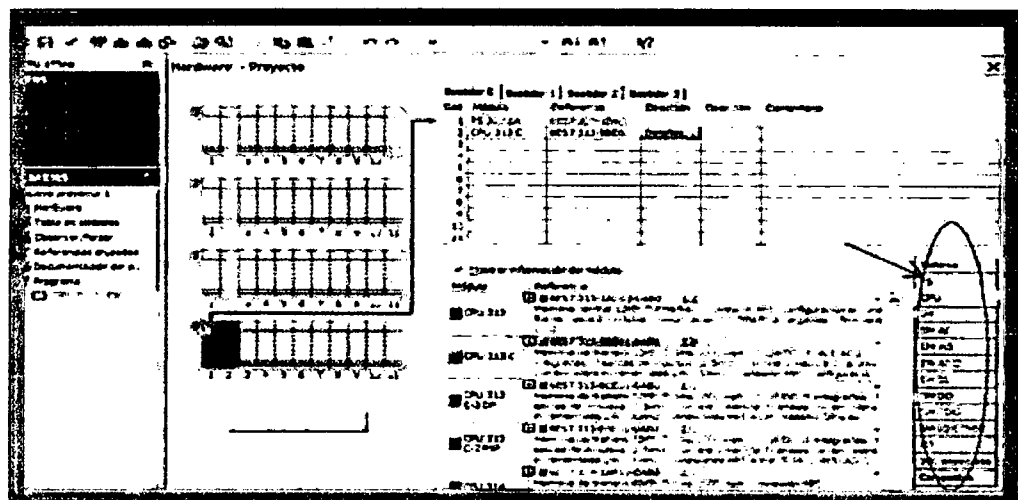


Figura 4.5. Desarrollo de programa en Step7 Lite.

Regresando al cuadro donde en un principio se encuentra hardware, hacia abajo se encuentra una opción "OB1: CYCL_EXC " (1), la cual es para empezar a formar nuestro programa. Pulsamos en Ver y utilizamos la opción KOP, ésta es para definir nuestro diagrama escalera.

Se observa en el centro, nuestra área de trabajo, en el lado derecho aparece un recuadro con opciones para comenzar a hacer el diagrama (2).

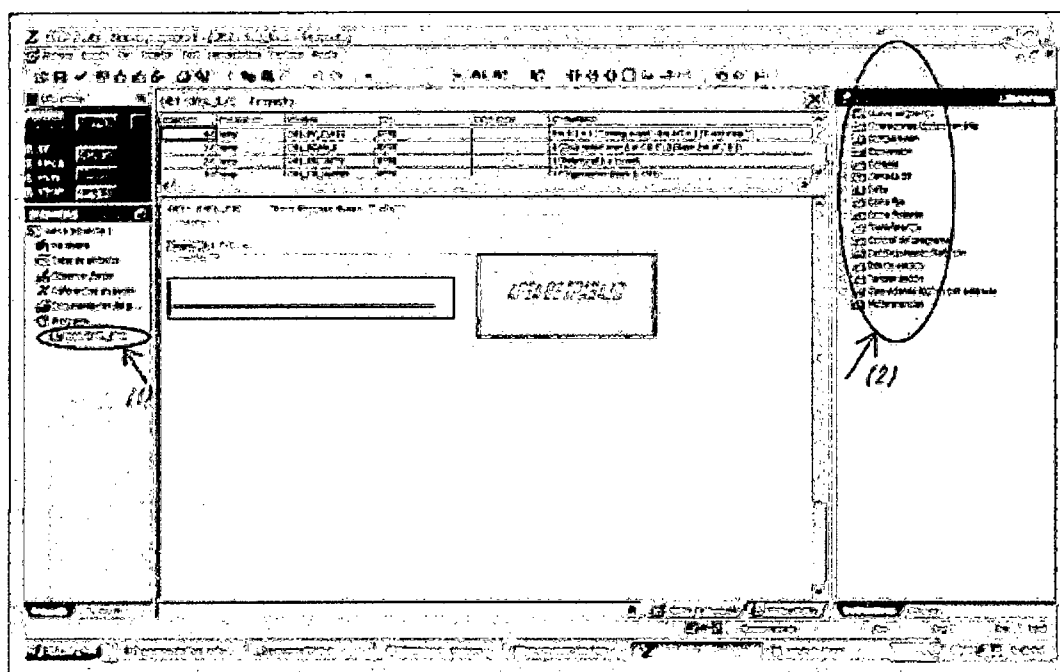


Figura 4.6. Desarrollo de programa en Step7 Lite.

Después de haber finalizado nuestro programa, establecemos coherencia, para saber si hay algún error y corregirlo. Observando que no hay error en programa, haremos conexión online entre software y el PLC.

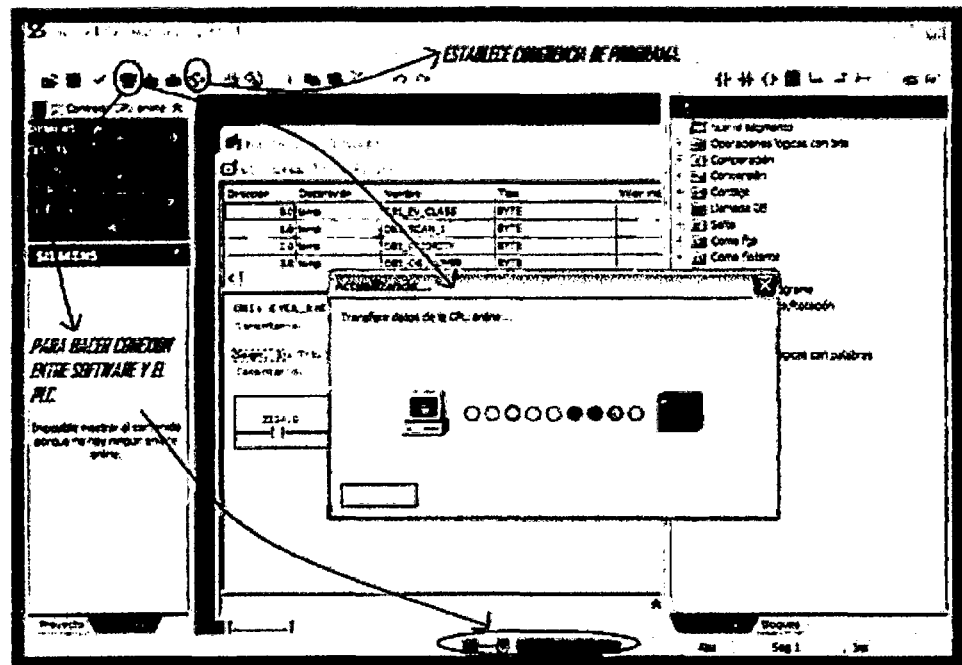


Figura 4.7. Desarrollo de programa en Step7 Lite.

Así pues es como se logra hacer conexión entre hardware y software de Siemens.

4.3. Desarrollo para declarar variables en OPC.

4.3.1. OPC Servidor de National Instruments (NI).

Para utilizar OPC Server de NI, vamos a Start/ All Programs/National Instruments/ NI OPC Server, nos aparece el recuadro y señalamos los iconos donde se insertan el nuevo dispositivo y el nuevo canal, para declarar mis tags (etiquetas). Los "Tags" son símbolos que representan cada una de las entradas y salidas que sean configuradas por el usuario, estas pueden ser analógicas o digitales.



Siemens S7 MPI. Las demás opciones pulsamos en siguiente que es por defecto hasta finalizar, -se puede modificar la velocidad (baud rate), el direccionamiento del puerto, etc.-.



[illegible]

65

4.3.2. OPC Servidor IBH Softec.

El OPC Servidor IBH se utiliza, ya que este contiene drivers que son exclusivos para el manejo de adaptadores y convertidores de Siemens, el OPC de NI también los contiene pero no es su mayoría. Parecido al OPC Servidor de NI se escogen los canales y dispositivos a utilizar, se declaran variables para crear mis nuevas tags y directamente se puede hacer un chequeo si hay congruencia desde mi PLC escogido y mis tags declaradas.

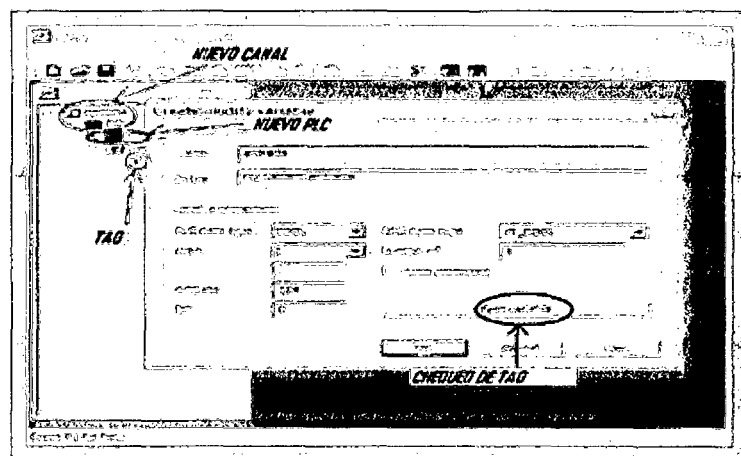


Figura 4.12. Utilizando OPC Servidor de IBH.

Para hacer la interacción entre OPC Servidor IBH y OPC Cliente de NI, primeramente e igual como se hizo con la configuración en OPC Servidor de NI, nos vamos a Inicio/National Instruments/NI OPC Server/OPC Quick Client.

Aparecerá un recuadro y pulsamos el icono de Nuevo Servidor, en este caso OPC IBH. Después OK.

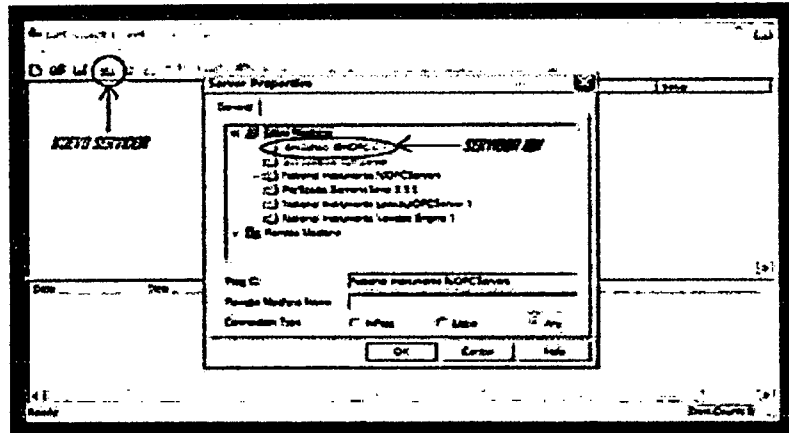


Figura 4.13. Utilizando OPC Servidor de IBH.

Teniendo el Servidor de IBH, creamos un nuevo grupo y le damos un nombre, después pulsamos en el icono de nuevo ítem, así aparecerá otro recuadro donde se dará nombre, el tipo de dato de las tags creadas desde OPC Servidor IBH o alguna personalización por agregar. Finalizamos pulsando OK.

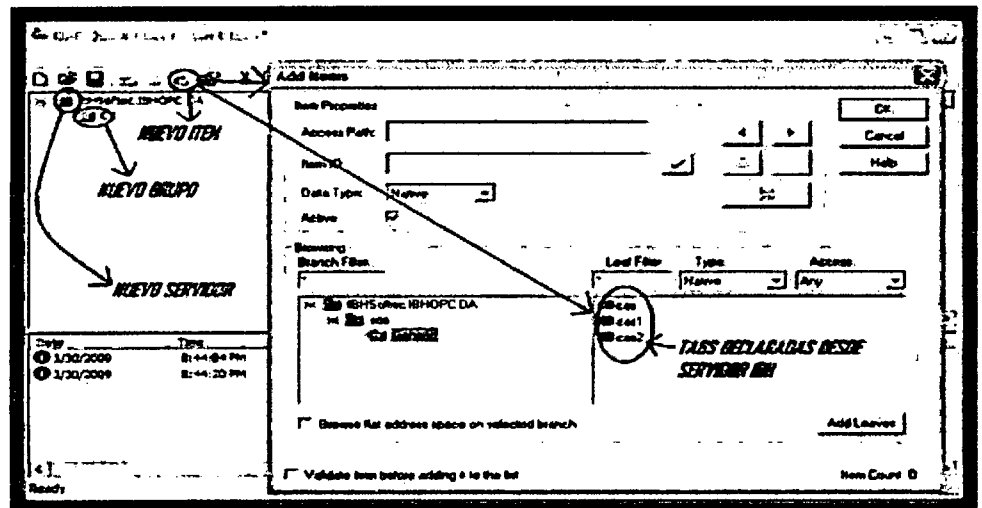


Figura 4.14. Utilizando OPC Servidor de IBH.

4.4. Configuración para interactuar con LabVIEW.

Para interactuar con LabVIEW primero vamos a ->All Programs/National Instruments/LabView 8.5. Aparece un recuadro, damos clic en Empty Project, donde dice My Computer pulsamos con el botón derecho del mouse y escogemos la opción New, elegimos I/O Server y aparecerá de nuevo otro recuadro y elegimos la opción OPC Client.

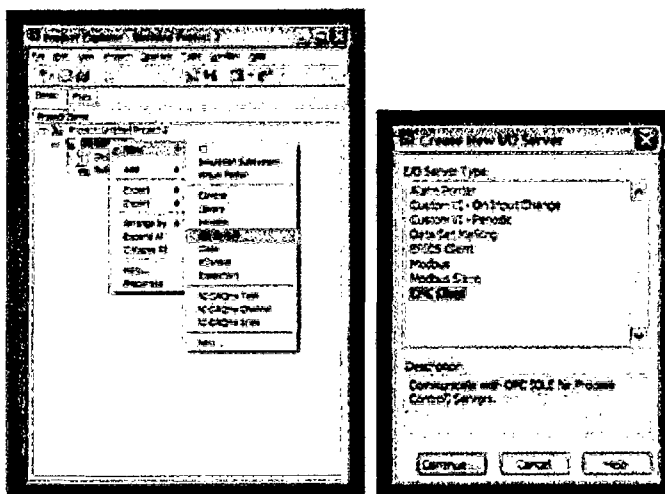


Figura 4.15. Interacción con LabVIEW.

Veremos otro recuadro donde se encontrarán registrados los OPC Server, elegimos con el que hayamos trabajado y damos OK.

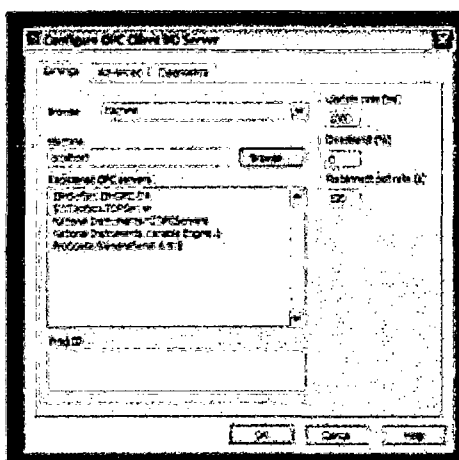


Figura 4.16. Interacción con LabVIEW.

En Project Explorer, hemos creado una nueva librería donde confirmamos nuestras tags creadas. En Untitled Library aparece OPC, damos clic con el botón derecho del mouse a la librería nueva y escogemos New/Variable.

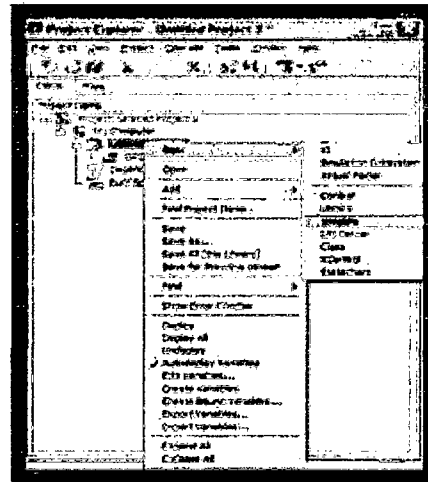


Figura 4.17. Interacción con LabVIEW.

Veremos otro recuadro, ahí daremos nombre a la variable, y para confirmar el tipo de dato escogemos la opción bind to source y damos clic en Browse.

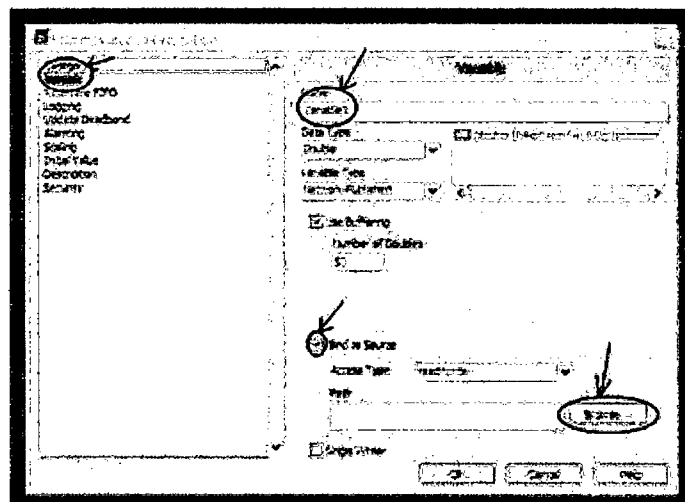


Figura 4.18. Interacción con LabVIEW.



Ahora en Project Explorer, en Nueva Librería aparece mi tag creada. Damos nuevamente clic con el botón derecho del mouse sobre My Computer ->New/VI, para crear nuestra área de trabajo VI, por consiguiente guardamos nuestra nueva librería.



Ahora, solo basta con arrastrar las variables creadas al Panel Frontal de mi VI.

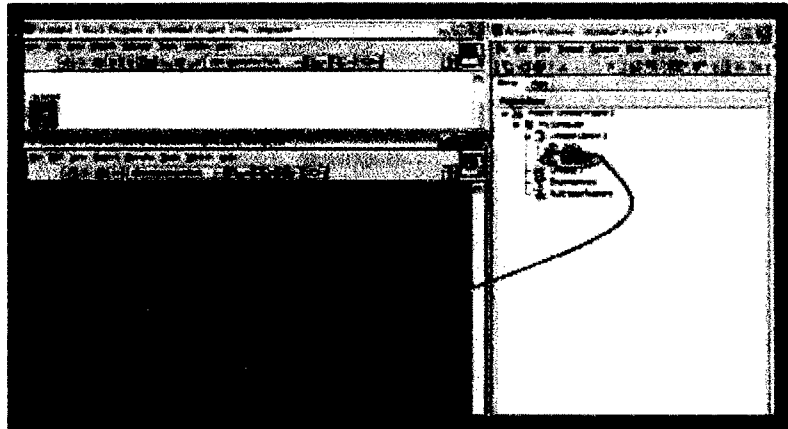


Figura 4.21. Interacción con LabVIEW.

Al correr nuestro programa, forzando una entrada del PLC observaremos en el Panel Frontal gráficamente, la respuesta del PLC. Así pues, nos daremos cuenta la interacción entre software y hardware de diferentes fabricantes.

4.5. Conexión PLC S7-300 CPU 313C con componentes de la planta hidráulica.

Para utilizar los componentes de la planta hidráulica, en el caso de las válvulas solenoidales y los convertidores electro-neumáticos se tendrá que disponer de un compresor, ya que necesitarán flujo de aire regulado automático para su funcionamiento. Se deberá de poner en funcionamiento la cabina de conexiones, esto es alimentarla con el voltaje convencional de 127 V ac, ya que en la cabina tendrá reguladores (24 V dc), protecciones como relevadores para el buen funcionamiento de los componentes de la planta. Para el transmisor, éste necesitará conectarse en serie con una resistencia de 250 ohms. En el caso del PLC éste se deberá de alimentar con un voltaje de 24 V dc, tanto para el CPU como a sus entradas y salidas.

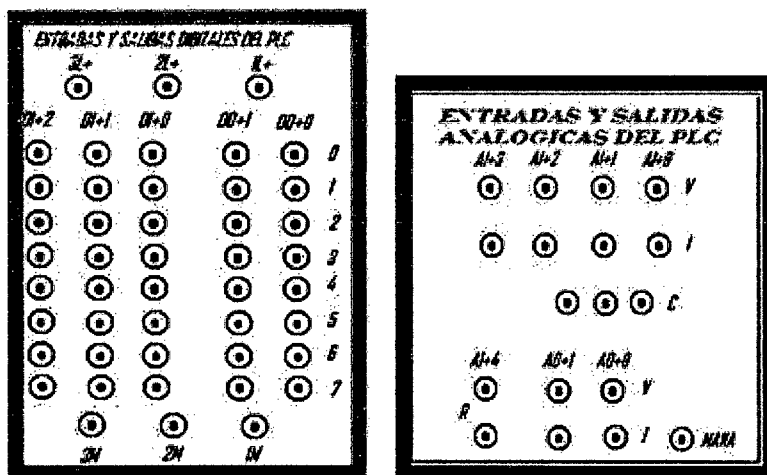


Figura 4.22. Tablero de conexión del PLC

Haciendo una tabla de conexiones entre los dispositivos de la planta y las entradas/salidas del PLC, se hará la relación siguiente.

DIRECCION	NOMBRE
Digitales/Entradas	
I124.0	Electronivel Bajo (LL)
I124.1	Electronivel Alto (HL)
I124.2	Pulsador de entrada y alto Total (PE)
I124.3	Transferencia y Recirculación (TVR)
Digitales/Salidas	
Q124.0	Bomba1 (B1)
Q124.1	Bomba2 (B2)
Q124.2	Válvula solenoide1 (SV1)
Q124.3	Válvula solenoide2 (SV2)
Analógicas/Entradas	
PIW752	Transmisor (LT1)
Analógicas/Salidas	
PQW752	Convertidor electroneumaticos1 (FY-01)
PQW753	Convertidor electroneumaticos2 (FY-02)

Tabla 2. Diagrama de control para planta piloto y PLC

Nota: En el caso del PLC S7-300 CPU 313C, dispone de 24 entradas y 16 salidas digitales, 5 entradas y 2 salidas analógicas, a partir del byte 124 respectivamente. En el idioma ingles I se refiere a entrada digital y Q a salida digital. En las analógicas PIW significa palabra de entrada periférica, y PQW palabra de salida periférica a partir del byte 752 respectivamente.

MANA; Tierra analógica.

Para el cableado de los elementos de la planta, con las entradas y salidas digitales del PLC se muestra a continuación la siguiente figura.

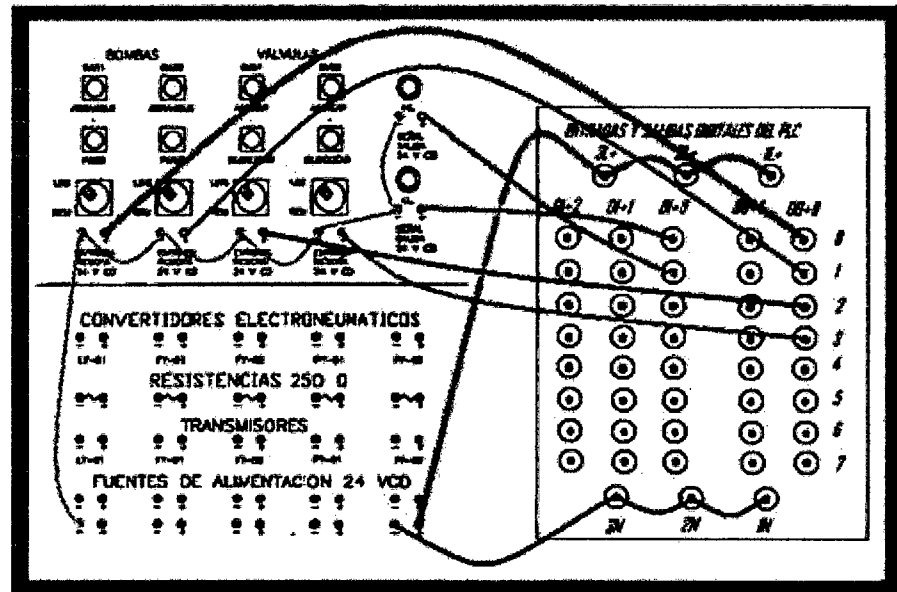


Figura 4.23. Cableado entre PLC y elementos de planta piloto.

Para el cableado de los elementos de la planta, con las entradas y salidas analógicas del PLC se muestra a continuación la siguiente figura.

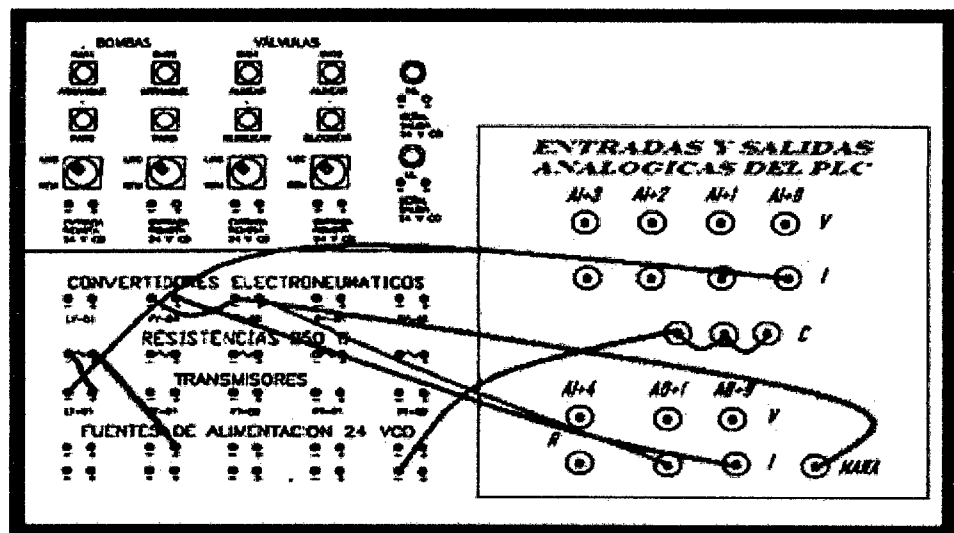


Figura 4.24. Cableado entre PLC y elementos de planta piloto.

4.6. Programación y Desarrollo.

En el siguiente recuadro nos basaremos para realizar nuestro proceso de la planta piloto.

LÍNEAS	VALVULA SW01	VALVULA RC01	VALVULA SW02	VALVULA RC02
TRANSFERIR (Tanque: 1 a Tanque: 1, Tanque: 1 a Tanque: 2) y RECIRCULAR (Tanque 2 a Tanque 1, mientras nivel HL está prendido)	ABIERTA/CIERTE	ABRIENDOSE! (si HL está apagado) CERRANDOSE (si HL está prendido)	ABIERTA/CIERTE	ABRIENDOSE! (si HL está prendido) CERRANDOSE (si HL está apagado)
RECIRCULAR (Tanque 2 a Tanque: 1)	NO IMPORTA	NO IMPORTA	NO IMPORTA	NO IMPORTA

Tabla 3. Proceso para Planta Piloto.

