ESCUELA SUPERIOR POLITECNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

MAESTRIA EN SEGURIDAD INFORMATICA APLICADA

"IMPLEMENTACIÓN DE UN ESQUEMA DE SEGURIDAD LÓGICA BASADA EN SOFTWARE LIBRE PARA LA DIRECCIÓN DISTRITAL DE SALUD DE CIUDAD DEL SOL"

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del grado de:

MAGÍSTER EN SEGURIDAD INFORMÁTICA APLICADA

LORENA ALEXANDRA VILLÓN MORENO

GUAYAQUIL - ECUADOR

2015

AGRADECIMIENTO

A Dios por el regalo que me ofrece cada día.

A Bachita y Pepito, por ser el motor que impulsa mi vida, por su amor incondicional.

A Mami María quien me ha visto crecer como una hija.

A mis amigos Sandra, Roberto y Fabricio por apoyarme en los momentos que más necesite, y alentarme a culminar esta meta.

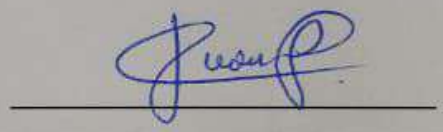
DEDICATORIA

Dedico el presente trabajo a Pepito y Bachita en reconocimiento a su apoyo incondicional.

TRIBUNAL DE SUSTENTACION

Ing. Lenin Freire Cobo

DIRECTOR DE LA MSIA



Ing. Juan Carlos García

PROFESOR DELEGADO

POR LA UNIDAD ACADEMICA

Ing. Lenin Freire Cobo

PROFESOR DELEGADO

POR LA UNIDAD ACADEMICA

RESUMEN

En el Capítulo 1 se presenta visión general de la situación actual de la Dirección Distrital de Salud de la Ciudad del Sol en cuanto a la falta de un esquema de seguridad lógica en la Unidad Distrital de Tecnologías de la Información y Comunicaciones.

En el Capítulo 2 se revisaran los resultados de un Análisis de Riesgos Tecnológicos, identificándose los activos principales y vulnerabilidades de la institución.

En el Capítulo 3 se define e implementa el esquema de seguridad requerido para solucionar los problemas de seguridad encontrados en la Unidad Distrital de Tecnologías.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

Actualmente se está creando conciencia en cuanto a una cultura de seguridad, garantizando la protección de la información como activo principal de las instituciones.

La seguridad de la información tal como lo menciona la Norma ISO/IEC 17799:2005 es la preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.

Con el desarrollo de las redes de computadoras y con el acceso a la nube desde cualquier parte del mundo, se van incrementando los riesgos de ser víctimas de ataques, afectando principalmente a la información expuesta en la web o servicios que se ofrecen a través de esta.

A través del presente trabajo se detallara las políticas implementadas en la Dirección Distrital de Salud de Ciudad del Sol para minimizar los riesgos de ser víctimas de ataques a nuestra seguridad de la información.

CAPÍTULO 1

GENERALIDADES

1.1. Antecedentes

La Dirección Distrital de Salud de Ciudad de Sol forma parte de la nueva Estructura del Ministerio de Salud, dedicada a dirigir y administrar el sistema de salud en su jurisdicción, en el marco de las políticas nacionales del sector y normativa vigente, para brindar una atención integral a la población, con calidad, eficiencia y equidad.

A partir de Junio del 2014 se inició el proceso de Distritalización, finalizando la etapa que inicio en el año 2008 como Dirección Provincial de Salud de Ciudad del Sol.

Como parte de dicho proceso los activos fueron divididos, siendo asignado a otra Dirección Distrital el servidor de correo electrónico.

1.2. Descripción del problema

Al momento la Unidad Distrital de Tecnologías de la Información y Comunicación de la Dirección de Salud de Ciudad del Sol no cuenta con un esquema de seguridad implementado.

- Se inicia funciones con un acceso a internet de 4Mbps de ancho de banda, los mismos que un equipo CISCO 800 series se encarga de distribuir en la red LAN.

- Un equipo sobre el que se configuro un servidor PROXY y DHCP.

- Un equipo sobre el que se configuro un servidor de aplicaciones (Sistema FALCO, módulo de Inventario y Bodega).

- Adicional se accede al servidor de correo institucional que fue configurado para la Dirección Provincial de Salud.

