UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ
EXTENSIÓN EN EL CARMEN
CARRERA DE INGENIERÍA EN SISTEMAS
Creada Ley No. 10 – Registro Oficial 313 de Noviembre 13 de 1985

PROYECTO DE INVESTIGACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS

Estudio de seguridad en redes para la información sanitaria en la "Dirección Distrital de Salud 13D05 El Carmen – zona 4."

Carlos Daniel Valdez Toral

Autor

A.S Jaime Zambrano Quiroz Mg.

Tutor

EL CARMEN, ENERO DEL 2020

DECLARACIÓN DE AUTORÍA

Quien suscribe el presente trabajo Valdez Toral Carlos Daniel con cedula de ciudadanía 172512081-8, estudiante de la Universidad Laica “Eloy Alfaro de Manabí “Extensión en El Carmen de la Carrera de Ingeniería en Sistemas, declaro que las opiniones, aportes, criterios y resultados me correspondan en su totalidad, cuyo tema es “Estudio de seguridad en redes para la información sanitaria en la “Dirección Distrital de Salud 13D05 el Carmen – zona 4.” Y de la misma manera los derechos patrimoniales a la Universidad Laica Eloy Alfaro de Manabí.

_____

Valdez Toral Carlos Daniel

172512081-8

CERTIFICACIÓN

En calidad de docente tutor(a) de la Extensión El Carmen, de la Universidad Laica "Eloy Alfaro" de Manabí, certifico:

Haber dirigido y revisado el trabajo de titulación, cumpliendo el total de 64 horas, bajo la modalidad de proyecto de investigación, cuyo tema del proyecto es **"Estudio de Seguridad en Redes para la Información Sanitara en la "Dirección Distrital de Salud 13D05 El Carmen- Zona 4"**, el mismo que ha sido desarrollado de acuerdo a los lineamientos internos de la modalidad en mención y en apego al cumplimiento de los requisitos exigidos por el Reglamento de Régimen Académico, por tal motivo CERTIFICO, que el mencionado proyecto reúne los méritos académicos, científicos y formales, suficientes para ser sometido a la evaluación del tribunal de titulación que designe la autoridad competente.

La autoría del tema desarrollado, corresponde al señor/señora/señorita **Valdez Toral Carlos Daniel,** estudiante de la carrera de Ingeniería en Sistemas, período académico 2019-2020(2), quien se encuentra apto para la sustentación de su trabajo de titulación.

Particular que certifico para los fines consiguientes, salvo disposición de Ley en contrario.

El Carmen, 8 de enero del 2020.

Lo certifico,

A.S. Javier Zambrano Quiroz, Mg.
Docente Tutor(a)
Área: Sistemas

16/01/2020
16h00

APROBACIÓN DE PROYECTO DE INVESTIGACIÓN

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ
EXTENSIÓN EN EL CARMEN
CARRERA DE INGENIERÍA EN SISTEMAS
Creada Ley No. 10 – Registro Oficial 313 de Noviembre 13 de 1985

APROBACIÓN DE PROYECTO DE INVESTIGACIÓN

Los miembros del tribunal examinador dan aprobado el informe del proyecto de investigación con el tema. **ESTUDIO DE SEGURIDAD EN REDES PARA LA INFORMACIÓN SANITARIA EN LA "DIRECCIÓN DISTRITAL DE SALUD 13D05 EL CARMEN- ZONA 4,** con autoría de Valdez Toral Carlos Daniel, estudiante de la carrera de Ingeniería en Sistemas.

El Carmen, 21 de febrero del 2020

Ing. Patricio Quiroz Msc.,
Tribunal I

Ing. Víctor García Peña Msc.,
Tribunal II

Ing. Diego Cáceres Msc
Tribunal III

DEDICATORIA

Dedico el esfuerzo de este trabajo a Dios siendo el pilar de la fe por el cual no nos rendimos y no desmayamos hasta cumplir con nuestro objetivo en todo momento y en todo lugar, a mis madres que siempre están en todo momento y de alguna u otra forma siempre están apoyándome, dándome ánimos para continuar en este camino como lo es la Educación Superior.