Al realizar nuestro programa en STEP7 Lite hay que resaltar, que en el caso de las entradas y salidas analógicas, para los elementos de control (transmisor y convertidores electroneumáticos) se manejarán con una corriente dentro de un rango de 4 a 20 mA. Estas variables se utilizarán con unas funciones de bloque, la cual permitirán entradas y salidas de señales analógicas de los dispositivos. Esto es, el PLC hará conversión análoga-digital y recíprocamente que en su CPU realizará.

Para entradas analógicas se utiliza el bloque de Escalar (Scale);

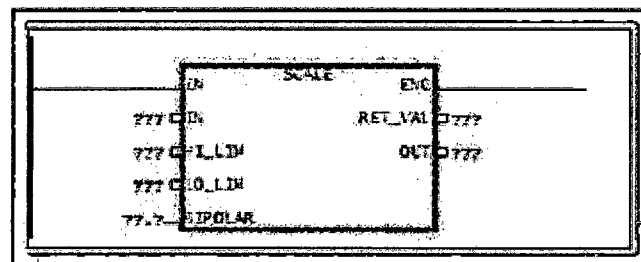


Figura 4.25. Función Scale.

Parámetros de la función SCALE (FC105):

Parámetros de entrada:

- ✚ IN (INT): Valor de entrada a escalar en valor real
- ✚ HI_LIM (REAL): Límite superior del rango de escala
- ✚ LO_LIM (REAL): Límite inferior del rango de escala
- ✚ BIPOLAR (BOOL): 1 para entrada bipolar, 0 para entrada unipolar

Parámetros de salida:

- ✚ OUT (REAL): Resultado de la conversión a escala
- ✚ RET_VAL (WORD): Código de retorno. Si devuelve el código W#16#0000 es que no se han producido errores.

Para las salidas analógicas se utiliza el bloque de Desescalar (Unscale);

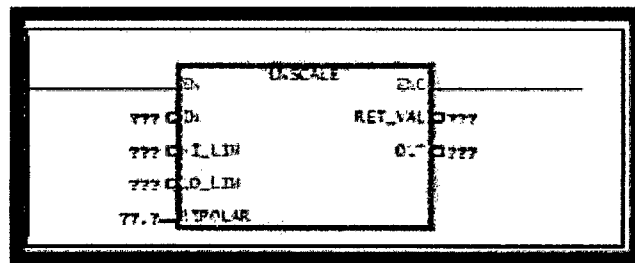


Figura 4.26. Función Unscale.

Parámetros de la función UNSCALE (FC106): Parámetros de entrada:

- ✚ IN (REAL): Valor de entrada a desescalar, convirtiéndolo en un valor entero
- ✚ HI_LIM (REAL): Límite superior del rango de escala
- ✚ LO_LIM (REAL): Límite inferior del rango de escala
- ✚ BIPOLAR (BOOL): 1 para entrada bipolar, 0 para entrada unipolar

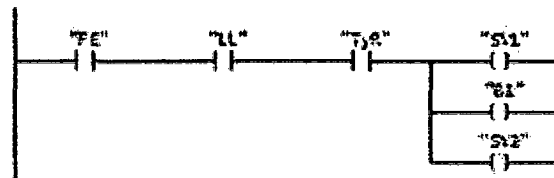
Parámetros de salida:

- ✚ OUT (INT): Resultado del desescalado
- ✚ RET_VAL (WORD): Código de retorno. Si devuelve el código W#16#0000 es que no se han producido errores.

Una vez teniendo lo anterior proseguimos en la realización del diagrama en escalera que a su vez se guardará en la memoria del PLC o en una memory card propia del mismo.

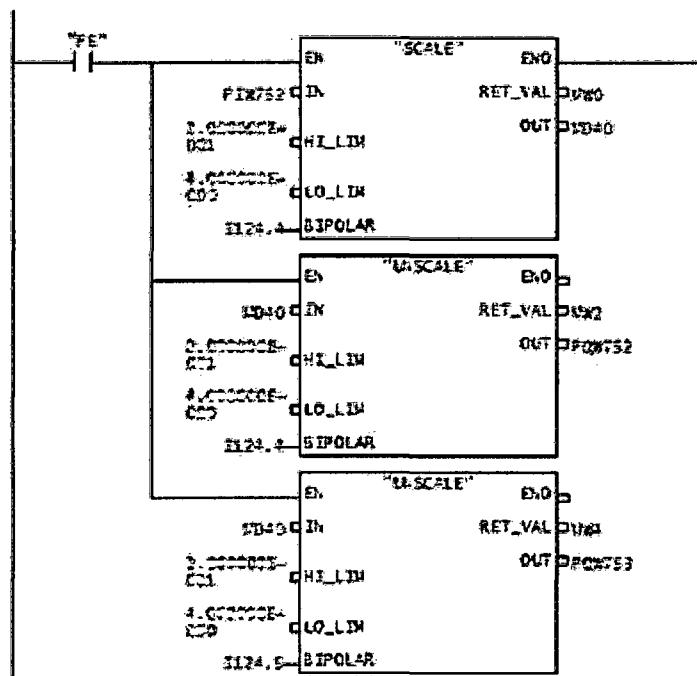
Segm. 1: Transferir y Rectricular

Comentarios:



Segm. 2: Chequeo analogico

Comentarios:



Segm. 3: RECTRICULAR

Comentarios:



Figura 4.27. Diagrama en escalera del diseño.

Teniendo así el diagrama, declaramos las variables en el OPC Servidor-Cliente.

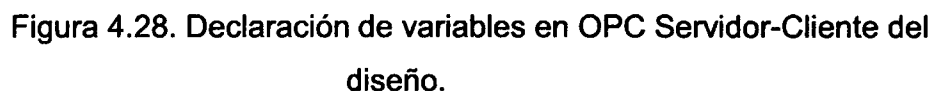


Figura. 4.29. Diagrama de Bloques en LabVIEW del sistema SCADA.

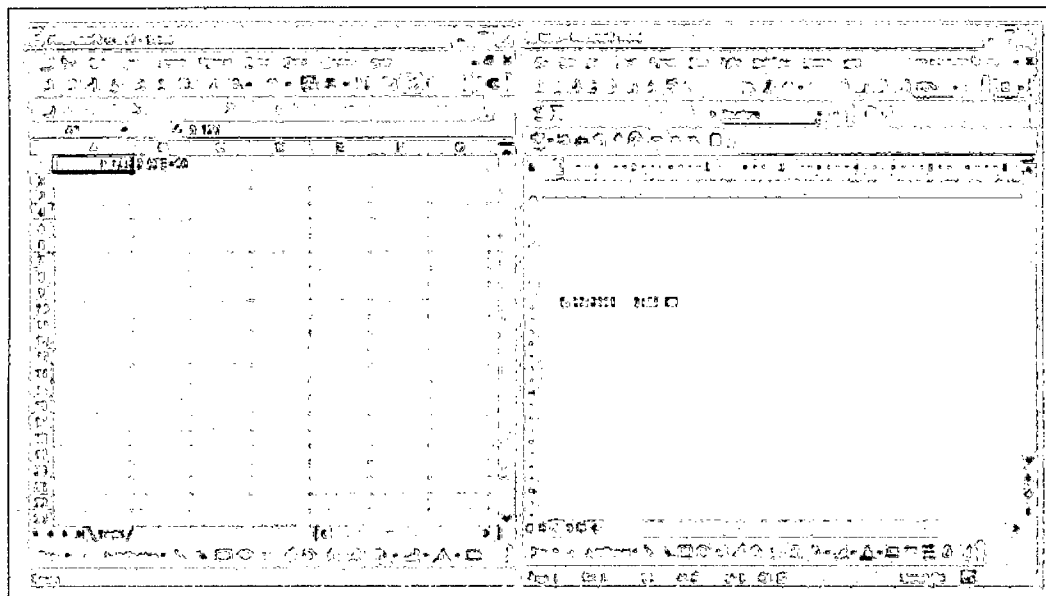


Figura 4.30. Adquisición de datos en Excel y Word.

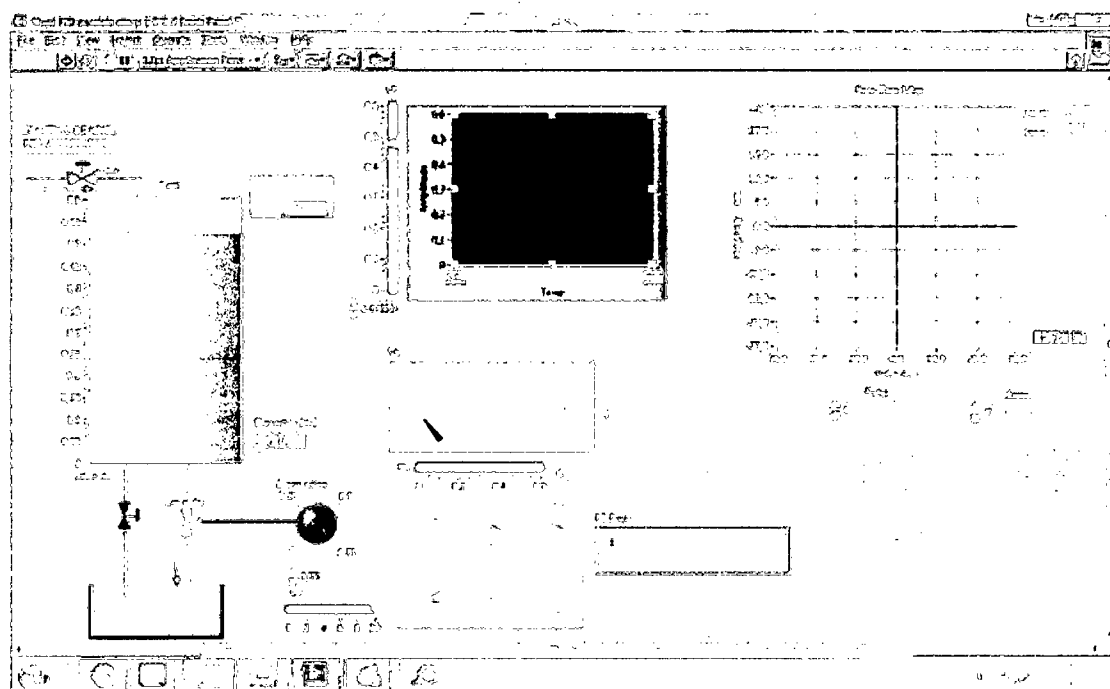


Figura 4.31. Control y Monitoreo SCADA de la Planta Piloto.



5. Amenazas Lógicas

Los protocolos de comunicación utilizados carecen (en su mayoría) de seguridad o esta ha sido implementada en forma de "parche" tiempo después de su creación.

- Existen agujeros de seguridad en los sistemas operativos.
- Existen agujeros de seguridad en las aplicaciones.
- Existen errores en las configuraciones de los sistemas.
- Los usuarios carecen de información respecto al tema.

Esta lista podría seguir extendiéndose a medida que se evalúen mayor cantidad de elementos de un Sistema Informático.

Las empresas u organizaciones no se pueden permitir el lujo de denunciar ataques a sus sistemas, pues el nivel de confianza de los clientes (ciudadanos) bajaría enormemente.

Los Administradores tienen cada vez mayor conciencia respecto de la seguridad de sus sistemas y arreglan por sí mismos las deficiencias detectadas. A esto hay que añadir las nuevas herramientas de seguridad disponibles en el mercado.

Los "advisories" (documentos explicativos) sobre los nuevos agujeros de seguridad detectados y la forma de solucionarlos, lanzados por el CERT, han dado sus frutos.

5.1. Acceso - Uso – Autorización

La identificación de estas palabras es muy importante ya que el uso de algunas implica un uso desapropiado de las otras.

Específicamente "Acceso" y "Hacer Uso" no son el mismo concepto cuando se estudian desde el punto de vista de un usuario y de un intruso. Por ejemplo:

- Cuando un **usuario** tiene **acceso autorizado**, implica que tiene **autorizado el uso** de un recurso.



- Cuando un **atacante** tiene **acceso desautorizado** está haciendo **uso desautorizado** del sistema.
- Pero, cuando un **atacante** hace **uso desautorizado** de un sistema, esto implica que el **acceso fue autorizado** (simulación de usuario).

Luego un **Ataque** será un intento de acceso, o uso desautorizado de un recurso, sea satisfactorio o no. Un **Incidentes** envuelve un conjunto de ataques que pueden ser distinguidos de otro grupo por las características del mismo (grado, similitud, técnicas utilizadas, tiempos, etc.).

John D. Howard (1) en su tesis estudia la cantidad de ataques que puede tener un incidente. Al concluir dicho estudio y basado en su experiencia en los laboratorios del CERT afirma que esta cantidad varía entre 10 y 1.000 y estima que un número razonable para estudios es de 100 ataques por incidentes.

5.2. Detección de Intrusos

A finales de 1996, Dan Farmer (creador de una de las herramientas más útiles en la detección de intrusos: SATAN) realizó un estudio sobre seguridad analizando 2.203 sistemas de sitios en Internet. Los sistemas objeto del estudio fueron Web Sites orientados al comercio y con contenidos específicos, además de un conjunto de sistemas informáticos aleatorios con los que realizar comparaciones.

El estudio se realizó empleando técnicas sencillas y no intrusivas. Se dividieron los problemas potenciales de seguridad en dos grupos: rojos (red) y amarillos (yellow).

Los problemas del grupo rojo son los más serios y suponen que el sistema está abierto a un atacante potencial, es decir, posee problemas de seguridad conocidos en disposición de ser explotados. Así por ejemplo, un problema de seguridad del grupo rojo es un equipo que tiene el servicio de FTP anónimo mal configurado. Los problemas



de seguridad del grupo amarillo son menos serios pero también reseñables. Implican que el problema detectado no compromete inmediatamente al sistema pero puede causarle serios daños o bien, que es necesario realizar tests más intrusivos para determinar si existe o no un problema del grupo rojo.

La tabla resume los sistemas evaluados, el número de equipos en cada categoría y los porcentajes de vulnerabilidad para cada uno. Aunque los resultados son límites superiores, no dejan de ser... escandalosos.

Tipo de sitio	# Total sitios testeados	% Total Vulnerables	% Yellow	% Red
Bancos	660	68,34	32,73	35,61
Créditos	274	51,1	30,66	20,44
Sitios Federales US	47	61,7	23,4	38,3
News	312	69,55	30,77	38,78
Sexo	451	66,08	40,58	25,5
Totales	1.734	64,93	33,85	31,08
Grupo aleatorio	469	33,05	15,78	17,27

Figura. 5.1

Como puede observarse, cerca de los dos tercios de los sistemas analizados tenían serios problemas de seguridad y Farmer destaca que casi un tercio de ellos podían ser atacados con un mínimo esfuerzo.

5.3. Identificación de las Amenazas

La identificación de amenazas requiere conocer los tipos de ataques, el tipo de acceso, la forma operacional y los objetivos del atacante.

Las consecuencias de los ataques se podrían clasificar en:

- **Data Corruption:** la información que no contenía defectos pasa a tenerlos.
- **Denial of Service (DoS):** servicios que deberían estar disponibles no lo están.

- **Leakage:** los datos llegan a destinos a los que no deberían llegar.

Desde 1990 hasta nuestros días, el CERT viene desarrollando una serie de estadísticas que demuestran que cada día se registran más ataques informáticos, y estos son cada vez más sofisticados, automáticos y difíciles de rastrear.

La Tabla 7.2 detalla el tipo de atacante, las herramientas utilizadas, en qué fase se realiza el ataque, los tipos de procesos atacados, los resultados esperados y/u obtenidos y los objetivos perseguidos por los intrusos.

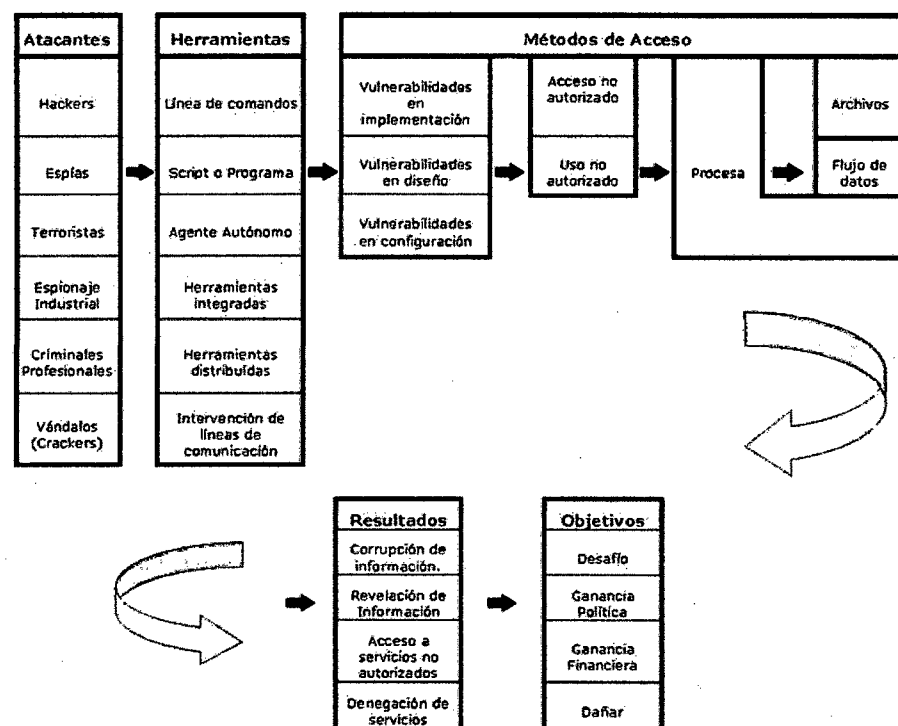


Figura 5.2

Cualquier adolescente de 15 años (Script Kiddies), sin tener grandes conocimientos, pero con una potente y estable herramienta de ataque desarrollada por los Gurús, es capaz de dejar fuera de servicio cualquier servidor de información de cualquier organismo en Internet,



simplemente siguiendo las instrucciones que acompañan la herramienta.

Los números que siguen no pretenden alarmar a nadie ni sembrar la semilla del futuro Hacker. Evidentemente la información puede ser aprovechada para fines menos lícitos que para los cuales fue pensada, pero esto es algo ciertamente difícil de evitar.

Año	Incidentes Reportados	Vulnerabilidades Reportadas	Mensajes Recibidos
1988	6		539
1989	132		2.868
1990	252		4.448
1991	406		9.629
1992	773		14.463
1993	1.334		21.267
1994	2.340		29.580
1995	2.412	171	32.084
1996	2.573	345	31.268
1997	2.134	311	39.626
1998	3.734	262	41.871
1999	9.859	417	34.612
2000	21.756	1.090	56.365
2001 (4 meses)	15.476	1.151	39.181
Total	63.187	3.747	357.802

Figura 5.3

Nota I: Estos incidentes sólo representan el 30% correspondiente a los Hackers.

Nota II: En 1992 el DISA (2) realizó un estudio durante el cual se llevaron a cabo 38.000 ataques a distintas sitios de organizaciones gubernamentales (muchas de ellas militares). El resultado de los ataques desde 1992 a 1995 se resume en el siguiente cuadro (3):

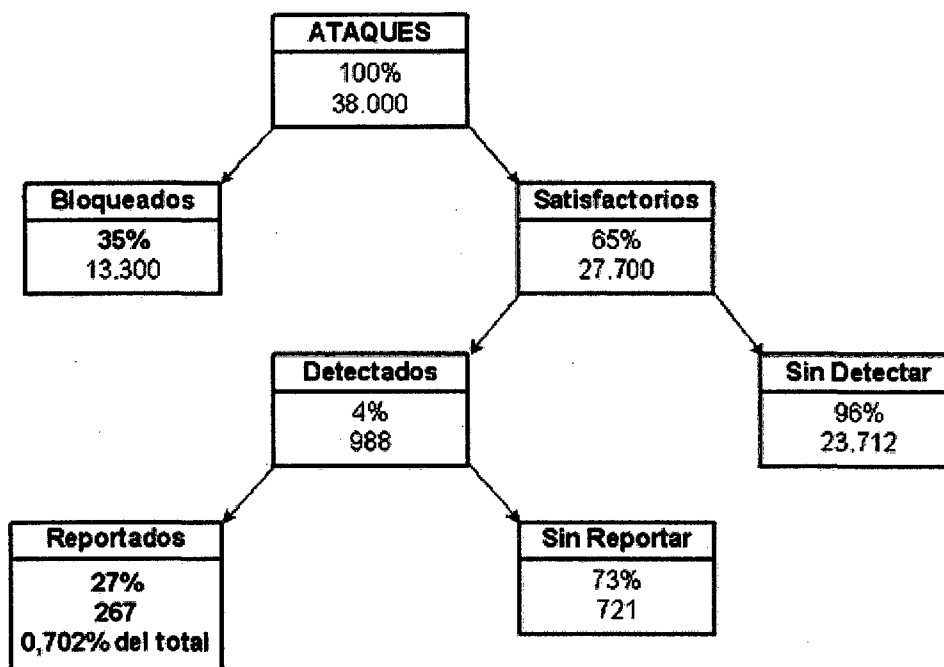


Figura 5.4

Puede observarse que solo el 0,70% (267) de los incidentes fueron reportados. Luego, si en el año 2000 se denunciaron 21.756 casos eso arroja 3.064.225 incidentes en ese año.

Nota III: Puede observarse que los incidente reportados en 1997 con respecto al año anterior es menor. Esto puede deberse a diversas causas:

Las empresas u organizaciones no se pueden permitir el lujo de denunciar ataques a sus sistemas, pues el nivel de confianza de los clientes (ciudadanos) bajaría enormemente.

Los administradores tienen cada vez mayor conciencia respecto de la seguridad de sus sistemas y arreglan por sí mismos las deficiencias detectadas. A esto hay que añadir las nuevas herramientas de seguridad disponibles en el mercado.

Los "Advisories" (documentos explicativos) sobre los nuevos agujeros de seguridad detectados y la forma de solucionarlos, lanzados por el CERT, han dado sus frutos.



5.4. Tipos de Ataques

A continuación se expondrán diferentes tipos de ataques perpetrados, principalmente, por Hackers. Estos ataques pueden ser realizados sobre cualquier tipo de red, sistema operativo, usando diferentes protocolos, etc.

En los primeros tiempos, los ataques involucraban poca sofisticación técnica. Los Insiders (operadores, programadores, data entrys) utilizaban sus permisos para alterar archivos o registros. Los Outsiders ingresaban a la red simplemente averiguando una password válida. A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar "agujeros" en el diseño, configuración y operación de los sistemas.

- Ingeniería Social
- Ingeniería Social Inversa
- Trashing (Cartoneo)
- Ataques de Monitorización
- Ataques de Autenticación
- Denial of Service (DoS)
- Ataques de Modificación – Daño

5.5. Errores de Diseño, Implementación y Operación

Muchos sistemas están expuestos a "agujeros" de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje. Estas vulnerabilidades ocurren por variadas razones, y miles de "puertas invisibles" son descubiertas (cada día) en sistemas operativos, aplicaciones de software, protocolos de red, browsers de Internet, correo electrónico y todas clase de servicios informático disponible.



Los Sistemas operativos abiertos (como Unix y Linux) tienen agujeros más conocidos y controlados que aquellos que existen en sistemas operativos cerrados (como Windows®). La importancia (y ventaja) del código abierto radica en miles de usuarios analizan dicho código en busca de posibles bugs y ayudan a obtener soluciones en forma inmediata.

Constantemente encontramos en Internet avisos de nuevos descubrimientos de problemas de seguridad (y herramientas de Hacking que los explotan), por lo que hoy también se hace indispensable contar con productos que conocen esas debilidades, puedan diagnosticarlas y actualizar el programa afectado con el parche adecuado.

5.6. Implementación de las Técnicas

A lo largo de mi investigación he recopilado distinto tipos de programas que son la aplicación de las distintas técnicas enumeradas anteriormente. La mayoría de los mismos son encontrados fácilmente en Internet en versiones ejecutables, y de otros se encuentra el código fuente, generalmente en lenguaje C, Java y Perl.

Cada una de las técnicas explicadas (y más) pueden ser utilizadas por un intruso en un ataque. A continuación se intentarán establecer el orden de utilización de las mismas, pero siempre remarcando que un ataque insume mucha paciencia, imaginación acumulación de conocimientos y experiencia dada (en la mayoría de los casos) por prueba y error.

Identificación del problema (víctima): en esta etapa se recopila toda la información posible de la víctima. Cuanta más información se acumule, más exacto y preciso será el ataque, más fácil será eliminar las evidencias y más difícil será su rastreo.

Exploración del sistema víctima elegido: en esta etapa se recopila información sobre los sistemas activos de la víctima, cuales son los más vulnerables y cuales se encuentran disponibles. Es importante



remarcar que si la víctima parece apropiada en la etapa de Identificación, no significa que esto resulte así en esta segunda etapa. Enumeración: en esta etapa se identificarán las cuentas activas y los recursos compartidos mal protegidos. La diferencia con las etapas anteriores es que aquí se establece una conexión activa a los sistemas y la realización de consultas dirigidas. Estas intrusiones pueden (y deberían) ser registradas, por el administrador del sistema, o al menos detectadas para luego ser bloqueadas.

Intrusión propiamente dicha: en esta etapa el intruso conoce perfectamente el sistema y sus debilidades y comienza a realizar las tareas que lo llevaron a trabajar, en muchas ocasiones, durante meses.

Contrariamente a lo que se piensa, los sistemas son difíciles de penetrar si están bien administrados y configurados. Ocasionalmente los defectos propios de la arquitectura de los sistemas proporciona un fácil acceso, pero esto puede ser, en la mayoría de los casos, subsanado aplicando las soluciones halladas.

5.7. ¿Cómo defenderse de estos Ataques?

La mayoría de los ataques mencionados se basan en fallos de diseño inherentes a Internet (y sus protocolos) y a los sistemas operativos utilizados, por lo que no son "solucionables" en un plazo breve de tiempo.

La solución inmediata en cada caso es mantenerse informado sobre todos los tipos de ataques existentes y las actualizaciones que permanentemente lanzan las empresas desarrolladoras de software, principalmente de sistemas operativos.

Las siguientes son medidas preventivas. Medidas que toda red y administrador deben conocer y desplegar cuanto antes:

1. Mantener las máquinas actualizadas y seguras físicamente
2. Mantener personal especializado en cuestiones de seguridad (o subcontratarlo).



3. Aunque una máquina no contenga información valiosa, hay que tener en cuenta que puede resultar útil para un atacante, a la hora de ser empleada en un DoS coordinado o para ocultar su verdadera dirección.
4. No permitir el tráfico "broadcast" desde fuera de nuestra red. De esta forma evitamos ser empleados como "multiplicadores" durante un ataque Smurf.
5. Filtrar el tráfico IP Spoof.
6. Auditorias de seguridad y sistemas de detección.
7. Mantenerse informado constantemente sobre cada una de las vulnerabilidades encontradas y parches lanzados. Para esto es recomendable estar suscripto a listas que brinden este servicio de información.
8. Por último, pero quizás lo más importante, **la capacitación continúa del usuario.**

5.7.1. Amenazas lógicas – Tipo de ataques

A continuación se expondrán diferentes tipos de ataques perpetrados, principalmente, por Hackers. Estos ataques pueden ser realizados sobre cualquier tipo de red, sistema operativo, usando diferentes protocolos, etc.