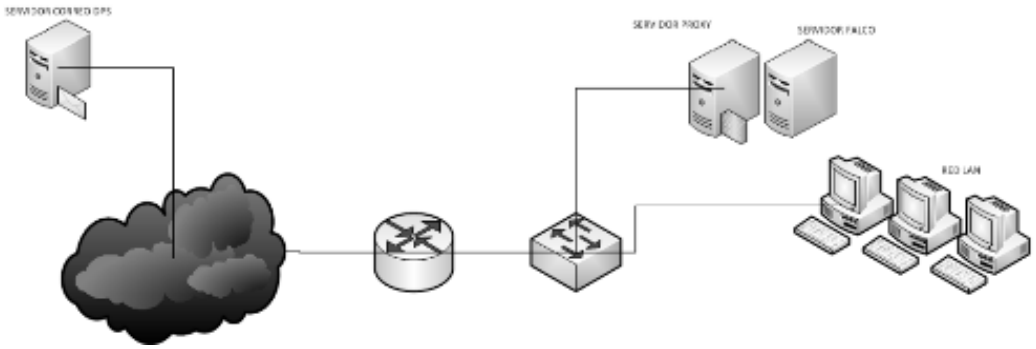


Figura 1.1 Diagrama de Red del Distrito – Noviembre 2014

1.3. Solución Propuesta

Teniendo en cuenta que actualmente la red de la Dirección Distrital de Salud de Ciudad del Sol no cuenta con un esquema de seguridad implementado, se requiere que se proteja los activos de información con el fin de minimizar los impactos que podrían generar las vulnerabilidades presentes en la actualidad.

Al ser una empresa pública se utilizara software libre para la implementación del esquema antes mencionado.

Por tal motivo debemos considerar:

- ✓ Análisis de riesgo, de esta manera se determinaran los requerimientos de seguridad para evitar que puntos débiles y/o vulnerabilidades afecten los activos de la institución.
- ✓ Diseñar e implementar mecanismos que se requieren para salvaguardar los activos de la institución.

CAPÍTULO 2

ANÁLISIS DE RIESGOS TECNOLÓGICOS

2.1. Identificación de activos

Para efectos de este análisis se ha considerado 3 clases de activos: Información, Software y Hardware, los mismos que son de gran importancia para los procesos de la Dirección Distrital de Salud de Ciudad del Sol.

Tabla 1 Activos Información Dirección Distrital

ITEM	ACTIVOS	DETALLE
1	Base de datos de Sistema FALCO –	Información de ingresos y egresos de los bienes de las unidades operativas

	Modulo Inventario	de la Dirección Distrital
2	Base de datos de Sistema FALCO – Modulo Admisión	Información de registro de pacientes de las unidades operativas de la Dirección Distrital
3	Buzones de correo de los usuarios de la institución	Información de Gestión de los funcionarios de las unidades operativas de la desaparecida Dirección Provincial

Tabla 2 Activos Software del Distrito

ITEM	ACTIVOS	DETALLE
1	Sistema FALCO – Modulo Inventario	Módulo que maneja la información correspondiente al inventario de Bodega de las unidades operativas del Distrito
2	Sistema FALCO – Modulo Admisión	Módulo que maneja la información correspondiente a los datos de los

		pacientes que son atendidos en las unidades operativas del Distrito
3	eSIGEF	Sistema de Gestión Financiera (eSigef), un software de uso de entidades publicas
4	QUIPUX	Sistema de Gestión Documental de entidades publicas
5	SGI	Sistema de Gestión de Inventarios

Tabla 3 Activos Hardware del Distrito

ITEM	ACTIVOS	DETALLE
1	Servidor FALCO	Equipo que almacena la base de datos del Sistema FALCO, tanto Modulo de Inventario como Modulo Admisión
2	Router	Equipo que permite la conexión a

		internet
3	Switch	Equipo que permite estructurar la red interna
4	Computadores Personales	Estaciones de trabajo de los funcionarios del Distrito
5	Puntos de Acceso	Hardware inalámbrico que facilita la conexión

2.2. Identificación de vulnerabilidades existentes

Se consideran como tipos de amenazas los detallados a continuación:

- Amenazas naturales, las que son determinadas por las condiciones del ambiente; por ejemplo: Desastres naturales.
- Amenazas involuntarias, tal como su nombre lo indican son acciones involuntarias realizadas por los usuarios y/o sistemas.
- Amenazas intencionales, son acciones realizadas con la intención de generar un problema en la seguridad de los activos; por ejemplo: accesos no autorizados por usuarios internos y externos.

Tabla 4 Tasación de Activos de la Dirección Distrital.

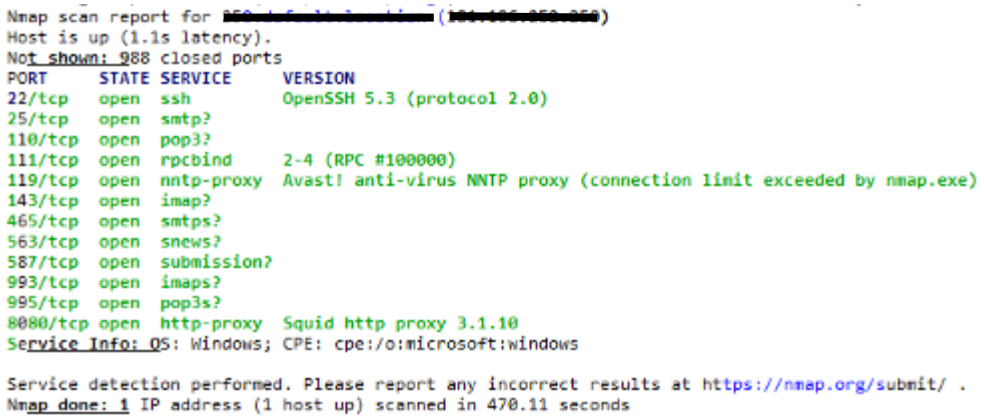
ACTIVOS	TASACION			
	Confidencialidad	Integridad	Disponibilidad	Total
Buzones de correo de los usuarios de la institución	A	A	A	A
Sistema FALCO – Modulo Inventario	A	A	A	A
Sistema FALCO – Modulo Admisión	A	A	A	A
eSIGEF	A	A	A	A
QUIPUX	A	A	A	A
SGI	A	A	A	A

Servidor FALCO	A	A	A	A
Router	-	A	A	A
Switch	-	A	A	A
Computadores Personales	A	A	A	A
Puntos de Acceso	-	A	A	A

A continuación se realiza el analisis de vulnerabilidades de los equipos servidores de la Dirección Distrital de Salud con el software Zenmap.

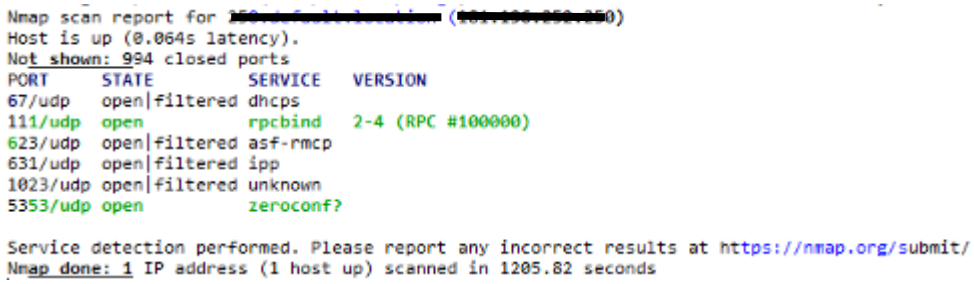
```
Nmap scan report for [redacted] ([redacted])
Host is up (0.052s latency).
Not shown: 996 closed ports
PORT     STATE    SERVICE    VERSION
22/tcp   open     ssh        OpenSSH 5.3 (protocol 2.0)
25/tcp   filtered smtp
111/tcp  open     rpcbind    2-4 (RPC #100000)
8080/tcp open     http-proxy Squid http proxy 3.1.10

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.64 seconds
```

Figura 2.1 Análisis de versión de servicios SERVIDOR PROXY



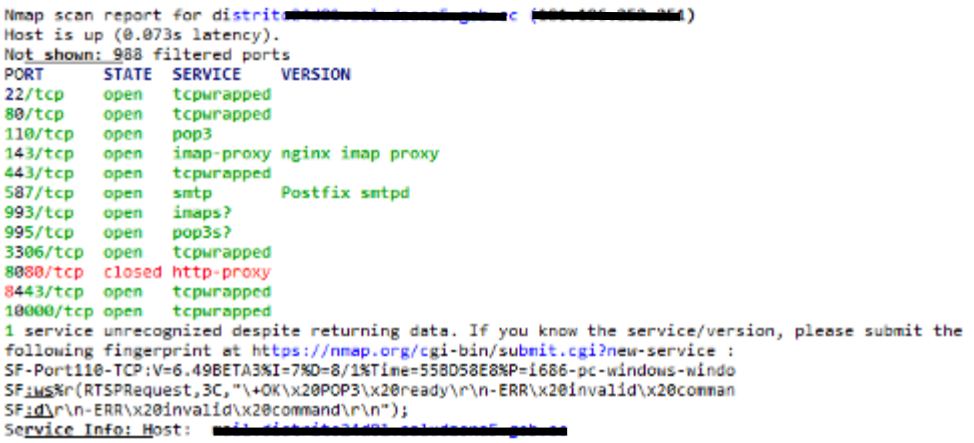
```
Nmap scan report for [redacted]
Host is up (1.1s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 5.3 (protocol 2.0)
25/tcp   open  smtp?
110/tcp  open  pop3?
111/tcp  open  rpcbind     2-4 (RPC #100000)
119/tcp  open  nntp-proxy  Avast! anti-virus NNTP proxy (connection limit exceeded by nmap.exe)
143/tcp  open  imap?
465/tcp  open  smtps?
563/tcp  open  snews?
587/tcp  open  submission?
993/tcp  open  imaps?
995/tcp  open  pop3s?
8080/tcp open  http-proxy  Squid http proxy 3.1.10
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 470.11 seconds
```

Figura 2.2 Análisis de Puertos TCP SERVIDOR PROXY



```
Nmap scan report for [redacted]
Host is up (0.064s latency).
Not shown: 994 closed ports
PORT     STATE         SERVICE   VERSION
67/udp   open|filtered dhcps
111/udp  open          rpcbind   2-4 (RPC #100000)
623/udp  open|filtered asf-rmcp
631/udp  open|filtered ipp
1023/udp open|filtered unknown
5353/udp open          zeroconf?

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 1205.82 seconds
```