En los primeros tiempos, los ataques involucraban poca sofisticación técnica. Los Insiders (operadores, programadores, data entrys) utilizaban sus permisos para alterar archivos o registros. Los Outsiders ingresaban a la red simplemente averiguando una password válida. A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar "agujeros" en el diseño, configuración y operación de los sistemas.

Son muchos los autores que describen con detalle las técnicas y las clasifican de acuerdo a diferentes características de las mismas. Ante la diversificación de clasificaciones de amenazas y la inminente aparición de nuevas técnicas, para la realización del presente los

ataques serán clasificados y categorizados según mi experiencia y conocimiento de cada caso.

Otra lista de términos asociada con los ataques puede ser la siguiente (1):

<i>Trojan horses</i>	<i>Fraud networks</i>	<i>Fictitious people</i>	<i>Infrastructure observation</i>	<i>e-mail overflow</i>
<i>Time bombs</i>	<i>Get a job</i>	<i>Protection limit poke</i>	<i>Infrastructure interference</i>	<i>Human engineering</i>
<i>Bribes</i>	<i>Dumpster diving</i>	<i>Sympathetic vibration</i>	<i>Password guessing</i>	<i>Packet insertion</i>
<i>Data diddling</i>	<i>Computer viruses</i>	<i>Invalid values on calls</i>	<i>Van Eck bugging</i>	<i>Packet watching</i>
<i>Login spoofing</i>	<i>Data diddling</i>	<i>Wiretapping</i>	<i>Combined attacks</i>	<i>e-mail spoofing</i>
<i>Scanning</i>	<i>Dumpster diving</i>	<i>Eavesdropping</i>	<i>Denial-of-service</i>	<i>Harassment</i>
<i>Masquerading</i>	<i>Software piracy</i>	<i>Data copying</i>	<i>Degradation of service</i>	<i>Traffic analysis</i>
<i>Trap doors</i>	<i>Covert channels</i>	<i>Viruses and worms</i>	<i>Session hijacking</i>	<i>Timing attacks</i>
<i>Tunneling</i>	<i>Trojan horses</i>	<i>IP spoofing</i>	<i>Logic bombs</i>	<i>Salamis</i>
<i>Password sniffing</i>	<i>Excess privileges</i>			

Figura 5.5

Al describirlos no se pretende dar una guía exacta ni las especificaciones técnicas necesarias para su uso. Sólo se pretende dar una idea de la cantidad y variabilidad de los mismos, así como que su adaptación (y aparición de nuevos) continúa paralela a la creación de nuevas tecnologías.

Cabe destacar que para la utilización de estas técnicas no será necesario contar con grandes centros de cómputos, lo que queda fehacientemente demostrado al saber que algunos Hackers más famosos de la historia hackeaban con computadoras (incluso armadas con partes encontradas en basureros) desde la habitación de su hogar.

Cada uno de los ataques abajo descritos será dirigido remotamente. Se define **Ataque Remoto** como "un ataque iniciado contra una maquina sobre la cual el atacante no tiene control físico"(2). Esta máquina es distinta a la usada por el atacante y será llamada **Víctima**.

5.7.2. Ingeniería Social

Es la manipulación de las personas para convencerlas de que ejecuten acciones o actos que normalmente no realizan para que



revele todo lo necesario para superar las barreras de seguridad. Si el atacante tiene la experiencia suficiente (generalmente es así), puede engañar fácilmente a un usuario (que desconoce las mínimas medidas de seguridad) en beneficio propio. Esta técnica es una de las más usadas y efectivas a la hora de averiguar nombres de usuarios y passwords.

Por ejemplo, suele llamarse a un usuario haciéndose pasar por administrador del sistema y requerirle la password con alguna excusa convincente. O bien, podría enviarse un mail (falsificando la dirección origen a nombre del administrador) pidiendo al usuario que modifique su password a una palabra que el atacante suministra.

Para evitar situaciones de IS es conveniente tener en cuenta estas recomendaciones:

- Tener servicio técnico propio o de confianza.
- Instruir a los usuarios para que no respondan ninguna pregunta sobre cualquier característica del sistema y deriven la inquietud a los responsables que tenga competencia para dar esa información.

Asegurarse que las personas que llaman por teléfono son quien dice ser. Por ejemplo si la persona que llama se identifica como proveedor de Internet lo mejor es cortar y devolver la llamada a forma de confirmación.

5.7.3. Ingeniería Social Inversa

Consiste en la generación, por parte de los intrusos, de una situación inversa a la originada en Ingeniería Social.

En este caso el intruso publicita de alguna manera que es capaz de brindar ayuda a los usuarios, y estos lo llaman ante algún imprevisto. El intruso aprovechara esta oportunidad para pedir información necesaria para solucionar el problema del usuario y el suyo propio (la forma de acceso al sistema).



La ISI es más difícil de llevar cabo y por lo general se aplica cuando los usuarios están alertados de acerca de las técnicas de IS. Puede usarse en algunas situaciones específicas y después de mucha preparación e investigación por parte del intruso:

- Generación de una falla en el funcionamiento normal del sistema. Generalmente esta falla es fácil de solucionar pero puede ser difícil de encontrar por los usuarios inexpertos (sabotaje). Requiere que el intruso tenga un mínimo contacto con el sistema.
- Comunicación a los usuarios de que la solución es brindada por el intruso (publicidad).
- Provisión de ayuda por parte del intruso encubierto como servicio técnico.

5.7.4. Trashing (Cartoneo)

Generalmente, un usuario anota su login y password en un papelito y luego, cuando lo recuerda, lo arroja a la basura. Este procedimiento por más inocente que parezca es el que puede aprovechar un atacante para hacerse de una llave para entrar el sistema..."nada se destruye, todo se transforma".

El Trashing puede ser físico (como el caso descripto) o lógico, como analizar buffers de impresora y memoria, bloques de discos, etc.

El Trashing físico suele ser común en organizaciones que no disponen de alta confidencialidad, como colegios y universidades.

5.7.5. Ataques de Monitorización

Este tipo de ataque se realiza para observar a la víctima y su sistema, con el objetivo de establecer sus vulnerabilidades y posibles formas de acceso futuro.



5.7.6. Ataques de Autenticación

Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y password.

5.7.7. Denial of Service (DoS)

Los protocolos existentes actualmente fueron diseñados para ser empleados en una comunidad abierta y con una relación de confianza mutua. La realidad indica que es más fácil desorganizar el funcionamiento de un sistema que acceder al mismo; así los ataques de Negación de Servicio tienen como objetivo saturar los recursos de la víctima de forma tal que se inhabilita los servicios brindados por la misma.

5.7.8. Ataques de Modificación - Daño

5.8. Amenazas Lógicas Tipo de Ataques Motorizados

Este tipo de ataque se realiza para observar a la víctima y su sistema, con el objetivo de establecer sus vulnerabilidades y posibles formas de acceso futuro.

- **Shoulder Surfing**

Consiste en espiar físicamente a los usuarios para obtener el login y su password correspondiente. El Surfing explota el error de los usuarios de dejar su login y password anotadas cerca de la computadora (generalmente en post-it adheridos al monitos o teclado). Cualquier intruso puede pasar por ahí, verlos y memorizarlos para su posterior uso. Otra técnica relacionada al



surfing es aquella mediante la cual se ve, por encima del hombro, al usuario cuando teclea su nombre y password.

- **Decoy (Señuelos)**

Los Decoy son programas diseñados con la misma interface que otro original. En ellos se imita la solicitud de un logeo y el usuario desprevenido lo hace. Luego, el programa guardará esta información y dejará paso a las actividades normales del sistema. La información recopilada será utilizada por el atacante para futuras "visitas".

Una técnica semejante es aquella que, mediante un programa se guardan todas las teclas presionadas durante una sesión. Luego solo hará falta estudiar el archivo generado para conocer nombres de usuarios y claves.

- **Scanning (Búsqueda)**

El Scaneo, como método de descubrir canales de comunicación susceptibles de ser explotados, lleva en uso mucho tiempo. La idea es recorrer (scanear) tantos puertos de escucha como sea posible, y guardar información de aquellos que sean receptivos o de utilidad para cada necesidad en particular. Muchas utilidades de auditoría también se basan en este paradigma. El Scaneo de puertos pertenece a la Seguridad Informática desde que era utilizado en los sistemas de telefonía. Dado que actualmente existen millones de números de teléfono a los que se pueden acceder con una simple llamada, la solución lógica (para encontrar números que puedan interesar) es intentar conectarlos a todos.

La idea básica es simple: llamar a un número y si el módem devuelve un mensaje de conectado, grabar el número. En otro caso, la computadora cuelga el teléfono y llama al siguiente número.



Scanear puertos implica las mismas técnicas de fuerza bruta. Se envía una serie de paquetes para varios protocolos y se deduce que servicios están "escuchando" por las respuestas recibidas o no recibidas.

Existen diversos tipos de Scanning según las técnicas, puertos y protocolos explotados:

- **TCP Connect Scanning**

Esta es la forma básica del scaneo de puertos TCP. Si el puerto está escuchando, devolverá una respuesta de éxito; cualquier otro caso significará que el puerto no está abierto o que no se puede establecer conexión con él.

Las ventajas que caracterizan esta técnica es que no necesita de privilegios especiales y su gran velocidad.

Su principal desventaja es que este método es fácilmente detectable por el administrador del sistema. Se verá un gran número de conexiones y mensajes de error para los servicios en los que se ha conseguido conectar la máquina, que lanza el scanner, y también se verá su inmediata desconexión.

- **TCP SYN Scanning**

Cuando dos procesos establecen una comunicación usan el modelo Cliente/Servidor para establecerla. La aplicación del Servidor "escucha" todo lo que ingresa por los puertos. La identificación del Servidor se efectúa a través de la dirección IP del sistema en el que se ejecuta y del número de puerto del que depende para la conexión. El Cliente establece la conexión con el Servidor a través del puerto disponible para luego intercambiar datos.

La información de control de llamada HandShake (saludo) se intercambia entre el Cliente y el Servidor para establecer un

diálogo antes de transmitir datos. Los "paquetes" o segmentos TCP tienen banderas que indican el estado del mismo.

El protocolo TCP de Internet, sobre el que se basa la mayoría de los servicios (incluyendo el correo electrónico, el web y el IRC) implica esta conexión entre dos máquinas. El establecimiento de dicha conexión se realiza mediante lo que se llama Three-Way Handshake ("conexión en tres pasos") ya que intercambian tres segmentos.

En forma esquemática se tiene:

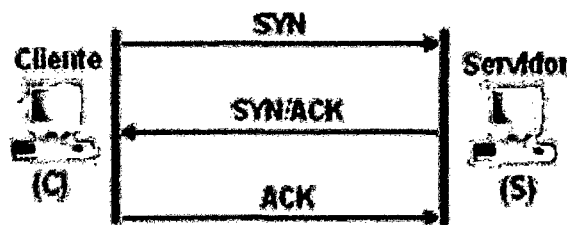


Figura 5.6

1. El programa Cliente (C) pide conexión al Servidor (S) enviándole un segmento SYN. Este segmento le dice a S que C desea establecer una conexión.
2. S (si está abierto y escuchando) al recibir este segmento SYN (activa el indicador) y envía una autenticación ACK de manera de acuse de recibo a C. Si S está cerrado envía un indicador RST.
3. C entonces ACKea (autentifica) a S. Ahora ya puede tener lugar la transferencia de datos.

Cuando las aplicaciones conectadas terminan la transferencia, realizan otra negociación a tres bandas con segmentos FIN en vez

SYN.

La técnica TCP SYN Scanning, implementa un scan de "media-apertura", dado que nunca se abre una sesión TCP completa.



Se envía un paquete SYN (como si se fuera a usar una conexión real) y se espera por la respuesta. Al recibir un SYN/ACK se envía, inmediatamente, un RST para terminar la conexión y se registra este puerto como abierto.

La principal ventaja de esta técnica de escaneo es que pocos sitios están preparados para registrarlos. La desventaja es que en algunos sistemas Unix, se necesitan privilegios de administrador para construir estos paquetes SYN.

- **TCP FIN Scanning– Stealth Port Scanning**

Hay veces en que incluso el scaneo SYN no es lo suficientemente "clandestino" o limpio. Algunos sistemas (Firewalls y filtros de paquetes) monitorizan la red en busca de paquetes SYN a puertos restringidos.

Para subsanar este inconveniente los paquetes FIN, en cambio, podrían ser capaces de pasar sin ser advertidos. Este tipo de Scaneo está basado en la idea de que los puertos cerrados tienden a responder a los paquetes FIN con el RST correspondiente. Los puertos abiertos, en cambio, suelen ignorar el paquete en cuestión.

Este es un comportamiento correcto del protocolo TCP, aunque algunos sistemas, entre los que se hallan los de Microsoft®, no cumplen con este requerimiento, enviando paquetes RST siempre, independientemente de si el puerto está abierto o cerrado. Como resultado, no son vulnerables a este tipo de scaneo. Sin embargo, es posible realizarlo en otros sistemas Unix.

Este último es un ejemplo en el que se puede apreciar que algunas vulnerabilidades se presentan en las aplicación de tecnologías (en este caso el protocolo TCP nacido en los años '70) y no sobre sus implementaciones. Es más, se observa que una implementación incorrecta (la de Microsoft®) soluciona el problema.



"Muchos de los problemas globales de vulnerabilidades son inherentes al diseño original de algunos protocolos"(1).

- **Fragmentation Scanning**

Esta no es una nueva técnica de scaneo como tal, sino una modificación de las anteriores. En lugar de enviar paquetes completos de sondeo, los mismos se peticionan en un par de pequeños fragmentos IP. Así, se logra partir una cabecera IP en distintos paquetes para hacerlo más difícil de monitorizar por los filtros que pudieran estar ejecutándose en la máquina objetivo.

Sin embargo, algunas implementaciones de estas técnicas tienen problemas con la gestión de este tipo de paquetes tan pequeños, causando una caída de rendimiento en el sistema del intruso o en el de la víctima. Problemas de esta índole convierte en detectables a este tipo de ataque.

- **Eavesdropping–Packet Sniffing**

Muchas redes son vulnerables al Eavesdropping, o a la pasiva intercepción (sin modificación) del tráfico de red.

Esto se realiza con Packet Sniffers, los cuales son programas que monitorean los paquetes que circulan por la red. Los Sniffers pueden ser colocados tanto en una estación de trabajo conectada a la red, como a un equipo Router o a un Gateway de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías. Cada máquina conectada a la red (mediante una placa con una dirección única) verifica la dirección destino de los paquetes TCP. Si estas direcciones son iguales asume que el paquete enviado es para ella, caso contrario libera el paquete para que otras placas lo analicen. Un Sniffers consiste en colocar a la placa de red en un modo llamado promiscuo, el cual desactiva



el filtro de verificación de direcciones y por lo tanto todos los paquetes enviados a la red llegan a esta placa (computadora donde está instalado el Sniffer). Inicialmente este tipo de software, era únicamente utilizado por los administradores de redes locales, aunque con el tiempo llegó a convertirse en una herramienta muy usada por los intrusos.

Actualmente existen Sniffers para capturar cualquier tipo de información específica. Por ejemplo passwords de un recurso compartido o de acceso a una cuenta, que generalmente viajan sin encriptar al ingresar a sistemas de acceso remoto. También son utilizados para capturar números de tarjetas de crédito y direcciones de e-mails entrantes y salientes. El análisis de tráfico puede ser utilizado también para determinar relaciones entre organizaciones e individuos.

Para realizar estas funciones se analizan las tramas de un segmento de red, y presentan al usuario sólo las que interesan. Normalmente, los buenos Sniffers, no se pueden detectar, aunque la inmensa mayoría, y debido a que están demasiado relacionados con el protocolo TCP/IP, si pueden ser detectados con algunos trucos.

- **Snooping–Downloading**

Los ataques de esta categoría tienen el mismo objetivo que el Sniffing: obtener la información sin modificarla. Sin embargo los métodos son diferentes. Aquí, además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de correo electrónico y otra información guardada, realizando en la mayoría de los casos un downloading (copia de documentos) de esa información a su propia computadora, para luego hacer un análisis exhaustivo de la misma. El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software. Los casos más resonantes de este tipo de ataques fueron: el robo de un



archivo con más de 1700 números de tarjetas de crédito desde una compañía de música mundialmente famosa, y la difusión ilegal de reportes oficiales reservados de las Naciones Unidas, acerca de la violación de derechos humanos en algunos países europeos en estado de guerra.

5.9. Amenazas lógicas de autenticación

Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y password.

- **Spoofing-Looping**

Spoofing puede traducirse como "hacerse pasar por otro" y el objetivo de esta técnica, justamente, es actuar en nombre de otros usuarios, usualmente para realizar tareas de Snooping o Tampering (ver a continuación Ataques de Modificación y Daño). Una forma común de Spoofing es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él. El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza este para entrar en otro, y así sucesivamente. Este proceso, llamado Looping, tiene la finalidad de "evaporar" la identificación y la ubicación del atacante. El camino tomado desde el origen hasta el destino puede tener muchas estaciones, que exceden obviamente los límites de un país. Otra consecuencia del Looping es que una compañía o gobierno pueden suponer que están siendo atacados por un competidor o una agencia de gobierno extranjera, cuando en realidad están seguramente siendo atacado por un Insider, o por un estudiante a miles de Kilómetros de distancia, pero que ha tomado la identidad de otros.



La investigación de procedencia de un Looping es casi imposible, ya que el investigador debe contar con la colaboración de cada administrador de cada red utilizada en la ruta.

El envío de falsos e-mails es otra forma de Spoofing que las redes permiten. Aquí el atacante envía e-mails a nombre de otra persona con cualquier motivo y objetivo. Tal fue el caso de una universidad en EE.UU. que en 1998, que debió reprogramar una fecha completa de exámenes ya que alguien en nombre de la secretaría había cancelado la fecha verdadera y enviado el mensaje a toda la nómina de estudiantes.

Muchos ataques de este tipo comienzan con Ingeniería Social, y los usuarios, por falta de cultura, facilitan a extraños sus identificaciones dentro del sistema usualmente través de una simple llamada telefónica.

- **Spoofing**

Este tipo de ataques (sobre protocolos) suele implicar un buen conocimiento del protocolo en el que se va a basar el ataque. Los ataques tipo Spoofing bastante conocidos son el IP Spoofing, el DNS Spoofing y el Web Spoofing

- **IP Spoofing**

Con el IP Spoofing, el atacante genera paquetes de Internet con una dirección de red falsa en el campo From, pero que es aceptada por el destinatario del paquete. Su utilización más común es enviar los paquetes con la dirección de un tercero, de forma que la víctima "ve" un ataque proveniente de esa tercera red, y no la dirección real del intruso. El esquema con dos puentes es el siguiente:

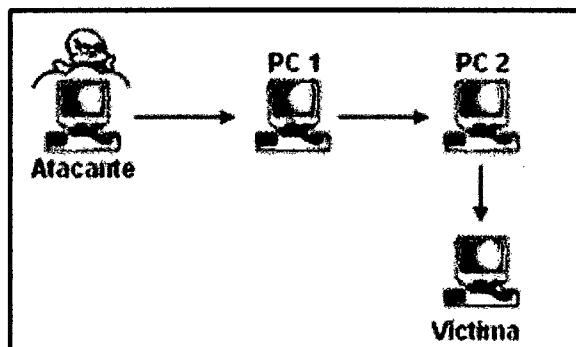


Figura 5.7

Nótese que si la Víctima descubre el ataque verá a la PC_2 como su atacante y no el verdadero origen.

- **DNS Spoofing**

Este ataque se consigue mediante la manipulación de paquetes UDP pudiéndose comprometer el servidor de nombres de dominios (Domain Name Server–DNS) de Windows NT®. Si se permite el método de recursión en la resolución de "Nombre«Dirección IP" en el DNS, es posible controlar algunos aspectos del DNS remoto. La recursión consiste en la capacidad de un servidor de nombres para resolver una petición de dirección IP a partir de un nombre que no figura en su base de datos. Este es el método de funcionamiento por defecto.

- **Web Spoofing**

En el caso Web Spoofing el atacante crea un sitio web completo (falso) similar al que la víctima desea entrar. Los accesos a este sitio están dirigidos por el atacante, permitiéndole monitorear todas las acciones de la víctima, desde sus datos hasta las passwords, números de tarjeta de créditos, etc. El atacante también es libre de modificar



cualquier dato que se esté transmitiendo entre el servidor original y la víctima o viceversa.

- **IP Splicing–Hijacking**

Se produce cuando un atacante consigue interceptar una sesión ya establecida. El atacante espera a que la víctima se identifique ante el sistema y tras ello le suplanta Como usuario autorizado.

Para entender el procedimiento supongamos la siguiente situación:

IP Cliente : IP 195.1.1.1
IP Servidor: IP 195.1.1.2
IP Atacante: IP 195.1.1.3

El cliente establece una conexión con su servidor enviando un paquete que contendrá la dirección origen, destino, número de secuencia (para luego armar el paquete) y un número de autenticación utilizado por el servidor para "reconocer" el paquete siguiente en la secuencia. Supongamos que este paquete contiene:

IP Origen : 195.1.1.1 Puerto 1025
IP Destino: 195.1.1.2 Puerto 23
SEQ = 3DF45ADA (el primero es al azar)
ACK = F454FDF5
Datos: Solicitud

El servidor, luego de recibir el primer paquete contesta al cliente con paquete Hecho (recibido).

IP Origen : 195.1.1.2 Puerto 1025
IP Destino: 195.1.1.1 Puerto 23
SEQ = F454FDF5 (ACK enviado por el cliente)
ACK = 3DF454E4
Datos: Recepción OK (Echo)



El cliente envía un paquete ACK al servidor, sin datos, en donde le comunica lo "perfecto" de la comunicación.

```
IP Origen : 195.1.1.1 Puerto 1025
IP Destino: 195.1.1.2 Puerto 23
SEQ = 3DF454E4 (ACK enviado por el servidor)
ACK = F454FDFF
Datos: Confirmación de Recepción (ACK)
```

El atacante que ha visto, mediante un Sniffer, los paquete que circularon por la red calcula el número de secuencia siguiente: el actual + tamaño del campo de datos. Para calcular el tamaño de este campo:

```
1° Paquete ACK Cliente = F454FDF5
2° Paquete ACK Cliente = F454FDFF
Tamaño del campo datos = F454FDFF - F454FDF5 = 0A
```

Hecho esto el atacante envía un paquete con la siguiente aspecto:

```
IP Origen : IP 195.1.1.1 (IP del Cliente por el atacante)
IP Destino: IP 195.1.1.2 (IP del Servidor)
SEQ = 3DF454E4 (Ultimo ACK enviado por el Cliente)
ACK = F454FE09 (F454FDFF + 0A)
```

El servidor al recibir estos datos no detectará el cambio de origen ya que los campos que ha recibido como secuencia y ACK son los que esperaba recibir. El cliente, a su vez, quedará esperando datos como si su conexión estuviera colgada y el atacante podrá seguir enviando datos mediante el procedimiento descrito.

5.9.1. Utilización de BackDoors

"Las puertas traseras son trozos de código en un programa que permiten a quien las conoce saltarse los métodos usuales de autenticación para realizar ciertas tareas. Habitualmente son



insertados por los programadores del sistema para agilizar la tarea de probar código durante la fase de desarrollo"(1).

Esta situación se convierte en una falla de seguridad si se mantiene, involuntaria o intencionalmente, una vez terminado el producto ya que cualquiera que conozca el agujero o lo encuentre en su código podrá saltarse los mecanismos de control normales.

5.9.2. Utilización de Exploits

Es muy frecuente ingresar a un sistema explotando agujeros en los algoritmos de encriptación utilizados, en la administración de las claves por parte la empresa, o simplemente encontrando un error en los programas utilizados. Los programas para explotar estos "agujeros" reciben el nombre de Exploits y lo que realizan es aprovechar la debilidad, fallo o error hallado en el sistema (hardware o software) para ingresar al mismo.

Nuevos Exploits (explotando nuevos errores en los sistemas) se publican cada día por lo que mantenerse informado de los mismos y de las herramientas para combatirlos es de vital importancia.

5.9.3. Obtención de Passwords

Este método comprende la obtención por "Fuerza Bruta" de aquellas claves que permiten ingresar a los sistemas, aplicaciones, cuentas, etc. atacados.

Muchas passwords de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario y, además, esta nunca (o rara vez) se cambia. En este caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y "diccionarios" que prueban millones de posibles claves hasta encontrar la password correcta.



La política de administración de password será discutida en capítulos posteriores.

5.9.4. Uso de Diccionarios.

Los Diccionarios son archivos con millones de palabras, las cuales pueden ser posibles passwords de los usuarios. Este archivo es utilizado para descubrir dicha password en pruebas de fuerza bruta.

El programa encargado de probar cada una de las palabras encripta cada una de ellas, mediante el algoritmo utilizado por el sistema atacado, y compara la palabra encriptada contra el archivo de passwords del sistema atacado (previamente obtenido). Si coinciden se ha encontrado la clave de acceso al sistema, mediante el usuario correspondiente a la clave hallada. Actualmente es posible encontrar diccionarios de gran tamaño orientados, incluso, a un área específico de acuerdo al tipo de organización que se este atacando.

Podemos observar el tiempo de búsqueda de una clave de acuerdo a su longitud y tipo de caracteres utilizados. La velocidad de búsqueda se supone en 100.000 passwords por segundo, aunque este número suele ser mucho mayor dependiendo del programa utilizado.

Cantidad de Caracteres	26-Letras minúsculas	36-Letras y dígitos	52-Mayúsculas y minúsculas	96-Todos los caracteres
6	51 minutos	6 horas	2,3 días	3 meses
7	22,3 horas	9 días	4 meses	24 años
8	24 días	10,5 meses	17 años	2.288 años
9	21 meses	32,6 años	890 años	219.601 años
10	45 años	1.160 años	45.840 años	21.081.705 años

Figura. 5.8

Aquí puede observarse la importancia de la utilización de passwords con al menos 8 caracteres de longitud y combinando todos los



caracteres disponibles. En el siguiente Capítulo podrá estudiarse las normas de claves relativamente seguras y resistentes.

5.10. Amenazas Logicas -Tipos de Ataques - Denial of Service (DoS)

Los protocolos existentes actualmente fueron diseñados para ser empleados en una comunidad abierta y con una relación de confianza mutua. La realidad indica que es más fácil desorganizar el funcionamiento de un sistema que acceder al mismo; así los ataques de Negación de Servicio tienen como objetivo saturar los recursos de la víctima de forma tal que se inhabilita los servicios brindados por la misma.

Más allá del simple hecho de bloquear los servicios del cliente, existen algunas razones importantes por las cuales este tipo de ataques pueden ser útiles a un atacante:

1. Se ha instalado un troyano y se necesita que la víctima reinicie la máquina para que surta efecto.
2. Se necesita cubrir inmediatamente sus acciones o un uso abusivo de CPU. Para ello provoca un "crash" del sistema, generando así la sensación de que ha sido algo pasajero y raro.
3. El intruso cree que actúa bien al dejar fuera de servicio algún sitio web que le disgusta. Este accionar es común en sitios pornográficos, religiosos o de abuso de menores.
4. El administrador del sistema quiere comprobar que sus instalaciones no son vulnerables a este tipo de ataques.
5. El administrador del sistema tiene un proceso que no puede "matar" en su servidor y, debido a este, no puede acceder al sistema. Para ello, lanza contra sí mismo un ataque DoS deteniendo los servicios.