Figura 2.3 Análisis de Puertos UDP SERVIDOR PROXY



```
Nmap scan report for [redacted]
Host is up (0.073s latency).
Not shown: 988 filtered ports
PORT     STATE  SERVICE    VERSION
22/tcp   open   tcpwrapped
80/tcp   open   tcpwrapped
110/tcp  open   pop3
143/tcp  open   imap-proxy nginx imap proxy
443/tcp  open   tcpwrapped
587/tcp  open   smtp       Postfix smtpd
993/tcp  open   imaps?
995/tcp  open   pop3s?
3306/tcp open   tcpwrapped
8080/tcp closed http-proxy
8443/tcp open   tcpwrapped
10000/tcp open  tcpwrapped
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port110-TCP:V=6.49BETA3%I=7%D=8/1%Time=558D58E8%P=i686-pc-windows-windo
SF:ws%r(RTSPRequest,3C,"\+OK\x20POP3\x20ready\r\n-ERR\x20invalid\x20comman
SF:d\r\n-ERR\x20invalid\x20command\r\n");
Service Info: Host:  [redacted]
```

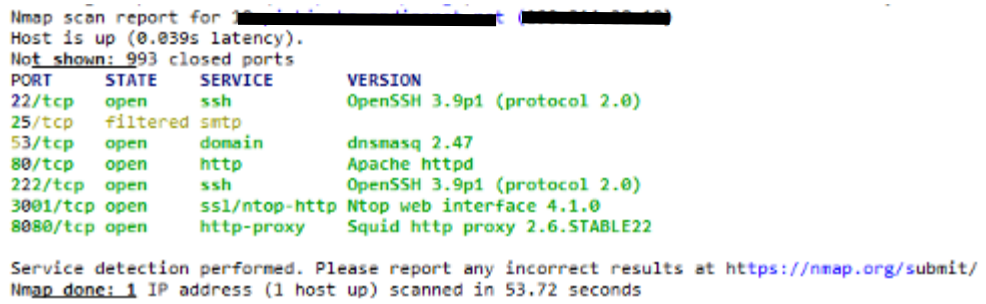
Figura 2.4 Análisis de versión de servicios SERVIDOR FALCO

```
Nmap scan report for distrito[redacted] ([redacted])
Host is up (0.00089s latency).
Not shown: 987 filtered ports
PORT     STATE SERVICE    VERSION
22/tcp   open  tcpwrapped
25/tcp   open  smtp?
80/tcp   open  tcpwrapped
110/tcp  open  pop3
119/tcp  open  nntp?
143/tcp  open  imap?
443/tcp  open  tcpwrapped
465/tcp  open  smtps?
563/tcp  open  snews?
587/tcp  open  smtp       Postfix smtpd
993/tcp  open  imaps?
995/tcp  open  pop3s?
3306/tcp open  tcpwrapped
2 services unrecognized despite returning data. If you know the service/version, please submit the
following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port110-TCP:V=6.49BETA3%I=7%D=8/1%Time=55BD69A9%P=i686-pc-windows-windo
SF:ws%r(RTSPRequest,3C,"\+OK\x20POP3\x20ready\r\n-ERR\x20invalid\x20comman
SF:d\r\n-ERR\x20invalid\x20command\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port143-TCP:V=6.49BETA3%I=7%D=8/1%Time=55BD69C4%P=i686-pc-windows-windo
SF:ws%r(SSLSessionReq,12,"\*\x20OK\x20IMAP4\x20ready\r\n")%r(SIPOptions,49
SF:,"\*\x20OK\x20IMAP4\x20ready\r\nOPTIONS\x20BAD\x20invalid\x20command\r\
SF:nVia:\x20BAD\x20invalid\x20command\r\n")%r(LANDesk-RC,12,"\*\x20OK\x20I
SF:MAP4\x20ready\r\n")%r(TerminalServer,12,"\*\x20OK\x20IMAP4\x20ready\r\n
SF:")%r(NCP,12,"\*\x20OK\x20IMAP4\x20ready\r\n")%r(NotesRPC,12,"\*\x20OK\x
SF:20IMAP4\x20ready\r\n")%r(WMSRequest,12,"\*\x20OK\x20IMAP4\x20ready\r\n"
SF:)%r(oracle-tns,12,"\*\x20OK\x20IMAP4\x20ready\r\n")%r(afp,12,"\*\x20OK\
SF:x20IMAP4\x20ready\r\n")%r(kumo-server,12,"\*\x20OK\x20IMAP4\x20ready\r\
SF:n");
Service Info: Host:  [redacted]
```

Figura 2.5 Análisis de puertos TCP SERVIDOR FALCO

```
Nmap scan report for distrito24d01.saludzona5.gob.ec (181.196.252.251)
Host is up (0.055s latency).
Not shown: 998 filtered ports
PORT    STATE         SERVICE        VERSION
623/udp open|filtered asf-rmcp
664/udp open|filtered secure-aux-bus

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 1149.24 seconds
```

Figura 2.6 Análisis de Puertos UDP SERVIDOR FALCO



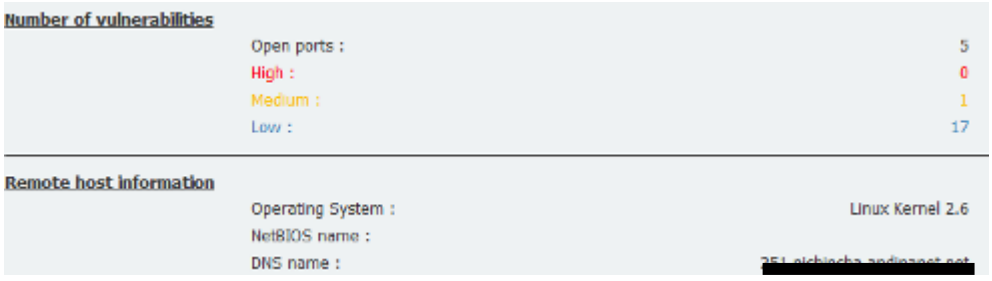
```
Nmap scan report for [redacted]
Host is up (0.039s latency).
Not shown: 993 closed ports
PORT     STATE    SERVICE       VERSION
22/tcp   open     ssh           OpenSSH 3.9p1 (protocol 2.0)
25/tcp   filtered smtp
53/tcp   open     domain        dnsmasq 2.47
80/tcp   open     http          Apache httpd
222/tcp  open     ssh           OpenSSH 3.9p1 (protocol 2.0)
3001/tcp open     ssl/ntop-http Ntop web interface 4.1.0
8080/tcp open     http-proxy    Squid http proxy 2.6.STABLE22

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 53.72 seconds
```

Figura 2.7 Análisis de servicios FIREWALL ENDIAN

Number of vulnerabilities	
Open ports :	4
High :	0
Medium :	1
Low :	24

Remote host information	
Operating System :	Linux Kernel 2.6
NetBIOS name :	
DNS name :	[redacted]

Figura 2.8 Análisis de vulnerabilidades realizado con Nessus al Servidor Proxy



Number of vulnerabilities	
Open ports :	5
High :	0
Medium :	1
Low :	17

Remote host information	
Operating System :	Linux Kernel 2.6
NetBIOS name :	
DNS name :	[redacted]

Figura 2.9 Análisis de vulnerabilidades realizado con Nessus al servidor de aplicaciones

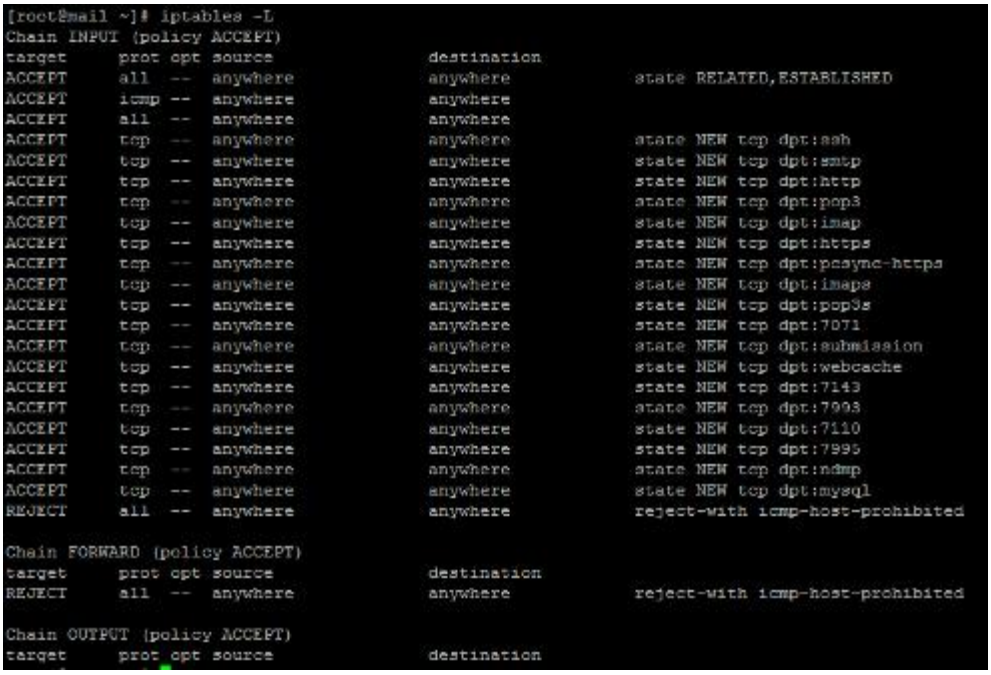


Figura 2.10 Reglas IPTABLES Servidor FALCO y de correos

2.3. Análisis de resultados

- En las Figuras 2.2, 2.3, 2.4 se muestran los resultados del Análisis de versión de servicios, Análisis de puertos TCP y UDP que se encuentran abiertos y filtrados en SERVIDOR PROXY, de lo que se puede obtener la versión SSH es la 5.3, que permite la conexión por el puerto 22 que se encuentra en estado abierto. Adicional se tiene el puerto 8080 en estado abierto y la versión de Squid es 3.1.10

- En las Figuras 2.5, 2.6, 2.7 se muestran los resultados del Análisis de versión de servicios, Análisis de puertos TCP y UDP que se

encuentran abiertos y filtrados en SERVIDOR del SISTEMA FALCO, de lo que se puede obtener la versión SSH es la 5.3, que permite la conexión por el puerto 22 que se encuentra en estado abierto. Adicional se tiene el puerto 8080 en estado abierto y la versión de Squid es 3.1.10

- Se realizó un análisis de vulnerabilidades a ambos servidores utilizando la herramienta Nessus, la que determino que el SERVIDOR PROXY tiene 4 puertos abiertos, una vulnerabilidad media (trafico mediante UDP) y 24 vulnerabilidades bajas. En el SERVIDOR del Sistema FALCO se detectaron 5 puertos abiertos, una vulnerabilidad media y 17 vulnerabilidades bajas.