- **Jamming o Flooding**

Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más pueda utilizarla.

Aquí el atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP usando Spoofing y Looping. El sistema responde al mensaje, pero como no recibe respuesta, acumula buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas. Muchos ISPs (proveedores de Internet) han sufrido bajas temporales del servicio por ataques que explotan el protocolo TCP. Muchos Hosts de Internet han sido dados de baja por el "ping de la muerte" (una versión-trampa del comando ping).

Mientras que el ping normal simplemente verifica si un sistema esta enlazado a la red, el ping de la muerte causa el bloqueo instantáneo del equipo. Esta vulnerabilidad ha sido ampliamente utilizada en el pasado pero, aún hoy pueden encontrarse sistemas vulnerables. Otra acción común es la de enviar millares de e-mails sin sentido a todos los usuarios posibles en forma continua, saturando los sistemas destinos.

- **Syn Flood**

Como ya se explicó en el TCP SYN Scanning el protocolo TCP se basa en una conexión en tres pasos. Pero, si el paso final no llega a establecerse, la conexión permanece en un estado denominado "semiabierto".

El SYN Flood es el más famoso de los ataques del tipo Denial of Service, publicado por primera vez en la revista under Phrack; y se basa en un "saludo" incompleto entre los dos



hosts. El Cliente envía un paquete SYN pero no responde al paquete ACK ocasionando que la pila TCP/IP espere cierta cantidad de tiempo a que el Host hostil responda antes de cerrar la conexión. Si se crean muchas peticiones incompletas de conexión (no se responde a ninguna), el Servidor estará inactivo mucho tiempo esperando respuesta. Esto ocasiona la lentitud en los demás servicios.

SYN Flood aprovecha la mala implementación del protocolo TCP, funcionando de la siguiente manera:

Se envía al destino, una serie de paquetes TCP con el bit SYN activado, (petición de conexión) desde una dirección IP Spoofeada. Esta última debe ser inexistente para que el destino no pueda completar el saludo con el cliente.

Aquí radica el fallo de TCP: ICMP reporta que el cliente es inexistente, pero TCP ignora el mensaje y sigue intentando terminar el saludo con el cliente de forma continua.

Cuando se realiza un Ping a una máquina, esta tiene que procesarlo. Y aunque se trate de un proceso sencillo, (no es más que ver la dirección de origen y enviarle un paquete Reply), siempre consume recursos del sistema. Si no es un Ping, sino que son varios a la vez, la máquina se vuelve más lenta... si lo que se recibe son miles de solicitudes, puede que el equipo deje de responder (Flood).

Es obligatorio que la IP origen sea inexistente, ya que sino el objetivo, logrará responderle al cliente con un SYN/ACK, y como esa IP no pidió ninguna conexión, le va a responder al objetivo con un RST, y el ataque no tendrá efecto. El problema es que muchos sistemas operativos tienen un límite muy bajo en el número de conexiones "semiabiertas" que pueden manejar en un momento determinado (5 a 30). Si se supera ese límite, el servidor sencillamente dejará de responder a las nuevas peticiones de conexión que le vayan llegando. Las conexiones "semiabiertas" van caducando tras un tiempo, liberando "huecos" para nuevas conexiones, pero mientras el



atacante mantenga el SYN Flood, la probabilidad de que una conexión recién liberada sea capturada por un nuevo SYN malicioso es muy alta.

- **Connection Flood**

La mayoría de las empresas que brindan servicios de Internet (ISP) tienen un límite máximo en el número de conexiones simultáneas. Una vez que se alcanza ese límite, no se admitirán conexiones nuevas. Así, por ejemplo, un servidor Web puede tener, por ejemplo, capacidad para atender a mil usuarios simultáneos. Si un atacante establece mil conexiones y no realiza ninguna petición sobre ellas, monopolizará la capacidad del servidor. Las conexiones van caducando por inactividad poco a poco, pero el atacante sólo necesita intentar nuevas conexiones, (como ocurre con el caso del SYN Flood) para mantener fuera de servicio el servidor.

- **Net Flood**

En estos casos, la red víctima no puede hacer nada. Aunque filtre el tráfico en sus sistemas, sus líneas estarán saturadas con tráfico malicioso, incapacitándolas para cursar tráfico útil. Un ejemplo habitual es el de un teléfono: si alguien quiere molestar, sólo tiene que llamar, de forma continua. Si se descuelga el teléfono (para que deje de molestar), tampoco se puede recibir llamadas de otras personas. Este problema es habitual, por ejemplo, cuando alguien intenta mandar un fax empleando el número de voz: el fax insiste durante horas, sin que el usuario llamado pueda hacer nada al respecto. En el caso de Net Flooding ocurre algo similar. El atacante envía tantos paquetes de solicitud de conexión que las conexiones auténticas simplemente no pueden competir.



En casos así el primer paso a realizar es el ponerse en contacto con el Proveedor del servicio para que intente determinar la fuente del ataque y, como medida provisional, filtre el ataque en su extremo de la línea.

El siguiente paso consiste en localizar las fuentes del ataque e informar a sus administradores, ya que seguramente se estarán usando sus recursos sin su conocimiento y consentimiento. Si el atacante emplea IP Spoofing, el rastreo puede ser casi imposible, ya que en muchos casos la fuente del ataque es, a su vez, víctima y el origen último puede ser prácticamente imposible de determinar (Looping).

- **Land Attack**

Este ataque consiste en un Bug (error) en la implementación de la pila TCP/IP de las plataformas Windows®. El ataque consiste en mandar a algún puerto abierto de un servidor (generalmente al NetBIOS 113 o 139) un paquete, maliciosamente construido, con la dirección y puerto origen igual que la dirección y puerto destino.

Por ejemplo se envían un mensaje desde la dirección 10.0.0.1:139 hacia ella misma. El resultado obtenido es que luego de cierta cantidad de mensajes enviados–recibidos la máquina termina colgándose. Existen ciertas variantes a este método consistente, por ejemplo, en enviar el mensaje a una dirección específica sin especificar el puerto.

- **Smurf o Broadcast Storm**

Este ataque es bastante simple y a su vez devastador. Consiste en recolectar una serie de direcciones BroadCast para, a continuación, mandar una petición ICMP (simulando un Ping) a cada una de ellas en serie, varias veces, falsificando la

dirección IP de origen (máquina víctima). Este paquete maliciosamente manipulado, será repetido en difusión (Broadcast), y cientos ó miles de hosts mandarán una respuesta a la víctima cuya dirección IP figura en el paquete ICMP.

Gráficamente:

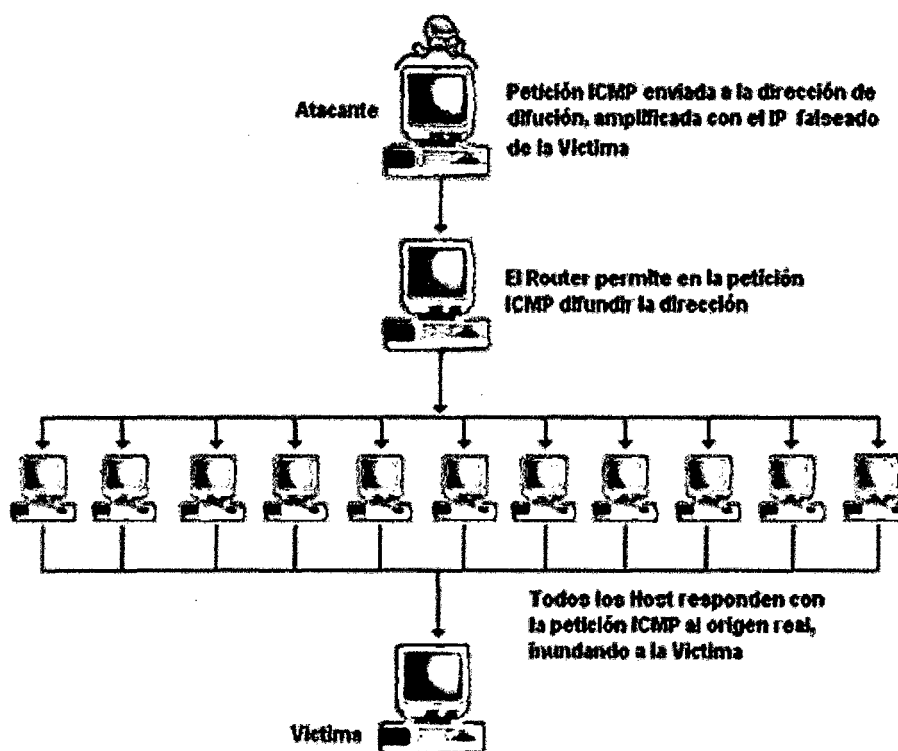


Figura 5.9

Suponiendo que se considere una red de tipo C la dirección de Broadcast sería .255; por lo que el "simple" envío de un paquete se convierte en un efecto multiplicador devastador. Desgraciadamente la víctima no puede hacer nada para evitarlo. La solución está en manos de los administradores de red, los cuales deben configurar adecuadamente sus Routers para filtrar los paquetes ICMP de petición indeseada (Broadcast); o bien configurar sus máquinas para que no



respondan a dichos paquetes. Es decir, que lo que se parchea son las máquinas/redes que puedan actuar de intermediarias (inocentes) en el ataque y no la máquina víctima.

También se podría evitar el ataque si el Router/Firewall de salida del atacante estuviera convenientemente configurado para evitar Spoofing. Esto se haría filtrando todos los paquetes de salida que tuvieran una dirección de origen que no perteneciera a la red interna.

- **OOB, Supernuke o Winnuke**

Un ataque característico, y quizás el más común, de los equipos con Windows® es el Nuke, que hace que los equipos que escuchan por el puerto NetBIOS sobre TCP/UDP 137 a 139, queden fuera de servicio, o disminuyan su rendimiento al enviarle paquetes UDP manipulados. Generalmente se envían fragmentos de paquetes Out Of Band, que la máquina víctima detecta como inválidos pasando a un estado inestable. OOB es el término normal, pero realmente consiste en configurar el bit Urgente (URG) en los indicadores del encabezamiento TCP, lo que significa que este bit es válido. Este ataque puede prevenirse instalando los parches adecuados suministrado por el fabricante del sistema operativo afectado. Un filtro efectivo debería garantizar la detección de una inundación de bits Urgentes.

- **Teardrop I y II-Newtear-Bonk-Boink**

Al igual que el Supernuke, los ataques Teardrop I y Teardrop II afectan a fragmentos de paquetes. Algunas implementaciones de colas IP no vuelven a armar correctamente los fragmentos que se superponen, haciendo que el sistema se cuelgue. Windows NT® 4.0 de Microsoft® es especialmente vulnerable a este ataque. Aunque existen Patches (parches) que pueden



aplicarse para solucionar el problema, muchas organizaciones no lo hacen, y las consecuencias pueden ser devastadoras. Los ataques tipo Teardrop son especialmente peligrosos ya que existen multitud de implementaciones (algunas de ellas forman paquetes), que explotan esta debilidad. Las más conocidas son aquellas con el nombre Newtear, Bonk y Boink.

- **E-Mail Bombing–Spamming**

- El e-mail Bombing consiste en enviar muchas veces un mensaje idéntico a una misma dirección, saturando así el mailbox del destinatario.
- El Spamming, en cambio se refiere a enviar un e-mail a miles de usuarios, haya estos solicitados el mensaje o no. Es muy utilizado por las empresas para publicitar sus productos.
- El Spamming está siendo actualmente tratado por las leyes europeas (principalmente España) como una violación de los derechos de privacidad del usuario.

5.11. Amenazas Lógicas - Tipos de Ataques - Ataques de Modificación (Daño)

- **Tampering o Data Diddling**

Esta categoría se refiere a la modificación desautorizada de los datos o el software instalado en el sistema víctima (incluyendo borrado de archivos). Son particularmente serios cuando el que lo realiza ha obtenido derechos de Administrador o Supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema. Aun así, si no hubo intenciones de "bajar" el sistema por parte del atacante; el Administrador posiblemente necesite darlo de baja por



horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada. Como siempre, esto puede ser realizado por Insiders o Outsiders, generalmente con el propósito de fraude o de dejar fuera de servicio a un competidor. Son innumerables los casos de este tipo: empleados bancarios (o externos) que crean falsas cuentas para derivar fondos de otras cuentas, estudiantes que modifican calificaciones de exámenes, o contribuyentes que pagan para que se les anule una deuda impositiva. Múltiples Web Sites han sido víctimas del cambio en sus páginas por imágenes (o manifiestos) terroristas o humorísticos, como el ataque de The Mentor, ya visto, a la NASA; o la reciente modificación del Web Site del CERT (mayo de 2001).

Otras veces se reemplazan versiones de software por otros con el mismo nombre pero que incorporan código malicioso (virus, troyanos, etc.). La utilización de programas troyanos y difusión de virus está dentro de esta categoría, y se profundizará sobre el tema en otra sección el presente capítulo.

- **Borrado de Huellas**

El borrado de huellas es una de las tareas más importantes que debe realizar el intruso después de ingresar en un sistema, ya que, si se detecta su ingreso, el administrador buscará como conseguir "tapar el hueco" de seguridad, evitar ataques futuros e incluso rastrear al atacante. Las **Huellas** son todas las tareas que realizó el intruso en el sistema y por lo general son almacenadas en Logs (archivo que guarda la información de lo que se realiza en el sistema) por el sistema operativo. Los archivos Logs son una de las principales herramientas (y el principal enemigo del atacante) con las que cuenta un administrador para conocer los detalles de las tareas realizadas en el sistema y la detección de intrusos.



- **Ataques Mediante Java Applets**

Java es un lenguaje de programación interpretado, desarrollado inicialmente por la empresa SUN. Su mayor popularidad la merece por su alto grado de seguridad. Los más usados navegadores actuales, implementan Máquinas Virtuales Java (MVJ) para ser capaces de ejecutar programas (Applets) de Java.

Estos Applets, al fin y al cabo, no son más que código ejecutable y como tal, susceptible de ser manipulado por intrusos. Sin embargo, partiendo del diseño, Java siempre ha pensado en la seguridad del sistema. Las restricciones a las que somete a los Applets son de tal envergadura (imposibilidad de trabajar con archivos a no ser que el usuario especifique lo contrario, imposibilidad de acceso a zonas de memoria y disco directamente, firma digital, etc.) que es muy difícil lanzar ataques. Sin embargo, existe un grupo de expertos (1) especializados en descubrir fallas de seguridad (2) en las implementaciones de las MVJ.

- **Ataques Mediante JavaScript y VBScript**

JavaScript (de la empresa Netscape®) y VBScript (de Microsoft®) son dos lenguajes usados por los diseñadores de sitios Web para evitar el uso de Java. Los programas realizados son interpretados por el navegador. Aunque los fallos son mucho más numerosos en versiones antiguas de JavaScript, actualmente se utilizan para explotar vulnerabilidades específicas de navegadores y servidores de correo ya que no se realiza ninguna evaluación sobre si el código.



- **Ataques Mediante ActiveX**

ActiveX es una de las tecnologías más potentes que ha desarrollado Microsoft®. Mediante ActiveX es posible reutilizar código, descargar código totalmente funcional de un sitio remoto, etc. Esta tecnología es considerada la respuesta de Microsoft® a Java. ActiveX soluciona los problemas de seguridad mediante certificados y firmas digitales. Una Autoridad Certificadora (AC) expende un certificado que acompaña a los controles activos y a una firma digital del programador. Cuando un usuario descarga una página con un control, se le preguntará si confía en la AC que expendió el certificado y/o en el control ActiveX. Si el usuario acepta el control, éste puede pasar a ejecutarse sin ningún tipo de restricciones (sólo las propias que tenga el usuario en el sistema operativo). Es decir, la responsabilidad de la seguridad del sistema se deja en manos del usuario, ya sea este un experto cibernauta consciente de los riesgos que puede acarrear la acción o un perfecto novato en la materia. Esta última característica es el mayor punto débil de los controles ActiveX ya que la mayoría de los usuarios aceptan el certificado sin siquiera leerlo, pudiendo ser esta la fuente de un ataque con un control dañino.

La filosofía ActiveX es que las Autoridades de Certificación se fían de la palabra del programador del control. Es decir, el programador se compromete a firmar un documento que asegura que el control no es nocivo. Evidentemente siempre hay programadores con pocos escrúpulos o con ganas de experimentar.

Así, un conocido grupo de hackers alemanes (3), desarrolló un control ActiveX maligno que modificaba el programa de Gestión Bancaria Personal Quicken95© de tal manera que si un usuario aceptaba el control, éste realizaba la tarea que supuestamente tenía que hacer y además modificaba el Quicken, para que la próxima vez que la víctima se conectara a su banco, se iniciara



automáticamente una transferencia a una cuenta del grupo alemán. Otro control ActiveX muy especialmente "malévolo" es aquel que manipula el código de ciertos exploradores, para que éste no solicite confirmación al usuario a la hora de descargar otro control activo de la Web. Es decir, deja totalmente descubierto, el sistema de la víctima, a ataques con tecnología ActiveX.

La autenticación de usuarios mediante Certificados y las Autoridades Certificadoras será abordada con profundidad en capítulos posteriores.

- **Vulnerabilidades en los Navegadores**

Generalmente los navegadores no fallan por fallos intrínsecos, sino que fallan las tecnologías que implementan, aunque en este punto analizaremos realmente fallos intrínsecos de los navegadores, como pueden ser los "Buffer Overflow"(4).

Los "Buffer Overflows" consisten en explotar una debilidad relacionada con los buffers que la aplicación usa para almacenar las entradas de usuario. Por ejemplo, cuando el usuario escribe una dirección en formato URL ésta se guarda en un buffer para luego procesarla. Si no se realizan las oportunas operaciones de comprobación, un usuario podría manipular estas direcciones. Los protocolo usado puede ser HTTP, pero también otros menos conocidos, internos de cada explorador, como el "res:" o el "mk:". Precisamente existen fallos de seguridad del tipo "Buffer Overflow" en la implementación de estos dos protocolos. Además la reciente aparición (octubre de 2000) de vulnerabilidades del tipo Transversal en el servidor Web Internet Información Server© de la empresa Microsoft®, explotando fallas en la traducción de caracteres Unicode, puso de manifiesto cuan fácil puede resultar explotar una cadena no validada. Por ejemplo:



```
www.servidor.com/_vti_bin/..%c0%af../..%c0%af../..%c0%af../wi  
nnt/system32/cmd.exe?/c+dir+c:\
```

devuelve el directorio de la unidad c: del servidor deseado. Para poder lanzar este tipo de ataques hay que tener un buen conocimiento de lenguaje Assembler y de la estructura interna de la memoria del sistema operativo utilizado o bien, leer la documentación de sitios web donde explican estas fallas. También se puede citar el fallo de seguridad descubierto por Cybersnot Industries® relativo a los archivos ".lnk" y ".url" de Windows 95® y NT® respectivamente. Algunas versiones de Microsoft Internet Explorer® podían ser utilizadas para ejecutar la aplicación que se deseara siempre que existiera en la computadora de la víctima (por ejemplo el tan conocido y temido *format.com*).

Para más información relacionada con los ataques intrínsecos a los navegadores, se aconsejan las páginas no oficiales de seguridad tanto en Internet Explorer®(5) como en Netscape Communicator®(6).

5.12. Firewall – Cortafuegos

Quizás uno de los elementos más publicitados a la hora de establecer seguridad, sean estos elementos. Aunque deben ser uno de los sistemas a los que más se debe prestar atención, distan mucho de ser la solución final a los problemas de seguridad.

De hecho, los Firewalls no tienen nada que hacer contra técnicas como la Ingeniería Social y el ataque de Insiders.

Un **Firewall** es un sistema (o conjunto de ellos) ubicado entre dos redes y que ejerce la una política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es (por ejemplo Internet).

Puede consistir en distintos dispositivos, tendientes a los siguientes objetivos:

1. Todo el tráfico desde dentro hacia fuera, y viceversa, debe pasar a través de él.
2. Sólo el tráfico autorizado, definido por la política local de seguridad, es permitido.

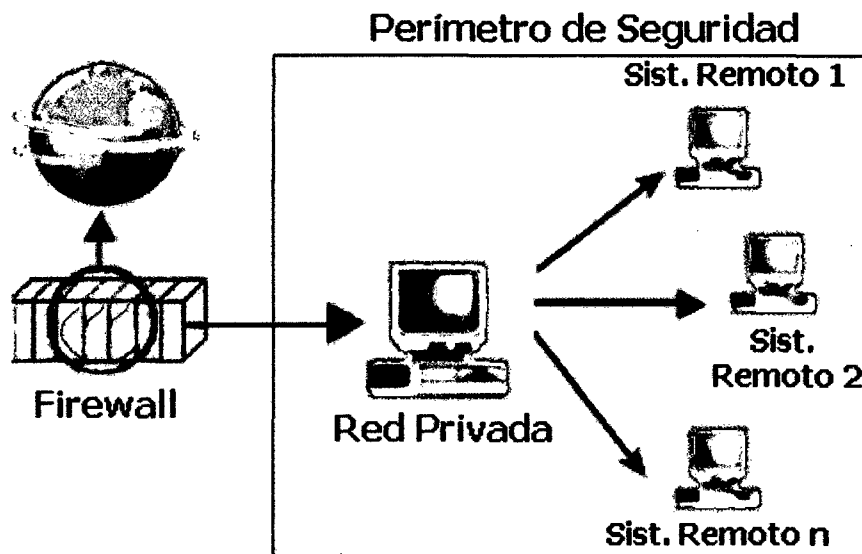


Figura. 5.10

Como puede observarse, el Muro Cortafuegos, sólo sirven de defensa perimetral de las redes, no defienden de ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa.

Algunos Firewalls aprovechan esta capacidad de que toda la información entrante y saliente debe pasar a través de ellos para proveer servicios de seguridad adicionales como la encriptación del tráfico de la red. Se entiende que si dos Firewalls están conectados, ambos deben "hablar" el mismo método de encriptación-des encriptación para entablar la comunicación.



5.13. Routers y Bridges

Cuando los paquetes de información viajan entre su destino y origen, vía TCP/IP, estos pasan por diferentes Routers (enrutadores a nivel de Red). Los Routers son dispositivos electrónicos encargados de establecer comunicaciones externas y de convertir los protocolos utilizados en las LAN en protocolos de WAN y viceversa. En cambio, si se conectan dos redes del tipo LAN se utilizan Bridges, los cuales son puentes que operan a nivel de Enlace. La evolución tecnológica les ha permitido transformarse en computadoras muy especializadas capaz de determinar, si el paquete tiene un destino externo y el camino más corto y más descongestionado hacia el Router de la red destino. En caso de que el paquete provenga de afuera, determina el destino en la red interna y lo deriva a la máquina correspondiente o devuelve el paquete a su origen en caso de que él no sea el destinatario del mismo.

Los Routers "toman decisiones" en base a un conjunto de datos, regla, filtros y excepciones que le indican que rutas son las más apropiadas para enviar los paquetes.

5.14. Tipos de Firewall

1. Filtrado de Paquetes
2. Proxy-Gateways de Aplicaciones
3. Dual-Homed Host
4. Screened Host
5. Screened Subnet
6. Inspección de Paquetes

Este tipo de Firewalls se basa en el principio de que cada paquete que circula por la red es inspeccionado, así como también su procedencia y destino. Se aplican desde la capa de Red hasta la de Aplicaciones. Generalmente son instalados cuando se requiere seguridad sensible al contexto y en aplicaciones muy complejas.



7. Firewalls Personales

Estos Firewalls son aplicaciones disponibles para usuarios finales que desean conectarse a una red externa insegura y mantener su computadora a salvo de ataques que puedan ocasionarle desde un simple "cuelgue" o infección de virus hasta la pérdida de toda su información almacenada.

5.14.1. Políticas de Diseño de Firewalls

Las políticas de accesos en un Firewalls se deben diseñar poniendo principal atención en sus limitaciones y capacidades pero también pensando en las amenazas y vulnerabilidades presentes en una red externa insegura.

Conocer los puntos a proteger es el primer paso a la hora de establecer normas de seguridad. También es importante definir los usuarios contra los que se debe proteger cada recurso, ya que las medidas diferirán notablemente en función de esos usuarios.

Generalmente se plantean algunas preguntas fundamentales que debe responder cualquier política de seguridad:

¿Qué se debe proteger? Se deberían proteger todos los elementos de la red interna (hardware, software, datos, etc.).

¿De quién protegerse? De cualquier intento de acceso no autorizado desde el exterior y contra ciertos ataques desde el interior que puedan preverse y prevenir.

Sin embargo, podemos definir niveles de confianza, permitiendo selectivamente el acceso de determinados usuarios externos a determinados servicios o denegando cualquier tipo de acceso a otros. ¿Cómo protegerse? Esta es la pregunta más difícil y está orientada a establecer el nivel de monitorización, control y respuesta deseado en la organización. Puede optarse por alguno de los siguientes paradigmas o estrategias:

Paradigmas de seguridad. Se permite cualquier servicio excepto aquellos expresamente prohibidos.



Se prohíbe cualquier servicio excepto aquellos expresamente permitidos. La más recomendada y utilizada aunque algunas veces suele acarrear problemas por usuarios descontentos que no pueden acceder a tal cual servicio.

Estrategias de seguridad

Paranoica: se controla todo, no se permite nada.

Prudente: se controla y se conoce todo lo que sucede.

Permisiva: se controla pero se permite demasiado.

Promiscua: no se controla (o se hace poco) y se permite todo.

¿Cuánto costará? Estimando en función de lo que se desea proteger se debe decidir cuánto es conveniente invertir.

5.14.2. Restricciones en el Firewall

La parte más importante de las tareas que realizan los Firewalls, la de permitir o denegar determinados servicios, se hacen en función de los distintos usuarios y su ubicación:

1. **Usuarios internos con permiso de salida para servicios restringidos:** permite especificar una serie de redes y direcciones a los que denomina **Trusted (validados)** . Estos usuarios, cuando provengan del interior, van a poder acceder a determinados servicios externos que se han definido.
2. **Usuarios externos con permiso de entrada desde el exterior:** este es el caso más sensible a la hora de vigilarse. Suele tratarse de usuarios externos que por algún motivo deben acceder para consultar servicios de la red interna.

También es habitual utilizar estos accesos por parte de terceros para prestar servicios al perímetro interior de la red. Sería conveniente que estas cuentas sean activadas y desactivadas bajo demanda y únicamente el tiempo que sean necesarias.



5.14.3. Beneficios de un Firewall

Los Firewalls manejan el acceso entre dos redes, y si no existiera, todas las computadoras de la red estarían expuestas a ataques desde el exterior. Esto significa que la seguridad de toda la red, estaría dependiendo de que tan fácil fuera violar la seguridad local de cada máquina interna.

El Firewall es el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataque, el administrador será el responsable de la revisión de estos monitorios.

Otra causa que ha hecho que el uso de Firewalls se haya convertido en uso casi imperativo es el hecho que en los últimos años en Internet han entrado en crisis el número disponible de direcciones IP, esto ha hecho que las intranets adopten direcciones sin clase, las cuales salen a Internet por medio de un "traductor de direcciones", el cual puede alojarse en el Firewall.

Los Firewalls también son importantes desde el punto de vista de llevar las estadísticas del ancho de banda "consumido" por el tráfico de la red, y que procesos han influido más en ese tráfico, de esta manera el administrador de la red puede restringir el uso de estos procesos y economizar o aprovechar mejor el ancho de banda disponible.

Los Firewalls también tienen otros usos. Por ejemplo, se pueden usar para dividir partes de un sitio que tienen distintas necesidades de seguridad o para albergar los servicios WWW y FTP brindados.

5.14.4. Limitaciones de un Firewall

La limitación más grande que tiene un Firewall sencillamente es el hueco que no se tapa y que coincidentemente o no, es descubierto por un intruso. Los Firewalls no son sistemas inteligentes, ellos actúan de acuerdo a parámetros introducidos por su diseñador, por ende si un paquete de información no se encuentra dentro de estos parámetros como una amenaza de peligro simplemente lo deja pasar.



Más peligroso aún es que ese intruso deje Back Doors, abriendo un hueco diferente y borre las pruebas o indicios del ataque original.

Otra limitación es que el Firewall "NO es contra humanos", es decir que si un intruso logra entrar a la organización y descubrir passwords o los huecos del Firewall y difunde esta información, el Firewall no se dará cuenta.

El Firewall tampoco provee de herramientas contra la filtración de software o archivos infectados con virus, aunque es posible dotar a la máquina, donde se aloja el Firewall, de antivirus apropiados.

Finalmente, un Firewall es vulnerable, él NO protege de la gente que está dentro de la red interna. El Firewall trabaja mejor si se complementa con una defensa interna. Como moraleja: "cuanto mayor sea el tráfico de entrada y salida permitido por el Firewall, menor será la resistencia contra los paquetes externos. El único Firewall seguro (100%) es aquel que se mantiene apagado" (1)

5.14.5. Firewall - Filtrado de Paquetes

Se utilizan Routers con filtros y reglas basadas en políticas de control de acceso. El Router es el encargado de filtrar los paquetes (un Choke) basados en cualquiera de los siguientes criterios:

1. Protocolos utilizados.
2. Dirección IP de origen y de destino.
3. Puerto TCP-UDP de origen y de destino.

Estos criterios permiten gran flexibilidad en el tratamiento del tráfico. Restringiendo las comunicaciones entre dos computadoras (mediante las direcciones IP) se permite determinar entre cuales máquinas la comunicación está permitida.

El filtrado de paquetes mediante puertos y protocolos permite establecer que servicios estarán disponibles al usuario y por cuales puertos. Se puede permitir navegar en la WWW (puerto 80 abierto) pero no acceder a la transferencia de archivos vía FTP (puerto 21 cerrado).



Debido a su funcionamiento y estructura basada en el filtrado de direcciones y puertos este tipo de Firewalls trabajan en los niveles de Transporte y de Red del Modelo OSI y están conectados a ambos perímetros (interior y exterior) de la red.

Tienen la ventaja de ser económicos, tienen un alto nivel de desempeño y son transparentes para los usuarios conectados a la red. Sin embargo presenta debilidades como:

- No protege las capas superiores a nivel OSI.

- Las necesidades aplicativas son difíciles de traducir como filtros de protocolos y puertos.

- No son capaces de esconder la topología de redes privadas, por lo que exponen la red al mundo exterior.

- Sus capacidades de auditoría suelen ser limitadas, al igual que su capacidad de registro de actividades.

- No soportan políticas de seguridad complejas como autenticación de usuarios y control de accesos con horarios prefijados.

5.14.6. Firewall - Dual-Homed Host

Son dispositivos que están conectados a ambos perímetros (interior y exterior) y no dejan pasar paquetes IP (como sucede en el caso del Filtrado de Paquetes), por lo que se dice que actúan con el "IP-Forwarding desactivado".

Un usuario interior que desee hacer uso de un servicio exterior, deberá conectarse primero al Firewall, donde el Proxy atenderá su petición, y en función de la configuración impuesta en dicho Firewall, se conectará al servicio exterior solicitado y hará de puente entre este y el usuario interior.

Es decir que se utilizan dos conexiones. Uno desde la máquina interior hasta el Firewall y el otro desde este hasta la máquina que albergue el servicio exterior.

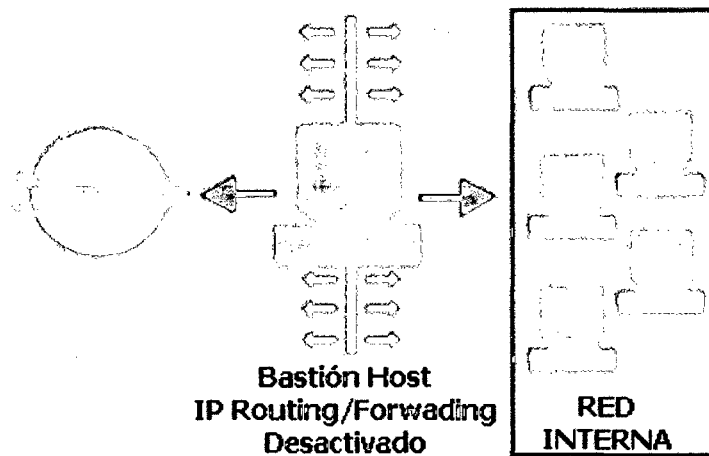


Figura 5.11

5.14.7. Firewall - Screened Host

En este caso se combina un Router con un host bastión y el principal nivel de seguridad proviene del filtrado de paquetes. En el bastión, el único sistema accesible desde el exterior, se ejecuta el Proxy de aplicaciones y en el Choke se filtran los paquetes considerados peligrosos y sólo se permiten un número reducido de servicios.

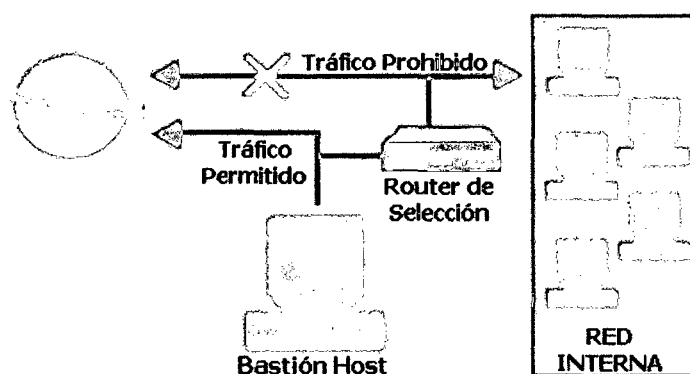


Figura 5.12

5.14.8. Firewall - Screened Subnet

En este diseño se intenta aislar la máquina más atacada y vulnerable del Firewall, el Nodo Bastión. Para ello se establece una Zona Desmilitarizada (DMZ) de forma tal que sin un intruso accede a esta máquina no consiga el acceso total a la subred protegida.

En este esquema se utilizan dos Routers: uno exterior y otro interior. El Router exterior tiene la misión de bloquear el tráfico no deseado en ambos sentidos: hacia la red interna y hacia la red externa. El Router interior hace lo mismo con la red interna y la DMZ (zona entre el Router externo y el interno).

Es posible definir varios niveles de DMZ agregando más Routers, pero destacando que las reglas aplicadas a cada uno deben ser distintas ya que en caso contrario los niveles se simplificarían a uno solo.

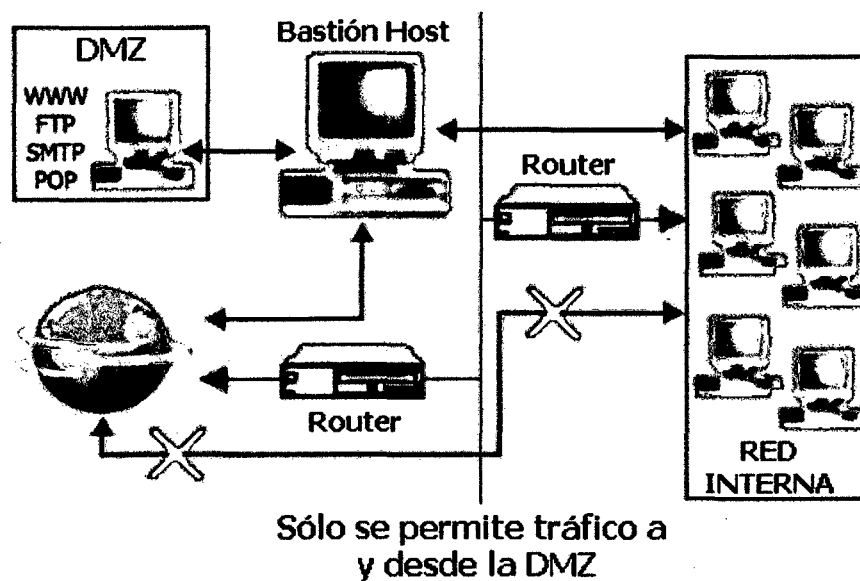


Figura 5.13



Como puede apreciarse la Zona Desmilitarizada aísla físicamente los servicios internos, separándolos de los servicios públicos. Además, no existe una conexión directa entre la red interna y la externa.

Los sistemas Dual-Homed Host y Screened pueden ser complicados de configurar y comprobar, lo que puede dar lugar, paradójicamente, a importantes agujeros de seguridad en toda la red. En cambio, si se encuentran bien configurados y administrados pueden brindar un alto grado de protección y ciertas ventajas:

1. Ocultamiento de la información: los sistemas externos no deben conocer el nombre de los sistemas internos. El Gateway de aplicaciones es el único autorizado a conectarse con el exterior y el encargado de bloquear la información no solicitada o sospechosa.
2. Registro de actividades y autenticación robusta: El Gateway requiere de autenticación cuando se realiza un pedido de datos externos. El registro de actividades se realiza en base a estas solicitudes.
3. Reglas de filtrado menos complejas: Las reglas del filtrado de los paquetes por parte del Router serán menos compleja dado a que él sólo debe atender las solicitudes del Gateway.

Así mismo tiene la desventaja de ser intrusivos y no transparentes para el usuario ya que generalmente este debe instalar algún tipo de aplicación especializada para lograr la comunicación. Se suma a esto que generalmente es más lentos porque deben revisar todo el tráfico de la red.

5.15. Protección

"Esto es lo que llamamos Criptograma, en el cual el sentido está oculto bajo letras embarulladas a propósito y que, convenientemente dispuestas, formarían una frase inteligible --dijo el profesor--

Viaje al centro de la tierra. Julio Verne



Una vez conocidas las vulnerabilidades y ataques a las que está expuesto un sistema es necesario conocer los recursos disponibles para protegerlo. Mientras algunas técnicas son evidentes (seguridad física por ejemplo) otras pautas no lo son tanto e incluso algunas pueden ocasionar una sensación de falsa seguridad.

Muchas de las vulnerabilidades estudiadas son el resultado de implementación incorrecta de tecnologías, otras son consecuencias de la falta de planeamiento de las mismas pero, como ya se ha mencionado, la mayoría de los agujeros de seguridad son ocasionados por los usuarios de dichos sistemas y es responsabilidad del administrador detectarlos y encontrar la mejor manera de cerrarlos.

En el presente capítulo, después de lo expuesto y vistas la gran cantidad de herramientas con las que cuenta el intruso, es el turno de estudiar implementaciones en la búsqueda de mantener el sistema seguro.

Siendo reiterativo, ninguna de las técnicas expuestas a continuación representará el 100% de la seguridad deseado, aunque muchas parezcan la panacea, será la suma de algunas de ellas las que convertirán un sistema interconectado en confiable.

5.15.1. Vulnerar Para Proteger.

Los intrusos utilizan diversas técnicas para quebrar los sistemas de seguridad de una red. Básicamente buscan los puntos débiles del sistema para poder colarse en ella. El trabajo de los Administradores y Testers no difiere mucho de esto. En lo que sí se diferencia, y por completo, es en los objetivos: mientras que un intruso penetra en las redes para distintos fines (investigación, daño, robo, etc.) un administrador lo hace para poder mejorar los sistemas de seguridad. En palabras de Julio C. Ardita (1): "(...) los intrusos cuentan con grandes herramientas como los Scanners, los cracking de passwords, software de análisis de vulnerabilidades y los exploits(...) un



administrador cuenta con todas ellas empleadas para bien, los Logs, los sistemas de detección de intrusos y los sistemas de rastreo de intrusiones".

Al conjunto de técnicas que se utilizan para evaluar y probar la seguridad de una red se lo conoce como Penetration Testing, uno de los recursos más poderosos con los que se cuenta hoy para generar barreras cada vez más eficaces.

Un test está totalmente relacionado con el tipo de información que se maneja en cada organización. Por consiguiente, según la información que deba ser protegida, se determinan la estructura y las herramientas de seguridad; no a la inversa

El software y el Hardware utilizados son una parte importante, pero no la única. A ella se agrega lo que se denomina "políticas de seguridad internas" que cada organización (y usuario) debe generar e implementar.

5.15.2. Firewalls

Quizás uno de los elementos más publicitados a la hora de establecer seguridad, sean estos elementos. Aunque deben ser uno de los sistemas a los que más se debe prestar atención, distan mucho de ser la solución final a los problemas de seguridad.

De hecho, los Firewalls no tienen nada que hacer contra técnicas como la Ingeniería Social y el ataque de Insiders. Un **Firewall** es un sistema (o conjunto de ellos) ubicado entre dos redes y que ejerce la una política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es (por ejemplo Internet).

5.15.3. Access Control Lists (ACL)

Las Listas de Control de Accesos proveen de un nivel de seguridad adicional a los clásicos provistos por los Sistemas Operativos. Estas listas permiten definir permisos a usuarios y grupos concretos. Por ejemplo pueden definirse sobre un Proxy una lista de todos los



usuarios (o grupos de ellos) a quien se le permite el acceso a Internet, FTP, etc. También podrán definirse otras características como limitaciones de anchos de banda y horarios.

5.15.4. Wrappers

Un Wrapper es un programa que controla el acceso a un segundo programa. El Wrapper literalmente cubre la identidad de este segundo programa, obteniendo con esto un más alto nivel de seguridad. Los Wrappers son usados dentro de la seguridad en sistemas UNIXs. Estos programas nacieron por la necesidad de modificar el comportamiento del sistema operativo sin tener que modificar su funcionamiento.

Los Wrappers son ampliamente utilizados, y han llegado a formar parte de herramientas de seguridad por las siguientes razones:

- Debido a que la seguridad lógica está concentrada en un solo programa, los Wrappers son fáciles y simples de validar.
- Debido a que el programa protegido se mantiene como una entidad separada, éste puede ser actualizado sin necesidad de cambiar el Wrapper.
- Debido a que los Wrappers llaman al programa protegido mediante llamadas estándar al sistema, se puede usar un solo Wrapper para controlar el acceso a diversos programas que se necesiten proteger.
- Permite un control de accesos exhaustivo de los servicios de comunicaciones, además de buena capacidad de Logs y auditorías de peticiones a dichos servicios, ya sean autorizados o no.

El paquete Wrapper más ampliamente utilizado es el TCP-Wrappers, el cual es un conjunto de utilidades de distribución libre, escrito por Wietse Venema (co-autor de SATAN, con Dan Farmer, y considerado el padre de los sistemas Firewalls) en 1990.

Consiste en un programa que es ejecutado cuando llega una petición a un puerto específico. Este, una vez comprobada la dirección de origen de la



petición, la verifica contra las reglas almacenadas, y en función de ellas, decide o no dar paso al servicio. Adicionalmente, registra estas actividades del sistema, su petición y su resolución.

Algunas configuraciones avanzadas de este paquete, permiten también ejecutar comandos en el propio sistema operativo, en función de la resolución de la petición. Por ejemplo, es posible que interese detectar una posible máquina atacante, en el caso de un intento de conexión, para tener más datos a la hora de una posible investigación. Este tipo de comportamiento raya en la estrategia paranoica, ya vista cuando se definió la política de seguridad del firewall.

Con lo mencionado hasta aquí, puede pensarse que los Wrappers son Firewall ya que muchos de los servicios brindados son los mismos o causan los mismos efectos: usando Wrappers, se puede controlar el acceso a cada máquina y los servicios accedidos. Así, estos controles son el complemento perfecto de un Firewall y la instalación de uno no está supeditada a la del otro.

5.15.5. Detección de Intrusos en Tiempo Real

La seguridad se tiene que tratar en conjunto. Este viejo criterio es el que recuerda que los sistemas de protección hasta aquí abordados, si bien son eficaces, distan mucho de ser la protección ideal.

Así, debe estar fuera de toda discusión la conveniencia de añadir elementos que controlen lo que ocurre dentro de la red (detrás de los Firewalls).

Como se ha visto, la integridad de un sistema se puede corromper de varias formas y la forma de evitar esto es con la instalación de sistemas de Detección de Intrusos en Tiempo Real, quienes:

Inspeccionan el tráfico de la red buscando posibles ataques.

Controlan el registro de los servidores para detectar acciones sospechosas (tanto de intrusos como de usuarios autorizados).

Mantienen una base de datos con el estado exacto de cada uno de los archivos (Integrity Check) del sistema para detectar la modificación de los mismos.



Controlan el ingreso de cada nuevo archivo al sistema para detectar Caballos de Troya o semejantes.

Controlan el núcleo del Sistema Operativo para detectar posibles infiltraciones en él, con el fin de controlar los recursos y acciones del mismo.

Avisan al administrador de cualquiera de las acciones mencionadas. Cada una de estas herramientas permiten mantener alejados a la gran mayoría de los intrusos normales. Algunos pocos, con suficientes conocimientos, experiencia y paciencia serán capaces de utilizar métodos sofisticados (u originales) como para voltear el perímetro de seguridad (interna + externa) y serán estos los casos que deban estudiarse para integrar a la política de seguridad existente mayor conocimiento y con él mayor seguridad.

5.15.6. Call Back

Este procedimiento es utilizado para verificar la autenticidad de una llamada vía modem. El usuario llama, se autentifica contra el sistema, se desconecta y luego el servidor se conecta al número que en teoría pertenece al usuario.

La ventaja reside en que si un intruso desea hacerse pasar por el usuario, la llamada se devolverá al usuario legal y no al del intruso, siendo este desconectado. Como precaución adicional, el usuario deberá verificar que la llamada-retorno proceda del número a donde llamó previamente.

5.15.7. Sistemas Anti-Sniffers

Esta técnica consiste en detectar Sniffers en el sistema. Generalmente estos programas se basan en verificar el estado de la placa de red, para detectar el modo en el cual está actuando (recordar que un Sniffer la coloca en Modo Promiscuo), y el tráfico de datos en ella.



5.15.8. Gestion de Claves "Seguras"

Si se utiliza una clave de 8 caracteres de longitud, con los 96 caracteres posibles, puede tardarse 2.288 años en descifrarla (analizando 100.000 palabras por segundo). Esto se obtiene a partir de las 96⁸ (7.213.895.789.838.340) claves posibles de generar con esos caracteres.

Partiendo de la premisa en que no se disponen de esa cantidad de años para analizarlas por fuerza bruta, se deberá comenzar a probar con las claves más posibles, comúnmente llamadas Claves Débiles.

5.15.9. Seguridad en Protocolos y Servicios

Se ha visto en capítulos anteriores la variedad de protocolos de comunicaciones existentes, sus objetivos y su funcionamiento. Como puede preverse todos estos protocolos tienen su debilidad ya sea en su implementación o en su uso. A continuación se describen los problemas de seguridad más comunes y sus formas de prevención.

Nuevamente no se verán los detalles sobre el funcionamiento de cada uno de ellos, simplemente se ofrecerán las potenciales puertas de entrada como fuentes de ataques que ni siquiera tienen por qué proporcionar acceso a la máquina (como las DoS por ejemplo).

5.15.10. Criptología.

La palabra **Criptografía** proviene etimológicamente del griego *Kruptoz* (Kriptos-Oculto) y *Grajein* (Grafo-Escritura) y significa "arte de escribir con clave secreta o de un modo enigmático" (2).

Aportando luz a la definición cabe aclarar que la Criptografía hace años que dejó de ser un arte para convertirse en una técnica (o



conjunto de ellas) que tratan sobre la protección (ocultamiento ante personas no autorizadas) de la información. Entre las disciplinas que engloba cabe destacar la Teoría de la Información, la Matemática Discreta, la Teoría de los Grandes Números y la Complejidad Algorítmica.

Es decir que la **Criptografía** es la ciencia que consiste en transformar un mensaje inteligible en otro que no lo es (mediante claves que sólo el emisor y el destinatario conocen), para después devolverlo a su forma original, sin que nadie que vea el mensaje cifrado sea capaz de entenderlo.

5.15.11. Inversión.

Los costos de las diferentes herramientas de protección se están haciendo accesibles, en general, incluso para las organizaciones más pequeñas. Esto hace que la implementación de mecanismos de seguridad se dé prácticamente en todos los niveles: empresas grandes, medianas, chicas y usuarios finales. Todos pueden acceder a las herramientas que necesitan y los costos (la inversión que cada uno debe realizar) van de acuerdo con el tamaño y potencialidades de la herramienta.

Pero no es sólo una cuestión de costos, los constantes cambios de la tecnología hacen que para mantener un nivel parejo de seguridad, se deba actualizar permanentemente las herramientas con las que se cuenta. Como los intrusos mejoran sus armas y metodologías de penetración de forma incesante, el recambio y la revisión constantes en los mecanismos de seguridad se convierten en imprescindibles. Y éste es un verdadero punto crítico.

Según Testers, "esto es tan importante como el tipo de elementos que se usen". Sin duda, éstos deben ser las que mejor se adapten al tipo de organización. Pero tan importante como eso es el hecho de conocer exactamente cómo funcionan y qué se puede hacer con



ellos. "Es prioritario saber los riesgos que una nueva tecnología trae aparejados".

5.15.12. Vulnerar para Proteger

5.16. Administración de la Seguridad

Es posible dividir las tareas de administración de seguridad en tres grandes grupos:

- **Autenticación:** se refiere a establecer las entidades que pueden tener acceso al universo de recursos de cómputo que cierto medio ambiente puede ofrecer.
- **Autorización:** es el hecho de que las entidades autorizadas a tener acceso a los recursos de cómputo, tengan acceso únicamente a las áreas de trabajo sobre las cuales ellas deben tener dominio.
- **Auditoría:** se refiere a la continua vigilancia de los servicios en producción. Entra dentro de este grupo el mantener estadísticas de acceso, estadísticas de uso y políticas de acceso físico a los recursos.

Por regla general, las políticas son el primer paso que dispone a una organización para entrar en un ambiente de seguridad, puesto que reflejan su "voluntad de hacer algo" que permita detener un posible ataque antes de que éste suceda (pro actividad). A continuación se citan algunos de los métodos de protección más comúnmente empleados.

1. **Sistemas de detección de intrusos:** son sistemas que permiten analizar las bitácoras de los sistemas en busca de patrones de comportamiento o eventos que puedan considerarse sospechosos, sobre la base de la información con la que han sido previamente alimentados. Pueden considerarse como monitores.
2. **Sistemas orientados a conexión de red:** monitorizan las conexiones que se intentan establecer en una red o equipo en particular, siendo capaces de efectuar una acción sobre la base



de métricas como: origen y destino de la conexión, servicio solicitado, permisos, etc. Las acciones que pueden emprender suelen ir desde el rechazo de la conexión hasta alerta al administrador. En esta categoría están los cortafuegos (Firewalls) y los Wrappers.

3. **Sistemas de análisis de vulnerabilidades:** analizan sistemas en busca de vulnerabilidades conocidas anticipadamente. La "desventaja" de estos sistemas es que pueden ser utilizados tanto por personas autorizadas como por personas que buscan acceso no autorizado al sistema.
4. **Sistemas de protección a la integridad de información:** sistemas que mediante criptografía o sumas de verificación tratan de asegurar que no ha habido alteraciones indeseadas en la información que se intenta proteger. Algunos ejemplos son los programas que implementan algoritmos como Message Digest (MD5) o Secure Hash Algorithm (SHA), o bien sistemas que utilizan varios de ellos como PGP, Tripwire y DozeCrypt.
5. **Sistemas de protección a la privacidad de la información:** herramientas que utilizan criptografía para asegurar que la información sólo sea visible para quien tiene autorización. Su aplicación se realiza principalmente en las comunicaciones entre dos entidades. Dentro de este tipo de herramientas se pueden citar a Pretty Good Privacy (PGP), Secure Sockets Layer (SSL) y los Certificados Digitales.

Resumiendo, un modelo de seguridad debe estar formado por múltiples componentes o capas que pueden ser incorporadas de manera progresiva al modelo global de seguridad en la organización, logrando así el método más efectivo para disuadir el uso no autorizado de sistemas y servicios de red.

Podemos considerar que estas capas son:

1. Política de seguridad de la organización.



2. Auditoría.
3. Sistemas de seguridad a nivel de Router-Firewall.
4. Sistemas de detección de intrusos.
5. Plan de respuesta a incidentes.
6. Penetration Test.

5.17. Penetration Test, Ethical Hacking o Prueba de Vulnerabilidad.

"El Penetration Test es un conjunto de metodologías y técnicas, para realizar una evaluación integral de las debilidades de los sistemas informáticos. Consiste en un modelo que reproduce intentos de acceso, a cualquier entorno informático, de un intruso potencial desde los diferentes puntos de entrada que existan, tanto internos como remotos." (1)

El objetivo general del Penetration Test es acceder a los equipos informáticos de la organización tratada e intentar obtener los privilegios del administrador del sistema, logrando así realizar cualquier tarea sobre dichos equipos. También se podrá definir otros objetivos secundarios que permitan realizar pruebas puntuales sobre algunos ámbitos particulares de la empresa.

El Penetration Test se compone de dos grandes fases de testeo:

1. **Penetration Test Externo:** el objetivo es acceder en forma remota a los equipos de la organización y posicionarse como administrador del sistema. Se realizan desde fuera del Firewall y consisten en penetrar la Zona Desmilitarizada para luego acceder a la red interna. Se compone de un elevado número de pruebas, entre las que se puede nombrar:
 - Pruebas de usuarios y la "fuerza" de sus passwords.
 - Captura de tráfico.
 - Detección de conexiones externas y sus rangos de direcciones.
 - Detección de protocolos utilizados.
 - canning de puertos TCP, UDP e ICMP.



- Intentos de acceso vía accesos remotos, módems, Internet, etc.
- Análisis de la seguridad de las conexiones con proveedores, trabajadores remotos o entidades externas a la organización.
- Pruebas de vulnerabilidades existentes y conocidas en el momento de realización del Test.
- Prueba de ataques de Denegación de Servicio.

2. Penetration Test Interno: este tipo de testeo trata de demostrar cual es el nivel de seguridad interno. Se deberá establecer que puede hacer un Insider y hasta donde será capaz de penetrar en el sistema siendo un usuario con privilegios bajos. Este Test también se compone de numerosas pruebas:

- Análisis de protocolos internos y sus vulnerabilidades.
- Autenticación de usuarios.
- Verificación de permisos y recursos compartidos.
- Test de los servidores principales (WWW, DNS, FTP, SMTP, etc.).
- Test de vulnerabilidad sobre las aplicaciones propietarias.
- Nivel de detección de la intrusión de los sistemas.
- Análisis de la seguridad de las estaciones de trabajo.
- Seguridad de la red.
- Verificación de reglas de acceso.
- Ataques de Denegación de Servicio.