- Para mitigar la vulnerabilidad media encontrada se agregan las siguientes líneas en el iptables, Considerando que no deben estar permitido tráfico UDP, salvo para recibir respuestas de servidores DNS por el puerto 53, se deberá agregar al firewall:

    - -A INPUT -p udp --source-port 53 -j ACCEPT
    - -A INPUT -p udp -j REJECT --reject-with icmp-port-unreachable

2.4. Definición de requerimientos de seguridad

En base a los activos de definidos se establecen los requerimiento de seguridad requeridos y se detallan la tabla siguiente.

Tabla 5 Definición de Requerimientos de Seguridad para los Activos.

ACTIVOS	REQUERIMIENTOS DE SEGURIDAD
Buzones de correo de los usuarios de la institución	Confidencialidad: Solo deben acceder los propietarios de los buzones Integridad: Solo deben acceder los propietarios de los buzones Disponibilidad: Acceso a los datos 24/7
Sistema FALCO – Modulo Inventario	Confidencialidad: Solamente área Administrativa Financiera podrá conocer la información del Módulo Integridad: Asignar perfiles de acceso para personal autorizado Disponibilidad: Acceso a los datos 24/5

Sistema FALCO – Modulo Admisión	Confidencialidad: Solamente área Admisión y Personal Médico podrá conocer la información del Módulo Integridad: Asignar perfiles de acceso para personal autorizado Disponibilidad: Acceso a los datos 24/5
eSIGEF	Confidencialidad: Solo acceso al personal autorizado con claves asignadas Integridad: Debe ser garantizada por el personal al que se asigna credenciales. Disponibilidad: Acceso a los datos 24/7
QUIPUX	Confidencialidad: Solo deben acceder los propietarios de los buzones Integridad: Solo deben acceder los propietarios de los buzones Disponibilidad: Acceso a los datos 24/7
SGI	Confidencialidad: Solo acceso al personal autorizado

	con claves asignadas Integridad: Debe ser garantizada por el personal al que se asigna credenciales. Disponibilidad: Acceso a los datos 24/7
Servidor FALCO	Integridad: Administrado por la Unidad Distrital de Tecnologías Disponibilidad: Acceso a los datos 24/7
Router	Integridad: Administrado por la Unidad Distrital de Tecnologías Disponibilidad: Acceso a los datos 24/7
Switch	Integridad: Administrado por la Unidad Distrital de Tecnologías Disponibilidad: Acceso a los datos 24/7
Puntos de Acceso	Integridad: Administrado por la Unidad Distrital de Tecnologías

	Disponibilidad: Acceso a los datos 24/7
Computadores Personales	Confidencialidad: Solo para el personal custodio Integridad: Administrado por la Unidad Distrital de Tecnologías Disponibilidad: Acceso a los datos 24/7

CAPÍTULO 3

IMPLEMENTACIÓN DEL ESQUEMA DE SEGURIDAD LÓGICA

3.1. Diseño de la Red

Para diseñar la red se utiliza la Arquitectura Modular de CISCO SAFE, la misma que puede ser aplicada a pequeñas y medianas empresas.

El principal objetivo del modelo de seguridad (SAFE) para redes de empresas de Cisco es ofrecer información sobre las mejores prácticas a las partes interesadas en el diseño e implementación de redes seguras.