5.18. HoneyPots-HoneyNets

Estas "Trampas de Red" son sistemas que se activan con la finalidad específica de que los expertos en seguridad puedan observar en secreto la actividad de los Hackers/Crackers en su hábitat natural.



Actualmente un equipo de Honeynet Project (2) trabaja en el desarrollo de un documento sobre la investigación y resultados de su trampa, la cual fue penetrada a la semana de ser activada (sin publicidad).

"Consiste en activar un servidor y llenarlo de archivos tentadores, hacer que sea difícil, pero no imposible penetrarlo y sentarse a esperar que aparezcan los intrusos. Los Honeynets dan a los crackers un gran espacio para recorrer. Presentan obstáculos que poseen el nivel de complejidad suficiente para atraerlos, pero sin irse al extremo para no desalentarlos (...). Ellos juegan con los archivos y conversan animadamente entre ellos sobre todos los 'fascinantes programas' que encuentran, mientras el personal de seguridad observa con deleite cada movimiento que hacen", dijo Dan Adams. "Francamente, siento una combinación de sentimientos con respecto a espiar a la gente, aunque no sean buenas personas" (3).

Esta última frase se está presentando a menudo en el tema de la investigación (y vigilancia) electrónica. Este es el caso del ex-director del proyecto Honeynet J. D. Glaser, quien renunció a su puesto después de aclarar que está convencido "que la vigilancia electrónica no es correcta, aunque se utilice en aras de la investigación (...). Ampliar un Honeynet es parecido a entrapar los derechos de otros, aunque sean los derechos de un delincuente."

Con respecto a algunos de los resultados obtenidos por el grupo de investigación puede observarse el siguiente ejemplo:

A un intruso le tomo menos de un minuto irrumpir en la computadora de su universidad a través de Internet, estuvo dentro menos de media hora y a los investigadores le tomo 34 horas descubrir todo lo que hizo.

Se estima que esas 34 horas de limpieza pueden costar U\$S 2.000 a una organización y U\$S 22.000 si se debiera tratar con un consultor especializado



5.19. Detección de Intrusos en Tiempo Real

5.19.1. Intrusión Detection Systems (IDS)

Un sistema de detección de intrusos es un componente más dentro del modelo de seguridad de una organización. Consiste en detectar actividades inapropiadas, incorrectas o anómalas desde el exterior-interior de un sistema informático.

Los sistemas de detección de intrusos pueden clasificarse, según su función y comportamiento en:

- **Host-Based IDS:** operan en un host para detectar actividad maliciosa en el mismo.
- **Network-Based IDS:** operan sobre los flujos de información intercambiados en una red.
- **Knowledge-Based IDS:** sistemas basados en Conocimiento.
- **Behavior-Based IDS:** sistemas basados en Comportamiento.

Se asume que una intrusión puede ser detectada observando una desviación respecto del comportamiento normal o esperado de un usuario en el sistema.

La idea central de este tipo de detección es el hecho de que la actividad intrusiva es un conjunto de actividades anómalas. Si alguien consigue entrar de forma ilegal al sistema, no actuará como un usuario comprometido; su comportamiento se alejará del de un usuario normal.

Sin embargo en la mayoría de las ocasiones una actividad intrusiva resulta del agregado de otras actividades individuales que por sí solas no constituyen un comportamiento intrusivo de ningún tipo. Así las intrusiones pueden clasificarse en:

- **Intrusivas pero no anómalas:** denominados Falsos Negativos (el sistema erróneamente indica ausencia de intrusión). En este caso la actividad es intrusiva pero como no es anómala no es detectada. No son deseables, porque dan una falsa sensación de seguridad del sistema.



- **No intrusivas pero anómalas:** denominados Falsos Positivos (el sistema erróneamente indica la existencia de intrusión). En este caso la actividad es no intrusiva, pero como es anómala el sistema "decide" que es intrusiva. Deben intentar minimizarse, ya que en caso contrario se ignorarán los avisos del sistema, incluso cuando sean acertados.
- **No intrusiva ni anómala:** son Negativos Verdaderos, la actividad es no intrusiva y se indica como tal.
- **Intrusiva y anómala:** se denominan Positivos Verdaderos, la actividad es intrusiva y es detectada.

Los detectores de intrusiones anómalas requieren mucho gasto computacional, ya que se siguen normalmente varias métricas para determinar cuánto se aleja el usuario de lo que se considera comportamiento normal.

5.19.2. Características de IDS

Cualquier sistema de detección de intrusos debería, sea cual sea el mecanismo en que esté basado, **debería** contar con las siguientes características:

Debe funcionar continuamente sin supervisión humana. El sistema debe ser lo suficientemente fiable para poder ser ejecutado en background dentro del equipo que está siendo observado. Sin embargo, no debe ser una "caja negra" (debe ser examinable desde el exterior).

Debe ser tolerante a fallos en el sentido de que debe ser capaz de sobrevivir a una caída del sistema.

En relación con el punto anterior, debe ser resistente a perturbaciones. El sistema puede monitorizarse a sí mismo para asegurarse de que no ha sido perturbado.

Debe imponer mínima sobrecarga sobre el sistema. Un sistema que ralentiza la máquina, simplemente no será utilizado.

Debe observar desviaciones sobre el comportamiento estándar.



Debe ser fácilmente adaptable al sistema ya instalado. Cada sistema tiene un patrón de funcionamiento diferente y el mecanismo de defensa debe adaptarse de manera sencilla a esos patrones.

Debe hacer frente a los cambios de comportamiento del sistema según se añaden nuevas aplicaciones al mismo.

Debe ser difícil de "engañar".

5.19.3. Fortalezas de IDS

Suministra información muy interesante sobre el tráfico malicioso de la red.

Poder de reacción para prevenir el daño.

Es una herramienta útil como arma de seguridad de la red.

Ayuda a identificar de dónde provienen los ataques que se sufren.

Recoge evidencias que pueden ser usadas para identificar intrusos.

Es una "cámara" de seguridad y una "alarma" contra ladrones.

Funciona como "disuasor de intrusos".

Alerta al personal de seguridad de que alguien está tratando de entrar.

Protege contra la invasión de la red.

Suministra cierta tranquilidad.

Es una parte de la infraestructura para la estrategia global de defensa.

La posibilidad de detectar intrusiones desconocidas e imprevistas.

Pueden incluso contribuir (parcialmente) al descubrimiento automático de esos nuevos ataques.

Son menos dependientes de los mecanismos específicos de cada sistema operativo.

Pueden ayudar a detectar ataques del tipo "abuso de privilegios" que no implica realmente ninguna vulnerabilidad de seguridad. En pocas palabras, se trata de una aproximación a la paranoia: "todo aquello que no se ha visto previamente es peligroso".

Menor costo de implementación y mantenimiento al ubicarse en puntos estratégicos de la red.

Dificulta el trabajo del intruso de eliminar sus huellas.



5.19.4. Debilidades de IDS

No existe un parche para la mayoría de bugs de seguridad.

Se producen falsas alarmas.

Se producen fallos en las alarmas.

No es sustituto para un buen Firewall, una auditoría de seguridad regular y una fuerte y estricta política de seguridad.

5.19.5. Inconvenientes de IDS

La alta tasa de falsas alarmas dado que no es posible cubrir todo el ámbito del comportamiento de un sistema de información durante la fase de aprendizaje.

El comportamiento puede cambiar con el tiempo, haciendo necesario un re-entrenamiento periódico del perfil, lo que da lugar a la no disponibilidad del sistema o la generación de falsas alarmas adicionales.

El sistema puede sufrir ataques durante la fase de aprendizaje, con lo que el perfil de comportamiento contendrá un comportamiento intrusivo el cual no será considerado anómalo.

5.19.6. Gestión de Claves Seguras

Como puede verse en la siguiente tabla (actualización 2009), si se utiliza una clave de 8 caracteres de longitud, con los 96 caracteres posibles, puede tardarse 2.288 años en descifrarla (analizando 100.000 palabras por segundo). Esto se obtiene a partir de las 96^8 (7.213.895.789.838.340) claves posibles de generar con esos caracteres.



Cantidad de Caracteres	26 Letras Minúsculas	36 Letras y Dígitos	52 Mayúsculas y minúsculas	96 Todos los Caracteres
6	51 minutos	6 horas	2,3 días	3 meses
7	22,3 horas	9 días	4 meses	24 años
8	24 días	10,5 meses	17 años	2.288 años
9	21 meses	32,6 años	890 años	219.601 años
10	45 años	1.160 años	45.840 años	21.081.705 años

Partiendo de la premisa en que no se disponen de esa cantidad de años para analizarlas por fuerza bruta, se deberá comenzar a probar con las claves más posibles, comúnmente llamadas Claves Débiles. Según demuestra el análisis de +NetBuL (1) realizado sobre 2.134 cuentas y probando 227.000 palabras por segundo:

- Con un diccionario 2.030 palabras (el original de John de Ripper 1.04), se obtuvieron 36 cuentas en solo 19 segundos (1,77%).
- Con un diccionario de 250.000 palabras, se obtuvieron 64 cuentas en 36:18 minutos (3,15%).

Otro estudio (2) muestra el resultado obtenido al aplicar un ataque, mediante un diccionario de 62.727 palabras, a 13.794 cuentas:

- En un año se obtuvieron 3.340 contraseñas (24,22%).
- En la primera semana se descubrieron 3.000 claves (21,74%).
- En los primeros 15 minutos se descubrieron 368 palabras claves (2,66%).

Según los grandes números vistos, sería válido afirmar que: es imposible encontrar ¡36 cuentas en 19 segundos!. También debe observarse, en el segundo estudio, que el porcentaje de hallazgos casi no varía entre un año y una semana.



Tal vez, ¿esto sucedió porque existían claves nulas; que corresponde al nombre del usuario; a secuencias alfabéticas tipo "abcd"; a secuencias numéricas tipo "1234"; a secuencias observadas en el teclado tipo "qwer"; a palabras que existen en un diccionario del lenguaje del usuario?. Sí, estas claves (las más débiles) son las primeras en ser analizadas y los tiempos obtenidos confirman la hipótesis.

5.20. Normas de Elección de Claves

Se debe tener en cuenta los siguientes consejos:

1. No utilizar contraseñas que sean palabras (aunque sean extranjeras), o nombres (el del usuario, personajes de ficción, miembros de la familia, mascotas, marcas, ciudades, lugares, u otro relacionado).
2. No usar contraseñas completamente numéricas con algún significado (teléfono, D.N.I., fecha de nacimiento, patente del automóvil, etc.).
3. Elegir una contraseña que mezcle caracteres alfabéticos (mayúsculas y minúsculas) y numéricos.
4. Deben ser largas, de 8 caracteres o más.
5. Tener contraseñas diferentes en máquinas diferentes. Es posible usar una contraseña base y ciertas variaciones lógicas de la misma para distintas máquinas.
6. Deben ser fáciles de recordar para no verse obligado a escribirlas. Algunos ejemplos son:
 - Combinar palabras cortas con algún número o carácter de puntuación: *soy2_yo3*
 - Usar un acrónimo de alguna frase fácil de recordar: *Ario Revuelto Ganancia de Pescadores -> ArRGdP*
 - Añadir un número al acrónimo para mayor seguridad: *A9r7R5G3d1P*



- Mejor incluso si la frase no es conocida: Hasta Ahora no he Olvidado mi Contraseña -> *aHoello*
- Elegir una palabra sin sentido, aunque pronunciable: *taChunda72*, *AtajulH*, *Wen2Mar*
- Realizar reemplazos de letras por signos o números: En Seguridad Más Vale Prevenir que Curar -> *35MVPq<*

5.20.1. Normas para Proteger una Clave

La protección de la contraseña recae tanto sobre el administrador del sistema como sobre el usuario. Al comprometer una cuenta se puede estar comprometiendo todo el sistema.

La siguiente frase difundida en UseNet resume algunas de las reglas básicas de uso de la contraseña: "Un password debe ser como un cepillo de dientes. Úsalo cada día; cámbialo regularmente; y NO lo compartas con tus amigos".

Algunos consejos a seguir:

1. No permitir ninguna cuenta sin contraseña. Si se es administrador del sistema, repasar este hecho periódicamente.
2. No mantener las contraseñas por defecto del sistema. Por ejemplo, cambiar las cuentas de Root, System, Test, Demo, Guest, etc.
3. Nunca compartir con nadie la contraseña. Si se hace, cambiarla inmediatamente.
4. No escribir la contraseña en ningún sitio. Si se escribe, no debe identificarse como tal y no debe identificarse al propietario en el mismo lugar.
5. No teclear la contraseña si hay alguien mirando. Es una norma tácita de buen usuario no mirar el teclado mientras alguien teclea su contraseña.
6. No enviar la contraseña por correo electrónico ni mencionarla en una conversación. Si se debe mencionar no hacerlo explícitamente diciendo: "mi clave es...".



7. No mantener una contraseña indefinidamente. Cambiarla regularmente. Disponer de una lista de contraseñas que puedan usarse cíclicamente (por lo menos 5).

Muchos sistemas incorporan ya algunas medidas de gestión y protección de las contraseñas. Entre ellas podemos citar las siguientes:

1. Número de intentos limitado. Tras un número de intentos fallidos, pueden tomarse distintas medidas:
 - Obligar a reescribir el nombre de usuario (lo más común).
 - Bloquear el acceso durante un tiempo.
 - Enviar un mensaje al administrador y/o mantener un registro especial.
2. Longitud mínima. Las contraseñas deben tener un número mínimo de caracteres (se recomienda 7 u 8 como mínimo).
3. Restricciones de formato. Las contraseñas deben combinar un mínimo de letras y números, no pueden contener el nombre del usuario ni ser un blanco.
4. Envejecimiento y expiración de contraseñas. Cada cierto tiempo se fuerza a cambiar la contraseña. Se obliga a no repetir cierta cantidad de la anterior. Se mantiene un periodo forzoso entre cambios, para evitar que se vuelva a cambiar inmediatamente y se repita la anterior.
5. Ataque preventivo. Muchos administradores utilizan crackeadores para intentar atacar las contraseñas de su propio sistema en busca de debilidades.

5.20.2. Contraseñas de un Sólo Uso

Las contraseñas de un solo uso (One-Time Passwords) son uno de los mecanismos de autenticación más seguros, debido a que su descubrimiento tan solo permite acceder al sistema una vez. Además, en muchas ocasiones se suelen utilizar dispositivos hardware para su generación, lo que las hace mucho más difíciles de descubrir.



Ejemplos de este tipo de contraseñas serían las basadas en funciones unidireccionales (sencillas de evaluar en un sentido pero imposible o muy costoso de evaluar en sentido contrario) y en listas de contraseñas.

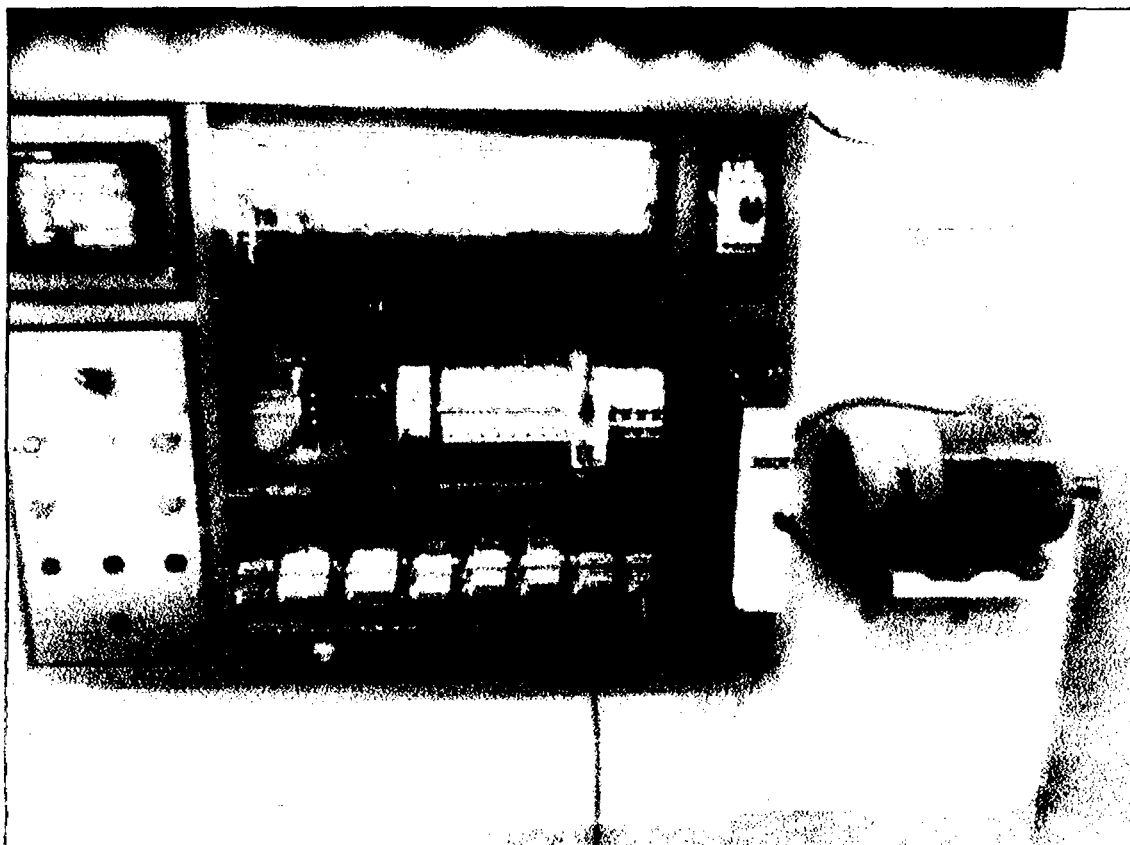
Se distinguen tres tipos de contraseñas de un solo uso:

1. Las que requieren algún dispositivo hardware para su generación, tales como calculadoras especiales o tarjetas inteligentes (Token Cards).
2. Las que requieren algún tipo de software de cifrado especial.
3. Las que se basan en una lista de contraseñas sobre papel.

La tarjeta genera periódicamente valores mediante a una función secreta y unidireccional, basada en el tiempo y en el número de identificación de la misma.

El usuario combina el número generado por la tarjeta con su palabra de paso para obtener el password de entrada, lo que le protege en caso de robo o pérdida.

6. Prueba de Captura de Datos, Contraseñas y Login.



6.1. Wireshark.

Wireshark es uno de esos programas que muchos administradores de red, auditores y una excelente forma de testear una la red interna, en este caso vamos a probar la red industrial demostrando, descubrir el contenido de correos electrónicos o incluso contraseñas de cuentas de usuario en páginas webs o servicios de mensajería instantánea y lo más importante demostrar que es necesaria una arquitectura de seguridad.



Time	Source	Destination	Protocol	Info
0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
1.0.0.0	1.0.0.0	1.0.0.0	1.0.0.0	1.0.0.0
2.0.0.0	2.0.0.0	2.0.0.0	2.0.0.0	2.0.0.0
3.0.0.0	3.0.0.0	3.0.0.0	3.0.0.0	3.0.0.0
4.0.0.0	4.0.0.0	4.0.0.0	4.0.0.0	4.0.0.0
5.0.0.0	5.0.0.0	5.0.0.0	5.0.0.0	5.0.0.0
6.0.0.0	6.0.0.0	6.0.0.0	6.0.0.0	6.0.0.0
7.0.0.0	7.0.0.0	7.0.0.0	7.0.0.0	7.0.0.0
8.0.0.0	8.0.0.0	8.0.0.0	8.0.0.0	8.0.0.0
9.0.0.0	9.0.0.0	9.0.0.0	9.0.0.0	9.0.0.0
10.0.0.0	10.0.0.0	10.0.0.0	10.0.0.0	10.0.0.0
11.0.0.0	11.0.0.0	11.0.0.0	11.0.0.0	11.0.0.0
12.0.0.0	12.0.0.0	12.0.0.0	12.0.0.0	12.0.0.0
13.0.0.0	13.0.0.0	13.0.0.0	13.0.0.0	13.0.0.0
14.0.0.0	14.0.0.0	14.0.0.0	14.0.0.0	14.0.0.0
15.0.0.0	15.0.0.0	15.0.0.0	15.0.0.0	15.0.0.0
16.0.0.0	16.0.0.0	16.0.0.0	16.0.0.0	16.0.0.0
17.0.0.0	17.0.0.0	17.0.0.0	17.0.0.0	17.0.0.0
18.0.0.0	18.0.0.0	18.0.0.0	18.0.0.0	18.0.0.0
19.0.0.0	19.0.0.0	19.0.0.0	19.0.0.0	19.0.0.0
20.0.0.0	20.0.0.0	20.0.0.0	20.0.0.0	20.0.0.0
21.0.0.0	21.0.0.0	21.0.0.0	21.0.0.0	21.0.0.0
22.0.0.0	22.0.0.0	22.0.0.0	22.0.0.0	22.0.0.0
23.0.0.0	23.0.0.0	23.0.0.0	23.0.0.0	23.0.0.0
24.0.0.0	24.0.0.0	24.0.0.0	24.0.0.0	24.0.0.0
25.0.0.0	25.0.0.0	25.0.0.0	25.0.0.0	25.0.0.0
26.0.0.0	26.0.0.0	26.0.0.0	26.0.0.0	26.0.0.0
27.0.0.0	27.0.0.0	27.0.0.0	27.0.0.0	27.0.0.0
28.0.0.0	28.0.0.0	28.0.0.0	28.0.0.0	28.0.0.0
29.0.0.0	29.0.0.0	29.0.0.0	29.0.0.0	29.0.0.0
30.0.0.0	30.0.0.0	30.0.0.0	30.0.0.0	30.0.0.0
31.0.0.0	31.0.0.0	31.0.0.0	31.0.0.0	31.0.0.0
32.0.0.0	32.0.0.0	32.0.0.0	32.0.0.0	32.0.0.0
33.0.0.0	33.0.0.0	33.0.0.0	33.0.0.0	33.0.0.0
34.0.0.0	34.0.0.0	34.0.0.0	34.0.0.0	34.0.0.0
35.0.0.0	35.0.0.0	35.0.0.0	35.0.0.0	35.0.0.0
36.0.0.0	36.0.0.0	36.0.0.0	36.0.0.0	36.0.0.0
37.0.0.0	37.0.0.0	37.0.0.0	37.0.0.0	37.0.0.0
38.0.0.0	38.0.0.0	38.0.0.0	38.0.0.0	38.0.0.0
39.0.0.0	39.0.0.0	39.0.0.0	39.0.0.0	39.0.0.0
40.0.0.0	40.0.0.0	40.0.0.0	40.0.0.0	40.0.0.0
41.0.0.0	41.0.0.0	41.0.0.0	41.0.0.0	41.0.0.0
42.0.0.0	42.0.0.0	42.0.0.0	42.0.0.0	42.0.0.0
43.0.0.0	43.0.0.0	43.0.0.0	43.0.0.0	43.0.0.0
44.0.0.0	44.0.0.0	44.0.0.0	44.0.0.0	44.0.0.0
45.0.0.0	45.0.0.0	45.0.0.0	45.0.0.0	45.0.0.0
46.0.0.0	46.0.0.0	46.0.0.0	46.0.0.0	46.0.0.0
47.0.0.0	47.0.0.0	47.0.0.0	47.0.0.0	47.0.0.0
48.0.0.0	48.0.0.0	48.0.0.0	48.0.0.0	48.0.0.0
49.0.0.0	49.0.0.0	49.0.0.0	49.0.0.0	49.0.0.0
50.0.0.0	50.0.0.0	50.0.0.0	50.0.0.0	50.0.0.0
51.0.0.0	51.0.0.0	51.0.0.0	51.0.0.0	51.0.0.0
52.0.0.0	52.0.0.0	52.0.0.0	52.0.0.0	52.0.0.0
53.0.0.0	53.0.0.0	53.0.0.0	53.0.0.0	53.0.0.0
54.0.0.0	54.0.0.0	54.0.0.0	54.0.0.0	54.0.0.0
55.0.0.0	55.0.0.0	55.0.0.0	55.0.0.0	55.0.0.0
56.0.0.0	56.0.0.0	56.0.0.0	56.0.0.0	56.0.0.0
57.0.0.0	57.0.0.0	57.0.0.0	57.0.0.0	57.0.0.0
58.0.0.0	58.0.0.0	58.0.0.0	58.0.0.0	58.0.0.0
59.0.0.0	59.0.0.0	59.0.0.0	59.0.0.0	59.0.0.0
60.0.0.0	60.0.0.0	60.0.0.0	60.0.0.0	60.0.0.0
61.0.0.0	61.0.0.0	61.0.0.0	61.0.0.0	61.0.0.0
62.0.0.0	62.0.0.0	62.0.0.0	62.0.0.0	62.0.0.0
63.0.0.0	63.0.0.0	63.0.0.0	63.0.0.0	63.0.0.0
64.0.0.0	64.0.0.0	64.0.0.0	64.0.0.0	64.0.0.0
65.0.0.0	65.0.0.0	65.0.0.0	65.0.0.0	65.0.0.0
66.0.0.0	66.0.0.0	66.0.0.0	66.0.0.0	66.0.0.0
67.0.0.0	67.0.0.0	67.0.0.0	67.0.0.0	67.0.0.0
68.0.0.0	68.0.0.0	68.0.0.0	68.0.0.0	68.0.0.0
69.0.0.0	69.0.0.0	69.0.0.0	69.0.0.0	69.0.0.0
70.0.0.0	70.0.0.0	70.0.0.0	70.0.0.0	70.0.0.0
71.0.0.0	71.0.0.0	71.0.0.0	71.0.0.0	71.0.0.0
72.0.0.0	72.0.0.0	72.0.0.0	72.0.0.0	72.0.0.0
73.0.0.0	73.0.0.0	73.0.0.0	73.0.0.0	73.0.0.0
74.0.0.0	74.0.0.0	74.0.0.0	74.0.0.0	74.0.0.0
75.0.0.0	75.0.0.0	75.0.0.0	75.0.0.0	75.0.0.0
76.0.0.0	76.0.0.0	76.0.0.0	76.0.0.0	76.0.0.0
77.0.0.0	77.0.0.0	77.0.0.0	77.0.0.0	77.0.0.0
78.0.0.0	78.0.0.0	78.0.0.0	78.0.0.0	78.0.0.0
79.0.0.0	79.0.0.0	79.0.0.0	79.0.0.0	79.0.0.0
80.0.0.0	80.0.0.0	80.0.0.0	80.0.0.0	80.0.0.0
81.0.0.0	81.0.0.0	81.0.0.0	81.0.0.0	81.0.0.0
82.0.0.0	82.0.0.0	82.0.0.0	82.0.0.0	82.0.0.0
83.0.0.0	83.0.0.0	83.0.0.0	83.0.0.0	83.0.0.0
84.0.0.0	84.0.0.0	84.0.0.0	84.0.0.0	84.0.0.0
85.0.0.0	85.0.0.0	85.0.0.0	85.0.0.0	85.0.0.0
86.0.0.0	86.0.0.0	86.0.0.0	86.0.0.0	86.0.0.0
87.0.0.0	87.0.0.0	87.0.0.0	87.0.0.0	87.0.0.0
88.0.0.0	88.0.0.0	88.0.0.0	88.0.0.0	88.0.0.0
89.0.0.0	89.0.0.0	89.0.0.0	89.0.0.0	89.0.0.0
90.0.0.0	90.0.0.0	90.0.0.0	90.0.0.0	90.0.0.0
91.0.0.0	91.0.0.0	91.0.0.0	91.0.0.0	91.0.0.0
92.0.0.0	92.0.0.0	92.0.0.0	92.0.0.0	92.0.0.0
93.0.0.0	93.0.0.0	93.0.0.0	93.0.0.0	93.0.0.0
94.0.0.0	94.0.0.0	94.0.0.0	94.0.0.0	94.0.0.0
95.0.0.0	95.0.0.0	95.0.0.0	95.0.0.0	95.0.0.0
96.0.0.0	96.0.0.0	96.0.0.0	96.0.0.0	96.0.0.0
97.0.0.0	97.0.0.0	97.0.0.0	97.0.0.0	97.0.0.0
98.0.0.0	98.0.0.0	98.0.0.0	98.0.0.0	98.0.0.0
99.0.0.0	99.0.0.0	99.0.0.0	99.0.0.0	99.0.0.0
100.0.0.0	100.0.0.0	100.0.0.0	100.0.0.0	100.0.0.0

6.2. Configuración de filtros.

Para eso usaríamos uno de estos dos filtros:

`ip.addr == 10.22.21.226`

También podríamos indicar si la información entra:

`ip.src == 10.22.21.226`

O si sale:

`ip.dst == 10.22.21.226`

Por último para filtrar por dirección mal sería algo así:

`eth.src == 00:1d:60:6b:ec:83`



Ahora que sabemos aplicar ese filtro podemos conjuntarlo con otro que nos muestre solo el tráfico http o las acciones GET y POST en este protocolo, es decir:

```
http.method.request == "GET" | http.method.request == "POST"
```

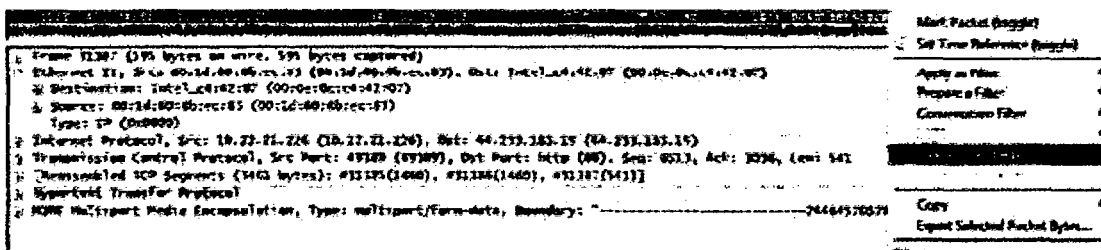
El primer filtro nos indicaría la información que la dirección IP recibe en el tráfico HTTP, y el segundo filtro nos serviría para ver qué información inyecta esa dirección IP en el tráfico HTTP.