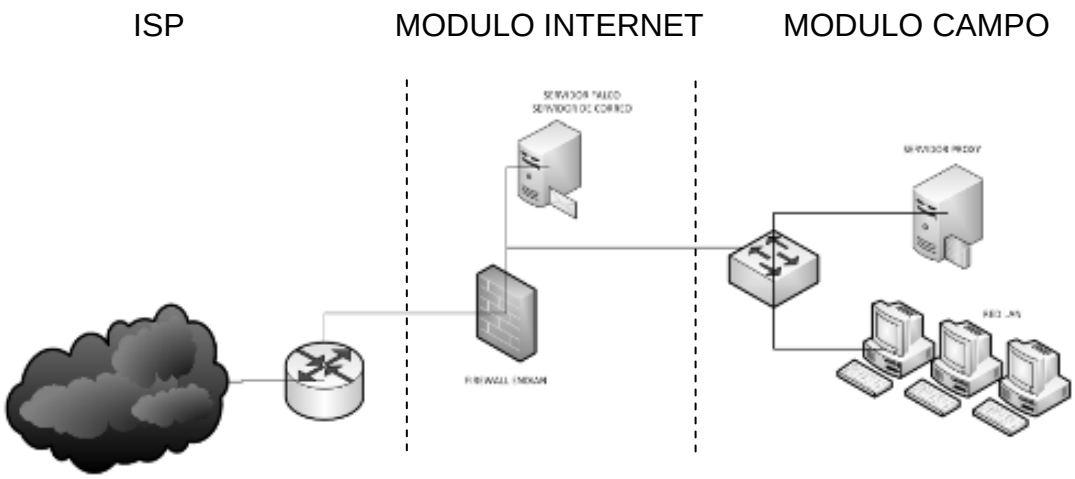


Figura 3.1 Arquitectura Modular de CISCO SAFE

- Modulo ISP, se contempla el Hardware de propiedad de CNT, mediante el cual nos llega el servicio de internet.

- Modulo Internet, se encuentra conformado por el Firewall que se configurara utilizando una PC con el Software ENDIAN, y el servidor de correo electrónico implementado con un dominio propio para la Dirección Distrital, en el que se tiene la base de datos del Sistema FALCO.

- Módulo Campo, se ha considerado el servidor proxy que da el servicio DHCP a la red interna, así como los puntos de acceso, estaciones de trabajo, impresoras de red de los funcionarios.

3.2. Políticas de Seguridad

Durante la evaluación de la red de la Dirección Distrital de Salud se pudo definir las principales políticas de Seguridad a ejecutarse tanto en Servidores como estaciones de trabajo.

- En el diseño de red con el que inicio la Dirección Distrital no fueron considerados requerimientos de seguridad debido a que los equipos expuestos a internet (Sistema FALCO) no tenía protección, por tal motivo se debe implementar una zona desmilitarizada.
- Las credenciales de acceso para los servidores deberán ser modificadas mínimo cada 3 meses, y cada uno de los administradores debe tener asignada credencial para poder identificar responsables de accesos y/o modificaciones mediante procesos de auditorías.
- Para efectos de auditorías se deben respaldar los archivos de configuración y logs de servidores.
- Se deberán ejecutar las actualizaciones de seguridad para los sistemas operativos tanto de los servidores como de las estaciones de trabajo.
- Cumplir las Políticas de Uso de Servicios de Red y Servicios Informáticos del MSP.
- Se debe realizar el respaldo periódico de la base de datos del Sistema FALCO, y del Servidor de Correo Electrónico en caso de requerirse

se podrá realizar la restauración de los datos ante alguna eventualidad.

- Se debe garantizar que las contraseñas que definan los usuarios propietarios de los buzones de correo sean robustas y no permita la repetición.
- Debido al Decreto Presidencial 1014 referente al Uso de Software Libre en equipos informáticos, se debe proceder a la instalación del Sistema Operativo Ubuntu, considerado el más óptimo para equipos clientes.
- Se establecerá restricciones a los usuarios propietarios de los equipos, y el personal de Tecnologías tendrá la clave de administrador para realizar cambios de configuraciones o instalación de programas.

3.3. Configuración de servidores

Considerando que la Dirección Distrital no contaba con correo institucional propio se procede a realizar la configuración del servidor de correo escogiendo la suite de colaboración Zimbra en el equipo que se tiene implementado el Sistema FALCO.

Se optimiza las particiones creadas utilizando LVM, se redimensionan la capacidad de la partición OPT, donde se almacenaran los buzones de correo.

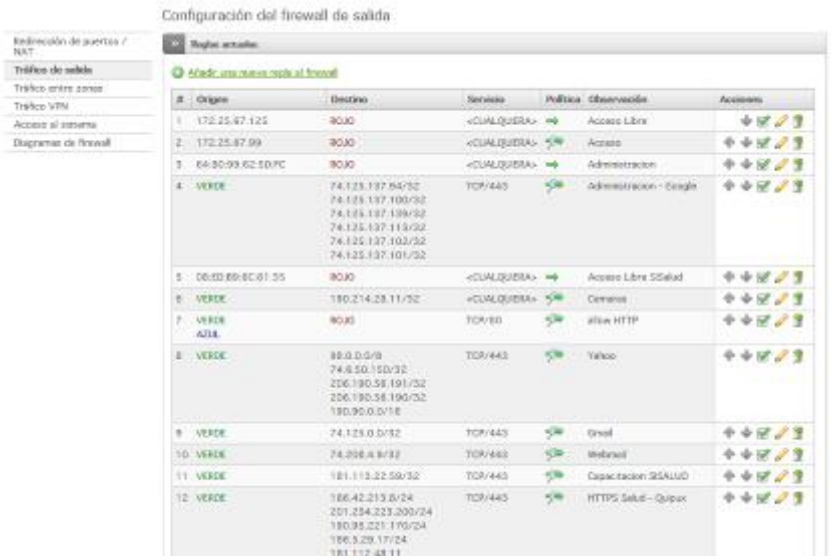
En la configuración de los dos servidores con los que cuenta la Dirección Distrital se debe implementar lo siguiente:

- Aplicar las actualizaciones del sistema operativo, de tal manera se garantiza que se apliquen los parches de seguridad para evitar problemas de seguridad.
- Se deberá considerar la habilitación del módulo de seguridad SELinux para el control de acceso.
- Realizar la el aseguramiento de la seguridad de los servidores, deshabilitando los servicios que se encuentran activos por defecto después de una instalación.
- Deshabilitar la opción sobre la información del sistema operativo, para que no sea detectado en la etapa de reconocimiento de cualquier ataque.