De modo que ambos filtros se podían combinar del siguiente modo:

```
ip.addr == 10.22.21.226 and http.request.method == "POST"
```

También podríamos hacer excepciones. Por ejemplo, si ponemos un filtro dentro de un signo de exclamación y unos paréntesis eso omitiría los resultados obtenidos de ese filtro en la salida del Wireshark. Por ejemplo ! (http.request.method == "GET") omitiría todos los resultados del tráfico correspondientes. También podríamos omitir determinadas direcciones IP o MAC.

6.3. Configuración de filtros.



Analizando el tráfico TCP podemos observar en la información del paquete. Hacemos clic con el botón derecho sobre él y escogemos **Follow TCP Stream**.



Nos empezará a filtrar los trazos TCP y nos saldrá una ventana como ésta:

```
Follow TCP Stream

Stream Content

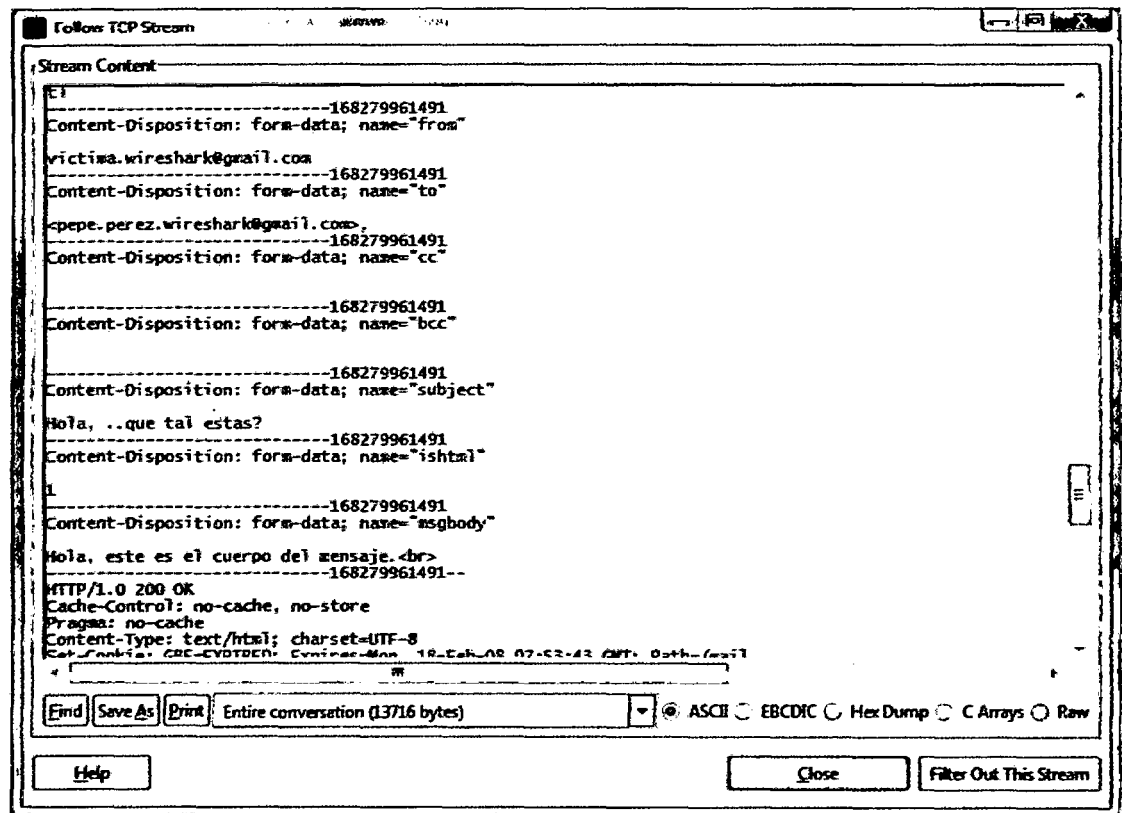
GET /mail/?ui=1&view=pagename=htmlcompose&ver=1chdyj2lqwixk HTTP/1.1
Host: mail.google.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.0; es-ES; rv:1.9b3) Gecko/2008020514 Firefox/3.0b3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: es-es,es;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*/*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://mail.google.com/mail/?ui=1&view=pagename=gp&ver=sh3fib53pgpk
Cookie: __utma=173272373.1266021523.1203336375.1203405715.2; __utmb=173272373;
__utmc=173272373; __utmx=173272373.00000882470492783055.1:0-0-0-0-0-0;
__utwz=173272373.1203405715.2.2.utmccn=(referral)|utmcsr=google.es|utmctt=/accounts/Logout2|
utmcd=referral;
S=gmail-OdS8U58_QATBSZWZUuOfw:gmail_yj=b_5MeTSZQEhMhR2oCGSw:gmproxy-nv05w8M0IeH:gmproxy_yj=oiQGL7SUNA
GC-DQAAAHYAAAC-IBKjW1ZAU8a_YsYcR3zcLRx4YAS5iitux7SH17YesCoipQ-xITGs-S6ruMdv80k9jahg00IejWDLRZP49cu3-
QaiKETx&FmLTn3r3R5KCKdGhZ8xhN7Gq9j-LgmdY7fzFboueI4FJedngZhko3yDE-_PUC3a0sFy0iWcg;
GMAIL_AT=xn3j350c97v0hrz0qvxfani2yxdvgam; gmailchat=victima.wireshark@gmail.com/561717; GBE=cv-p62Fcv-
pFh-1_f32Fcv-pfn-092Fa-1-rd62Fai-r-a-CV-862Fai-r-r1-CV-492Fai-t-a-CV-1;
PREF-ID=C572a94965b7cb58:TM=1203326088:LM=1203354900:GM=1:5=2bf_02cfmkIP6Ca6; rememberme=true;
MID=7-KEHnsphY44t-CX4ixZANuXCHdD0iHciisNo91qZq_yhISsNE_SKVQu2aRy1_eXqkukqM3Dk-
ZYajgoU51EPRA_edCv1CkiHuw8wD2tKQnsy3_-TnpXCX9-ZDlic3T3n; TZ=-60; GMAIL_RTT=329;
SID=DQAAAHQAAABPffdsOL3huvHj0Pemmuga20yacojGZsgqt3-N4Ca8IOJ4niSzzpnqj4eG1TMBR_HR-QaM4tcz_Rp-
sPg7xweaZL6Z_k7GLy8o1fv7g581-Bi2NscP8pLxP0nV7MbdFP2AvEnGmPmHttksit0pncw42UigZf8yLruACsZK7z1A;
GMAIL_HELP=hosted:0

HTTP/1.0 200 OK
Cache-Control: private
Content-Type: text/html; charset=UTF-8
Set-Cookie: GBE=EXPIRED; Expires=Mon, 18-Feb-08 07:30:30 GMT; Path=/mail
Set-Cookie: GMAIL_RTT=EXPIRED; Domain=.google.com; Expires=Mon, 18-Feb-08 07:30:30 GMT; Path=/mail
Etag: "11k62t5pxqs7n"
Last-Modified: Fri, 05 Sep 2003 02:11:15 GMT
Expires: Mon, 10 Mar 2008 07:30:30 GMT

[End] [Save As] [Print] Entire conversation (24134 bytes) [v] [ASCII] [EBCDIC] [Hex Dump] [C Arrays] [Raw]

[Help] [Close] [Filter Out This Stream]
```

A quí si bajamos más o menos a la mitad veremos lo siguiente (en color rojo):



Veremos cómo donde pone Content-Disposition: form-data; name="from" pone la dirección de login o el tráfico que esta pasando del que envía el correo, así como más abajo aparecen las direcciones de e-mail del o los destinatarios (Content-Disposition: form-data; name="to") el asunto del email (Content-Disposition: form-data; name="subject") y el cuerpo del mensaje (Content-Disposition: form-data; name="msgbody").

Ahora supongamos que esa persona se conecta al Messenger por eBuddy o algún medio similar que no de la protección suficiente. Veríamos lo siguiente:



No.	Time	Source	Destination	Protocol	Size	Info
100	00:00:00.000	192.168.1.1	192.168.1.1	HTTP	1024	GET / HTTP/1.1
101	00:00:00.000	192.168.1.1	192.168.1.1	HTTP	1024	GET / HTTP/1.1
102	00:00:00.000	192.168.1.1	192.168.1.1	HTTP	1024	GET / HTTP/1.1
103	00:00:00.000	192.168.1.1	192.168.1.1	HTTP	1024	GET / HTTP/1.1
104	00:00:00.000	192.168.1.1	192.168.1.1	HTTP	1024	GET / HTTP/1.1
105	00:00:00.000	192.168.1.1	192.168.1.1	HTTP	1024	GET / HTTP/1.1
106	00:00:00.000	192.168.1.1	192.168.1.1	HTTP	1024	GET / HTTP/1.1
107	00:00:00.000	192.168.1.1	192.168.1.1	HTTP	1024	GET / HTTP/1.1
108	00:00:00.000	192.168.1.1	192.168.1.1	HTTP	1024	GET / HTTP/1.1
109	00:00:00.000	192.168.1.1	192.168.1.1	HTTP	1024	GET / HTTP/1.1
110	00:00:00.000	192.168.1.1	192.168.1.1	HTTP	1024	GET / HTTP/1.1
111	00:00:00.000	192.168.1.1	192.168.1.1	HTTP	1024	GET / HTTP/1.1
112	00:00:00.000	192.168.1.1	192.168.1.1	HTTP	1024	GET / HTTP/1.1
113	00:00:00.000	192.168.1.1	192.168.1.1	HTTP	1024	GET / HTTP/1.1
114	00:00:00.000	192.168.1.1	192.168.1.1	HTTP	1024	GET / HTTP/1.1
115	00:00:00.000	192.168.1.1	192.168.1.1	HTTP	1024	GET / HTTP/1.1
116	00:00:00.000	192.168.1.1	192.168.1.1	HTTP	1024	GET / HTTP/1.1
117	00:00:00.000	192.168.1.1	192.168.1.1	HTTP	1024	GET / HTTP/1.1
118	00:00:00.000	192.168.1.1	192.168.1.1	HTTP	1024	GET / HTTP/1.1
119	00:00:00.000	192.168.1.1	192.168.1.1	HTTP	1024	GET / HTTP/1.1
120	00:00:00.000	192.168.1.1	192.168.1.1	HTTP	1024	GET / HTTP/1.1

Si debajo en la información desplegaríamos la sección Line-based text data veríamos los siguientes parámetros de envío:

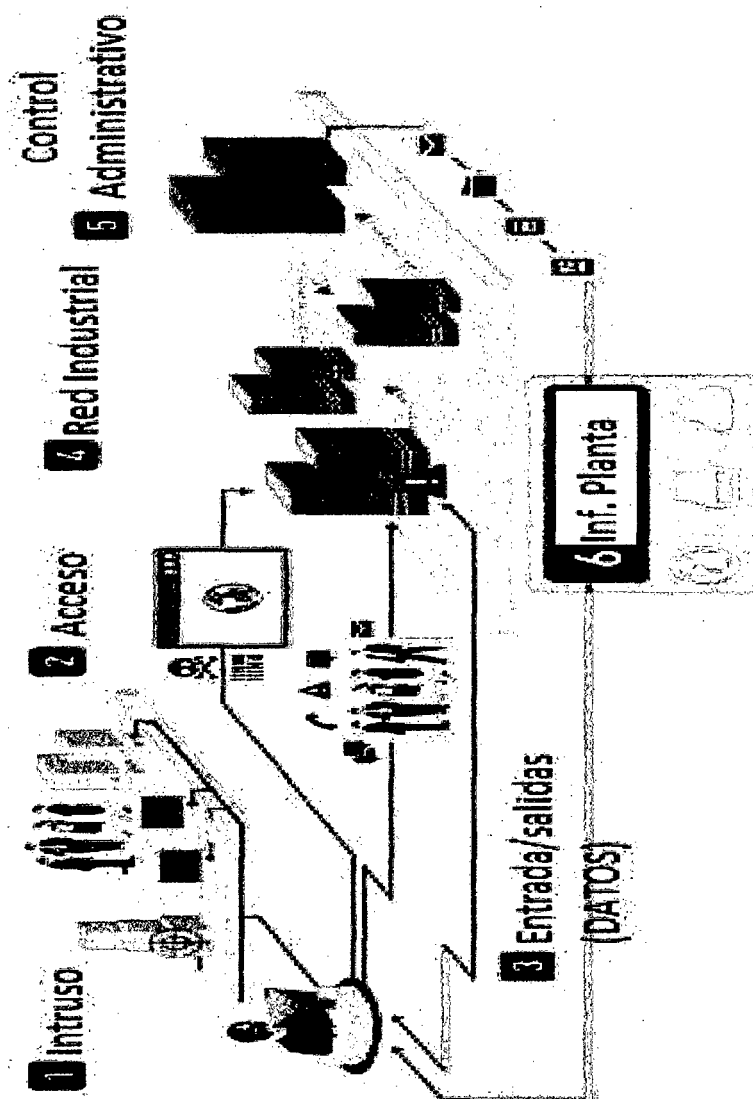
```
password=PepePerex&network=msn&initial=NLN&login_network=msn&username=victima.wireshark@40gmail.com&md5_init_status=NLN
```

```
@ L-nc-based text data: app=cat-on x=xxx-PORT=nr|encodes
password=PepePerez&network=nsn&initial=NL&login_network=nsn
```

En donde se ve perfectamente la contraseña (password=PepePerez),

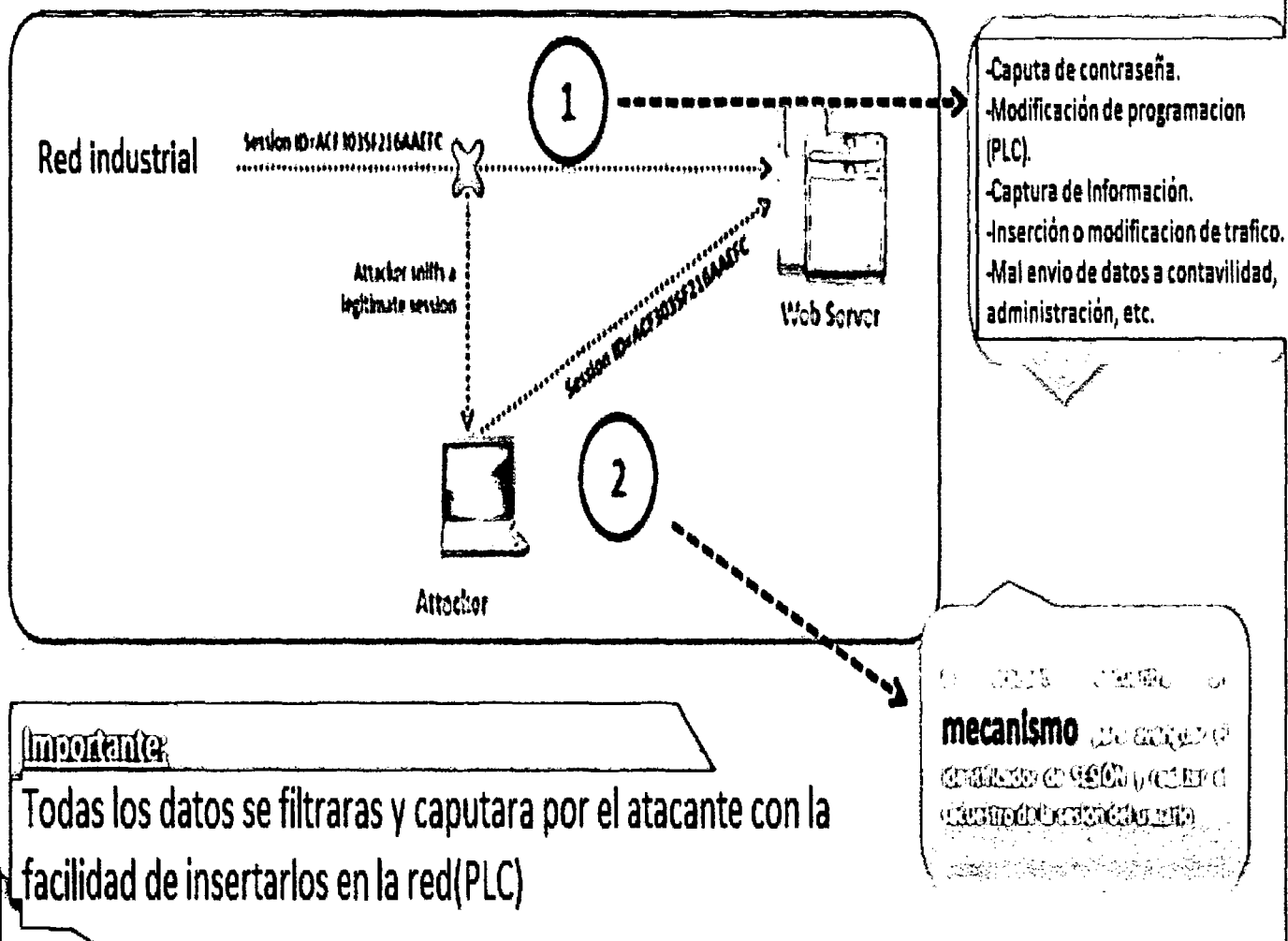
Ya que desde el punto de vista cualquier tipo de acceso directo o indirecto al PLC a través de Ethernet puede dañar toda la empresa.

En el diagrama A continuación nos muestra la capacidad del atacante no solo a red industrial sino también a otros niveles de acceso, administrativo, información delicada, etc. Pues toda la información que pasa en la red puede ser vulnerada, capturada y malintencionada.



7.1. Prueba de captura de contraseña e inserción de nuevos programas a través de la red (PLC)

Funcionamiento



- Captura de contraseña

Con estas pruebas queda demostrado que es necesaria una arquitectura de seguridad en redes para poder prevenir este tipo de ataques que pueden ser muy perjudiciales económicos como productivos. Nosotros planteamos un nivel de seguridad por ACL y seguridad de anillo.

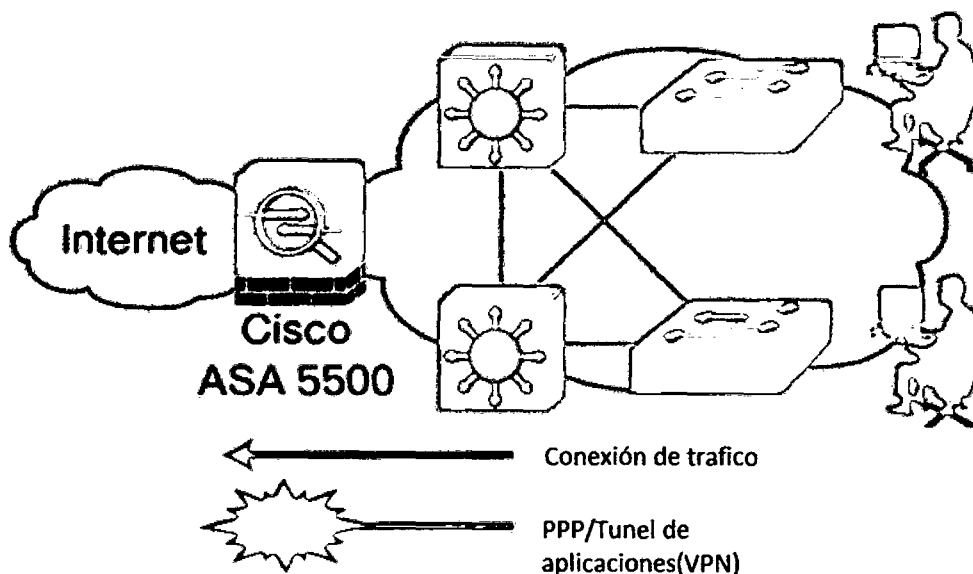
No.	Time	Source	Destination	Protocol	Info
1	0.102309	Cisco_3c:78:00	Broadcast	ARP	who has 198.133.219.25? Tell 10.21.148.177
6	0.102351	Cisco_b6:ce:04	Cisco_3c:78:00	APP	198.133.219.25 is at 00:08:a3:b6:ce:04
8	0.176444	10.21.148.177	198.133.219.25	TCP	80 → 80 [ACK] Seq=1000000000 Win=0 Len=0
10	0.176511	10.21.148.177	198.133.219.25	TCP	80 → 80 [ACK] Seq=1000000000 Win=0 Len=0
11	0.176511	198.133.219.25	10.21.148.177	TCP	80 → 80 [ACK] Seq=1000000000 Win=0 Len=0
12	0.176511	198.133.219.25	10.21.148.177	TCP	80 → 80 [ACK] Seq=1000000000 Win=0 Len=0


```

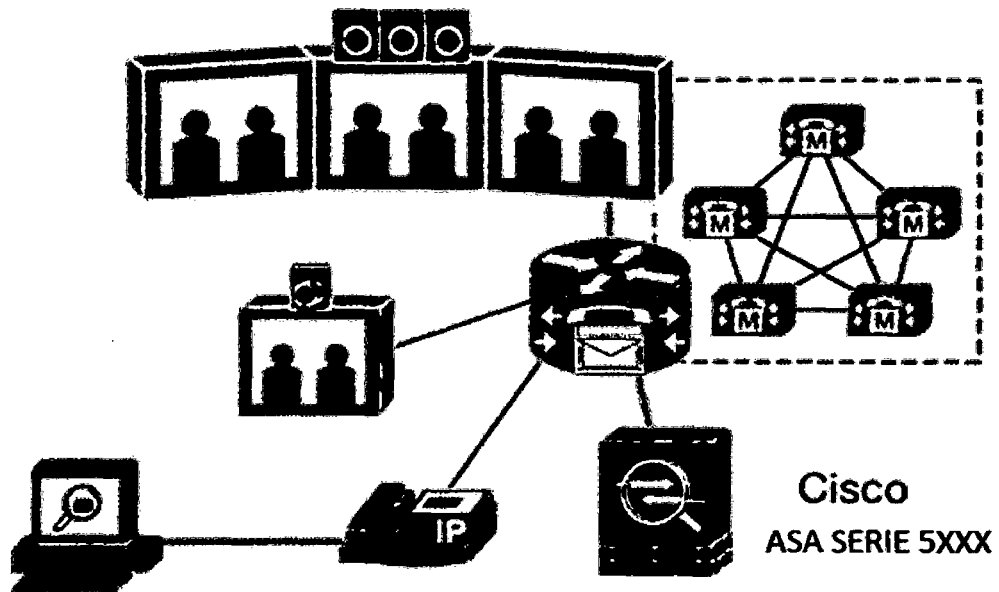
Ethernet II, Src: Cisco_3c:78:00 (00:05:9a:3c:78:00), Dst: Cisco_b6:ce:04 (00:08:a3:b6:ce:04)
Internet Protocol, Src: 10.21.148.177 (10.21.148.177), Dst: 198.133.219.25 (198.133.219.25)
Transmission Control Protocol, Src Port: 3351 (3351), Dst Port: http (80), Seq: 0, Len: 0
  Source port: 3351 (3351)
  Destination port: http (80)
  Sequence number: 0 (relative sequence number)
  Header length: 28 bytes
  Flags: 0x02 (SYN)
    0... .. = congestion window reduced (OW): not set
    0... .. = ECN-echo: not set
    0... .. = urgent: not set
    0... .. = ACK-acknowledgment: not set
    0... .. = push: not set
    0... .. = reset: not set
    0... .. = SYN: set
    0... .. = FIN: not set
  Window size: 65532
  
```

7.2. Posibilidades que nos presenta el cisco asa 5510

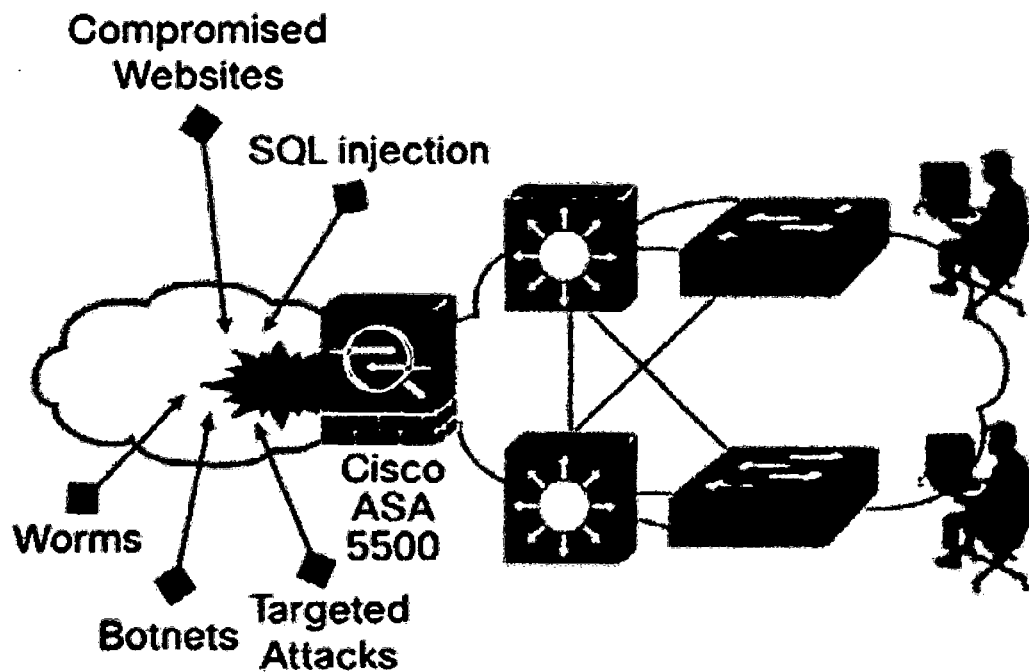
- Conexión de tráfico y VPN



- Protección de tráfico y filtrado de paquetes.

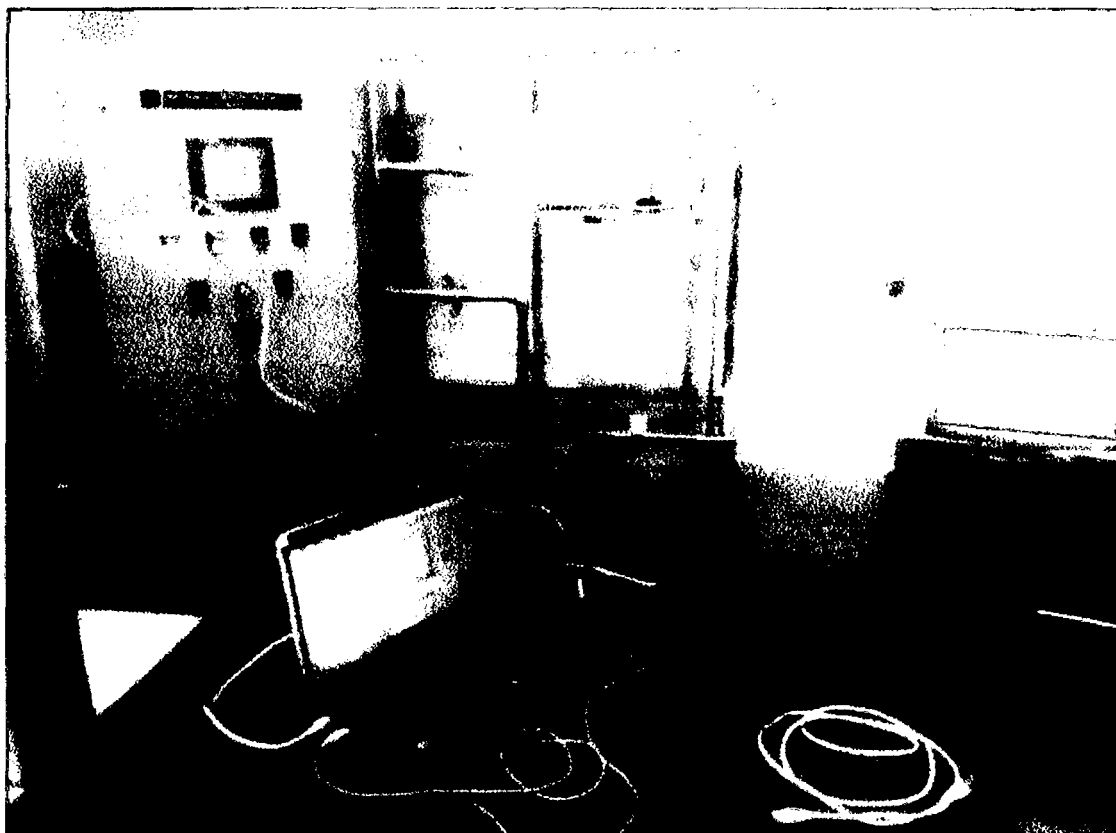


- Protección de ataques desde la nube.



Dada las posibilidades que nos presentan el equipo y la conexión de red desde el SW a la red de PLC se presenta la configuración de equipos desde el SW hasta el router con el firewall. Juntos.

7.3. Configuración de equipos



7.3.1. Configuración de SWITCH.

- Configuración de modo acceso
Switch# **configure terminal**
Switch(config)# **interface fastethernet0/0**
Switch(config-if)# **switchport mode access**
- Configuración de acceso a la VLAN (RED INDUSTRIAL)
SwitchA# **configure terminal**
SwitchA(config)# **interface fastethernet0/0**



SwitchA(config-if)# switchport access vlan 100

- Configuración de puerto de seguridad estático (RED INDUSTRIAL)

Switch# configure terminal

Switch(config)# interface fastethernet0/0

Switch(config-if)# switchport mode access

Switch(config-if)# switchport port-security

**Switch(config-if)# switchport port-security mac-address
0123.4567.8910**

- Configuración de Root Guard y STP.

Switch# configure terminal

Switch(config)# spanning-tree portfast bpduguard default

Switch(config)# interface fastethernet 0/0

Switch(config-if)# spanning-tree guard root

Switch(config-if)# spanning-tree bpduguard disable

- Configuración dinámica de ARP

Switch# configure terminal

Switch(config)# ip arp inspection vlan 100

Switch(config)# interface fastethernet0/0

Switch(config-if)# ip arp inspection trust

- Configuración Dinámica ARP inspector

Switch# configure terminal

Switch(config)# ip arp inspection vlan 100

Switch(config)# ip arp inspection validate src-mac

- Configuración Dinámica ARP (estática)

Switch# configure terminal

Switch(config)# arp access-list DAI_REDINDUSTRIAL



```
Switch(config-arp-nacl)# permit ip host 192.168.1.50 mac host  
abcd.ef01.1234
```

```
Switch(config-arp-nacl)# exit
```

```
Switch(config)# ip arp inspection filter DAI_example vlan 100
```

- **Configuración de VLAN privada para Red industrial.**

```
Switch# configure terminal
```

```
Switch(config)# vtp mode transparent
```

```
Switch(config)# vlan 200
```

```
Switch(config-vlan)# private-vlan community
```

```
Switch(config-vlan)# vlan 300
```

```
Switch(config-vlan)# private-vlan isolated
```

```
Switch(config-vlan)# vlan 100
```

```
Switch(config-vlan)# private-vlan primary
```

```
Switch(config-vlan)# private-vlan association 200,300
```

```
Switch(config-vlan)# exit
```

```
Switch(config)# int f0/0
```

```
Switch(config-if)# switchport mode private-vlan promiscuous
```

```
Switch(config-if)# switchport private-vlan mapping 100 and 200,300
```

```
Switch(config)# int f0/1
```

```
Switch(config-if)# switchport mode private-vlan host
```

```
Switch(config-if)# switchport private-vlan host-association 100 200
```

```
Switch(config-if)# int f0/2
```

```
Switch(config-if)# switchport mode private-vlan host
```

```
Switch(config-if)# switchport private-vlan host-association 100 300
```

- **Configuración para protección de Puerto(PVLAN)**

```
Switch# configure terminal
```

```
Switch(config)# interface fastetherent0/0
```

```
Switch(config-if)# switchport protected
```

```
Switch(config-if)# interface fastethernet0/1
```

```
Switch(config-if)# switchport protected
```



7.3.2. Configuración de Router

- Para acceso fuera de la red.

```
Router# configure terminal
```

```
Router(config)# radius-server host 10.1.1.1 auth-port 1812  
acct-port 1813 key rad123
```

```
Router(config)# exit
```

```
Router# copy running-config startup-config
```

- Configuración de acceso global

```
Router# configure terminal
```

```
Router(config)# aaa new model
```

```
Router(config)# exit
```

```
Router(config)# aaa authentication dot1x default group  
radius none
```

```
Router# copy running-config startup-config
```

- Configuración de autenticación (RADIUS)

```
Router# configure terminal
```

```
Router(config)# dot1x system-auth-control
```

```
Router(config)# interface FastEthernet 2/1
```

```
Router(config-if)# switchport mode access
```

```
Router(config-if)# switchport access vlan 90
```

```
Router(config-if)# authentication port-control auto
```

```
Router(config)# end
```

```
Router# copy running-config startup-config
```

- Configuración de autenticación y tiempo

```
Router# configure terminal
```

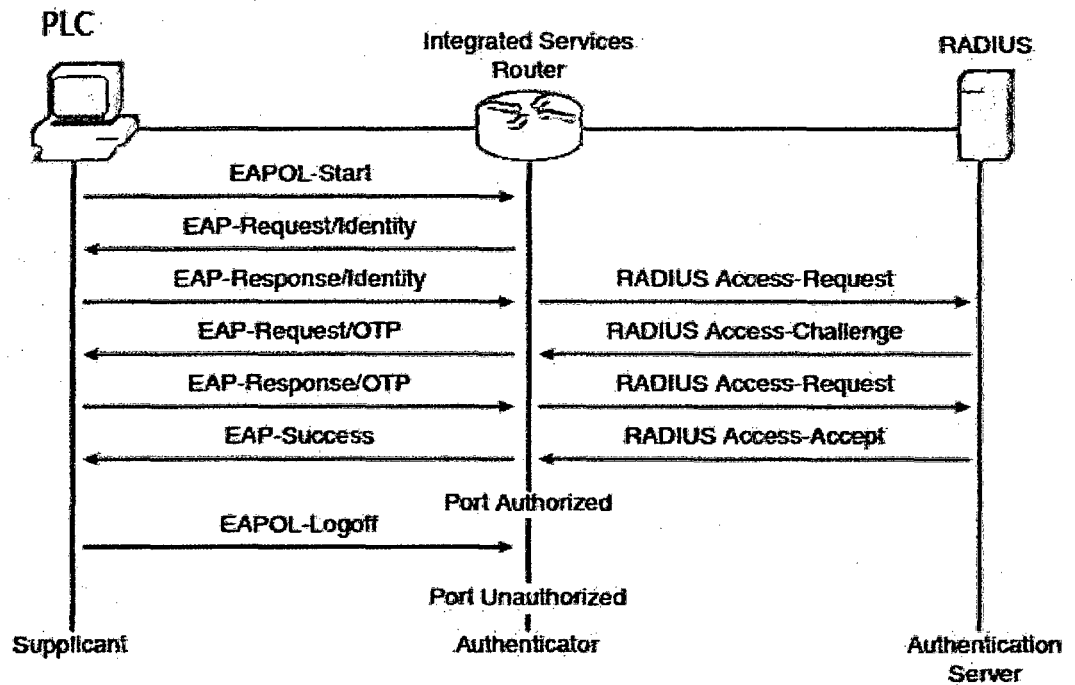
```
Router(config)# interface FastEthernet 2/1
```

```
Router(config-if)# authentication periodic
```

```
Router(config-if)# authentication timer reauthentication 600
```

```
Router(config)# end
```

```
Router# copy running-config startup-config
```



- Configuración de fallo de autenticación.

Router# **configure terminal**

Router(config)# **interface FastEthernet 2/1**

Router(config-if)# **authentication event fail retry 2 action authorize vlan 100**

Router(config-if)# **authentication event no-response action authorize vlan 100**

Router(config)# **end**

Router# **copy running-config startup-config**

- Ver salidas de control.

Router# **show dot1x**

Sysauthcontrol Enabled

Dot1x Protocol Version 2

Comando par aver accesos y autorizaciones

Router# **show dot1x all summary**



Interface	PAE	Client	Status
-----------	-----	--------	--------

Fa1 AUTH	000d.bcef.bfdc		AUTHORIZED
----------	----------------	--	------------

- Configuración por Autenticación automática de ACL (no recomendable)

Router# **configure terminal**

Router(config)# **aaa authorization network default group radius**

Router(config)# **radius-server vsa send authentication**

Router(config)# **ip device tracking**

Router(config)# **interface FastEthernet0/1**

Router(config-if)# **ip access-group inbound-ACL in**

Router(config)# **end**

Router(config)# **copy running-config startup-config**

- Configuración de Puerto critico para salida

Router# **configure terminal**

Router(config)# **authentication critical recovery delay 2000**

Router(config)# **interface FastEthernet0/1-24**

Router(config-if)# **authentication event server dead action
authorize vlan 100**

Router(config-if)# **authentication event server alive action
reinitialize**

Router(config-if)# **end**

Router(config)# **copy running-config startup-config**

- Configuración para permitir red en el router.

router(config)# **interface FastEthernet0/0**

router(config-if)# **ip address 192.168.100.1 255.255.255.0**

router(config-if)# **ip access-group 1 in**

router(config)# **access-list 1 permit 192.168.100.0 0.0.0.255**

- Configuración para permitir tráfico entrada y salida, reflejada en ACL.

Router (config)# ip access-list extended incoming

Router (config-ext-nacl)# permit tcp any any reflect tcp-traffic

Router (config)# ip access-list extended outgoing

Router (config-ext-nacl)# evaluate tcp-traffic

Router (config)# interface FastEthernet0/0

Router (config-if)# ip address 172.16.1.1 255.255.255.0

Router (config-if)# ip access-group incoming in

Router (config-if)# ip accesss-group outgoing out

7.3.3. Configuración del cisco asa 5-XXX.





- **Configuración para permitir HHTP**

ciscoasa(config)# **http server enable**

ciscoasa(config)# **no http server enable**

- **Configuración de mapeo para la VLAN(industrial)**

ciscoasa(config)# **interface ethernet0/1**

ciscoasa(config-if)# **switchport access vlan 10**

- **mirando configuración de salida.**

CISCOASA# **show port-channel summary**

Flags: D - down P - bundled in port-channel

I - stand-alone s - suspended

H - Hot-standby (LACP only)

U - in use N - not in use, no aggregation/nameif

M - not in use, no aggregation due to minimum links not met

w - waiting to be aggregated

Number of channel-groups in use: 1

Group Port-channel Protocol Ports

Group	Port-channel	Protocol	Ports
-----+-----+-----+-----1			
Po1(U)	LACP	Et0/1(P)	Et0/3(D)

- **Configurando troncal para salida de vlan.**

ciscoasa(config)# **interface ethernet0/1**

ciscoasa(config-if)# **no shutdown**

ciscoasa(config-if)# **interface ethernet0/1.1**

ciscoasa(config-subif)# **vlan 100**

ciscoasa(config-subif)# **no shutdown**

- **Configuración de ip RIP dentro de la red con KEY**

ciscoasa(config)# **access-list ripfilter standard permit 192.168.0.0**
255.255.0.0

ciscoasa(config)# **router rip**



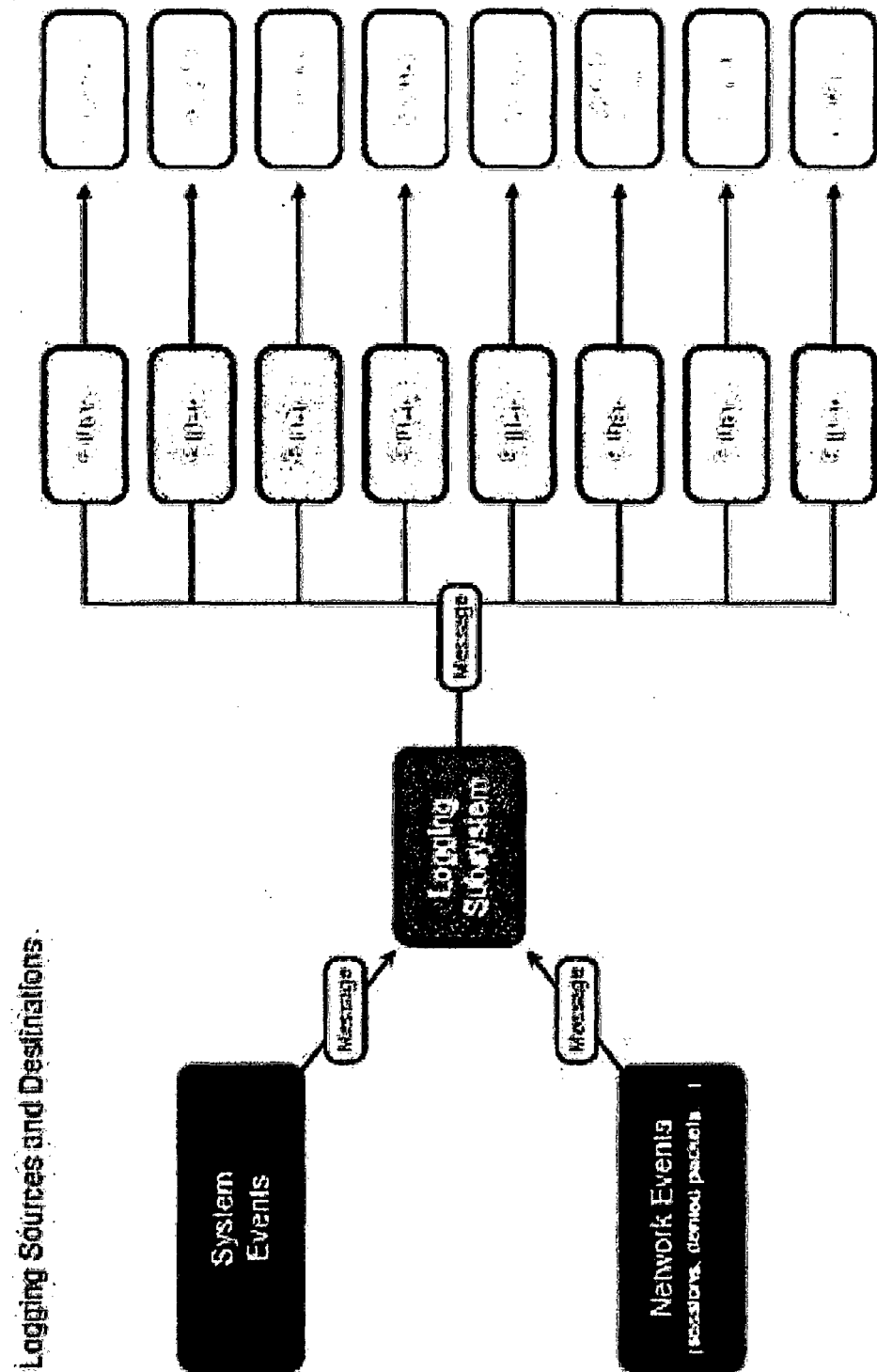
```
ciscoasa(config-router)# version 2
ciscoasa(config-router)# no auto-summary
ciscoasa(config-router)# default-information originate
ciscoasa(config-router)# network 192.168.1.0
ciscoasa(config-router)# distribute-list ripfilter in interface inside
ciscoasa(config-router)# exit
ciscoasa(config)# interface ethernet0/1
ciscoasa(config-if)# rip authentication mode md5
ciscoasa(config-if)# rip authentication key REDINDUSTRIAL key_id 1
```

- **Configuracion de logeo y nivel de seguridad**

```
ciscoasa(config)# interface ethernet0
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.4.1 255.255.255.0
ciscoasa(config-if)# rip authentication message-digest
ciscoasa(config-if)# rip message-digest-key 1 md5 REDINDUSTRIAL
ciscoasa(config-if)# exit
```

- **Configuracion de filtrado por red**

```
ciscoasa(config)# prefix-list InsideFilter 2 deny 192.168.99.0/32
ciscoasa(config)# prefix-list InsideFilter 1 permit 192.168.0.0/16
```





8. Conclusiones

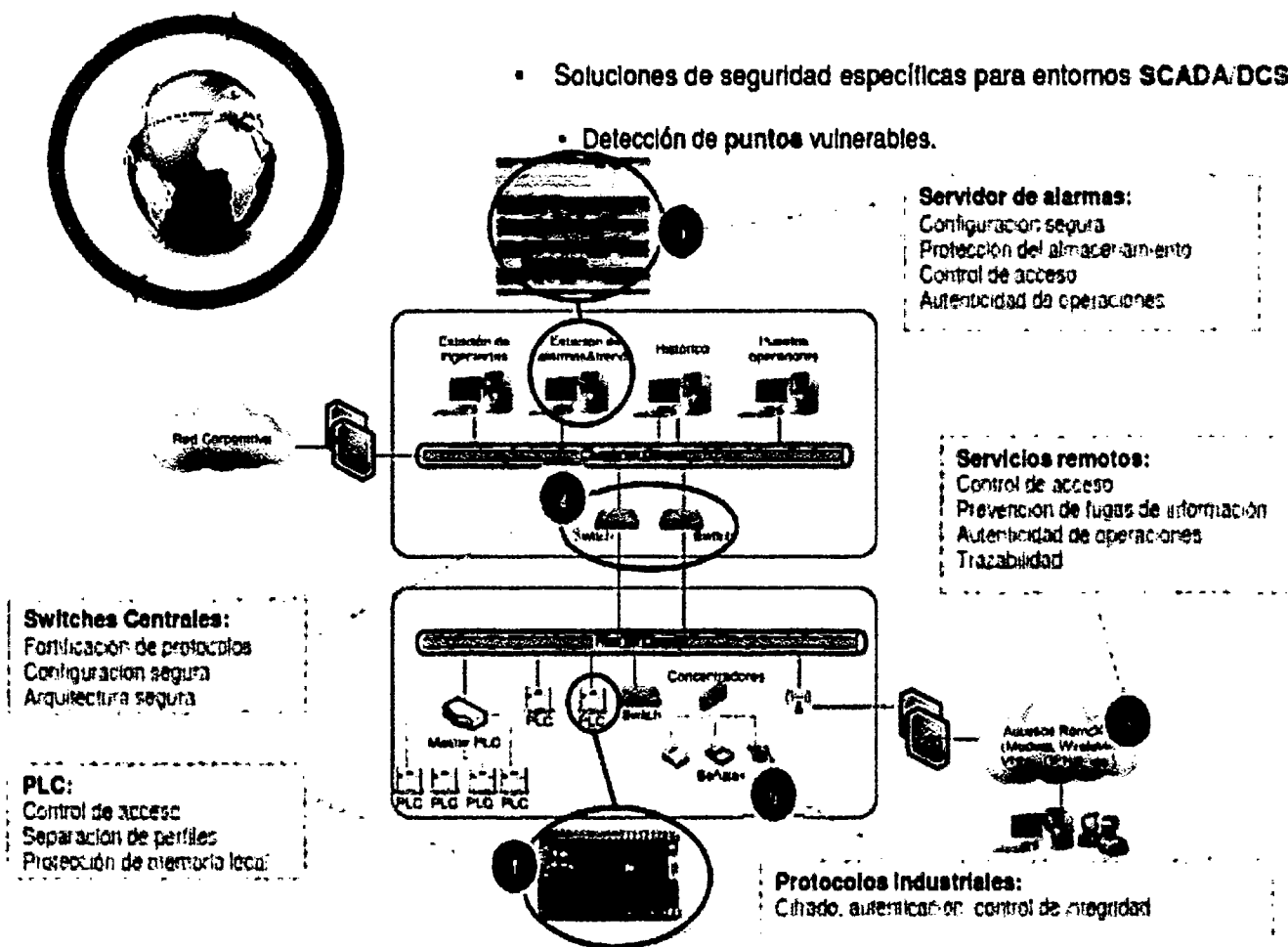
Se hace notar una necesidad de implementar un tipo de seguridad para evitar este tipo de ataques a través de y empezando desde el SW, ROUTER y firewall.

Consolidar la seguridad a nivel en la red industrial y administrativa, hacia a dentro y hacia afuera es fundamental para evitar pérdidas irremediables del equipo.

Esta arquitectura de seguridad que planteamos propone una seguridad desde el SW hasta el FIREWALL, mitigando riesgos no a un 100% pero a mayor o igual a un 85%, de ataques dentro y fuera de la red conocida.

La imagen a continuación muestra el nivel de seguridad que proponemos desde administrativos hasta la red PLC.

ARQUITECTURAS DE SEGURIDAD EN REDES DE CONTROL





9. Referencia Bibliográfica

[Dr. Hamadoun I. Touré, 2014] Dr. Hamadoun I. Touré, S. G. d. I. U. (2014). Banda ancha para el desarrollo sostenible. ITU news, 3:35.

[Lecoy, 2008] Lecoy, P. (2008). Optical fiber communication. ISTE Ltd and John Wiley & Sons, Inc., United States.

[Rajiv Ramaswami, 2010] Rajiv Ramaswami, Kumar N. Sivarajan, G. H. S. (2010). Optical Networks: A Practical Perspective. Morgan Kaufmann., United States.

[Banco Mundial, 2014] "Banco Mundial. 2014. El Pequeño libro de datos de Información y Tecnología de la Comunicación 2014. Washington, DC. © Banco

Mundial.<https://openknowledge.worldbank.org/handle/10986/18427>
Licencia: CC BY 3.0 IGO "

[Technical Guides, 2001] Technical Guides, The converged network infrastructure: An introductory guide. www.techguide.com

[1] Alzate, M. Conmutacion de paquetes de voz . Reporte de investigacion N° 6, Universidad Ditrital, Maestria en teleinformática, abril de 1995.

[3] Cisco Systems, (2001), Technical Considerations for converging Data, Voice and Video network. www.cisco.com

[6] Technical guides, (2001), Voice over IP VoIP.



10. Cronograma de actividades.

Activi dade s				Agosto'11				Setiembr e'08				Octubre'0 6				Noviembre '3				Noviemb re'24					
	Mese s																								
	Sema na	1	2	3	4	5	6	7	8	9	1 0	1 1	1 2	1 3	1 4	1 5	1 6	1 7	1 8	1 9					
Asesoría																									
Propuesta																									
Recolección de Datos																									
Clasificación del Material																									
Tratamiento de la Información																									
Observacione s																									
Diseño del Proyecto																									
Correcciones del Proyecto																									
Análisis e Interpretación																									
Elaboración del Informe																									
Presentación del Informe																									



11. Presupuesto.

El cuadro siguiente muestra la inversión total de la investigación

Descripción	Cantidad	Precio Unitario	Precio Total
Papel Bond A4	4 Millares	S/. 12.0	S/. 48.0
Fólder A4	10	S/. 0.5	S/. 5.0
CDs	10	S/. 4.5	S/. 45.0
Viajes	13	S/. 150	S/. 1950.0
Empastado	7	S/. 20	S/. 140.0
Impresiones	1000	S/. 0.35	S/. 350.0
Componentes Base de datos	Varios		S/. 1000.0
Total			S/. 3538.0

12. Financiación.

El financiamiento de la investigación será realizada por los investigadores

Fecha de Presentación

22/05/2015



Firma del Autor (Email-Telf. Fijo/Celular)

genady3@hotmail.com / 074 602109/ #971069092

Firma del Autor (Email-Telf. Fijo/Celular)

henryxd@live.com / #959579728

Firma del Asesor (Email-Telf. Fijo/Celular)

oromero@unprg.edu.pe / #969046490