Además cumpliendo con la Arquitectura SAFE de Cisco se procedió a la implementación de un Firewall utilizando ENDIAN, distribución de código abierto de Linux, solución integral que ofrece todos los servicios de seguridad perimetral que brinda un UTM,

Figura 3.2 Interfaz gráfica FIREWALL ENDIAN

A continuación se muestra la captura de la configuración del firewall.



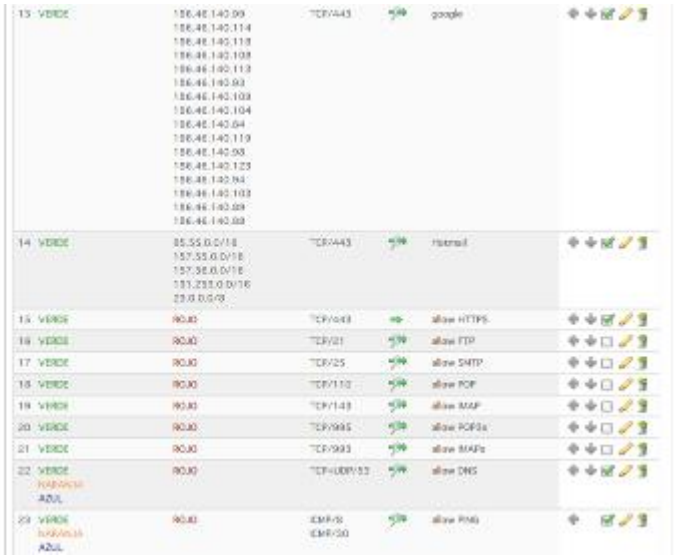


Figura 3.3 Configuración FIREWALL ENDIAN

CONCLUSIONES Y RECOMENDACIONES

Al finalizar el presente trabajo, luego de haber implementado un esquema de seguridad lógica para la Dirección Distrital de Salud de Ciudad del Sol, se concluye que:

1. Al realizar la aplicación de la Arquitectura SAFE de cisco en la Dirección Distrital, se estableció que la distribución de los equipos de red no era la adecuada para garantizar la seguridad de la red.

2. El crecimiento paulatino de usuarios de la Dirección Distrital, así como también la demanda de implementación de nuevos servicios género que se utilice para diferentes funciones un mismo equipo, a pesar de esto se ha realizado las configuraciones necesarias para que se garantice menor riesgo ante un ataque

3. Se requiere establecer revisiones periódicas a las configuraciones de los servidores que forman parte de los activos, así como realizar las actualizaciones de los Sistemas Operativos para de esta manera mitigar las probabilidades de ser víctimas de vulneración de seguridades.

4. La falta de conocimiento de la importancia de la seguridad de los activos ha generado pérdida parcial de la información (antiguo servidor de correo).

Al finalizar el presente trabajo, luego de haber implementado un esquema de seguridad lógica para la Dirección Distrital de Salud de Ciudad del Sol, se recomienda que:

1. En cuanto se cuente con presupuesto se realice la migración del Sistema FALCO hacia otro servidor, el mismo que deberá ser ubicado en la intranet.

2. Se realice la implementación de un Sistema de Gestión de la Seguridad de la Información para de esta manera garantizar que la Dirección se comprometa con la importancia de la seguridad de los activos de la institución.

3. Para garantizar la disponibilidad de los servicios que actualmente se requieren en la Dirección la adquisición de un generador de energía o un UPS de mayor capacidad ya que actualmente solo cuenta con un UPS que garantiza la continuidad por un lapso corto de tiempo.

4. Se realice capacitaciones continuas para los funcionarios de la Institución para que tengan conocimiento sobre la importancia de la seguridad de la información.

BIBLIOGRAFÍA

[1] ISO/IEC 17799:2005, Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información.

[2] ISO/IEC 27001:2011 Tecnología de la Información – Técnica de seguridad – Sistema de Gestión de la Seguridad de la Información (SGSI) – Requisitos.

[3] Astudillo Karina, *Hacking Ético* 101: Cómo hackear profesionalmente en 21 días o menos, 2013.

[4] Sean Convery, Bernie Trudel, Cisco SAFE: Un modelo de seguridad para las redes de las empresas, http://www.cisco.com/web/ES/assets/docs/safe_wp1.pdf, fecha de consulta julio 2015

[5] Políticas Uso de Servicios de Red y Servicios Informáticos del Ministerio de Salud Pública, http://instituciones.msp.gob.ec/somossalud/images/documentos/Pol%C3%ADticas_TICS.pdf,fecha de consulta julio 2015