Carlos Valdez

AGRADECIMIENTO

Agradecerle en primer lugar a Dios por brindarme cada día un día más de vida, por permitirme llegar hasta donde estoy en este momento sano y salvo, a mis madres ya que son dos les agradezco infinitamente por estar en cada momento por siempre creer en mí y a la vez por sus sabias palabras que ayudaron a que siga adelante.

A mi tutor por saberme guiar, sugerir con su conocimiento con el objetivo de mejorar y poder culminar mi proyecto de titulación, a los demás ingenieros de esta prestigiosa institución quienes también brindaron su apoyo y conocimiento para resolver cualquier duda de este proyecto de titulación y de todo el periodo académico de esta carrera.

El Autor

ÍNDICE GENERAL

PORTADA I
DECLARACIÓN DE AUTORÍA II
CERTIFICACIÓN III
DEDICATORIA V
AGRADECIMIENTO VI
ÍNDICE GENERAL VII
ÍNDICE DE ILUSTRACIONES XIII
ÍNDICE DE CUADROS XIV
ÍNDICE DE ANEXOS XV
RESUMEN XVI
SUMMARY XVII
INTRODUCCIÓN 1
CAPÍTULO I 3
1 MARCO TEÓRICO 3
1.1 Seguridad en Redes 3
1.1.1 La seguridad en redes 3
1.1.2 Aspectos generales de la seguridad en redes 3
1.1.2.1 Amenazas externas 4
1.1.2.2 Amenazas Internas 4
1.1.3 Cortafuegos 4
1.1.3.1 Firewall de Redes 5
1.1.3.2 Firewall de Equipo 5
1.1.4 Listas de Control ACL 6
1.1.5 Redes Inalámbricas 6
1.1.5.1 Interferencias 7

1.1.6 Vulnerabilidades de los servicios en Red 7
1.1.7 Monitorización 8
1.1.7.1 Herramientas de monitorización.....9
1.1.7.2 Herramientas de seguridad de redes 9
1.1.8 Proxies 12
1.1.8.1 Gestión unificada de amenaza.....12
1.1.9 Zonas desmilitarizadas.....13
1.1.9.1 DMZ Dual.....13
1.1.9.2 DMZ de una sola pata.....14
1.1.10 Criptografía 14
1.1.10.1 Criptografía Simétrica.....15
1.1.10.2 Criptografía de claves Asimétricas 15
1.2 Información Sanitaria 16
1.2.1 La información sanitaria 16
1.2.2 Procesos de la obtención de la información 16
1.2.3 Información de la enfermedad y tratamiento.....17
1.2.4 Adaptación e individualización de la información.....18
1.2.4.1 Contenidos y manera de informar 19
1.2.5 Utilidad de la informacion sanitaria 19
1.2.5.1 Toma de decisiones.....19
1.2.5.2 Control 20
1.2.5.3 Seguridad 20
1.2.6 Participación de la familia en la información 20
1.2.6.1 Acompañar 20
1.2.6.2 Ayuda a tomar decisiones.....21
1.2.7 Información de los resultados de los hospitales.....21

1.2.7.1 Información del sistema 21
1.2.7.2 Registros.....22
1.2.7.3 Indicadores de seguridad y calidad clínica 22
1.2.8 Las arquitecturas de los sistemas sanitarios 22
1.2.8.1 Modelos de reembolso.....23
1.2.8.2 Modelos de contratos.....23
1.2.9 Condicionantes del modelo sanitario 23
1.2.10 Planificacion y gestion del modelo sanitario 24
1.2.10.1 Necesidad 24
1.2.10.2 Eficacia 24
CAPITULO II 25
2 DIAGNÓSTICO.....25
2.1 Método de Investigación 25
2.1.1 Cuantitativo 25
2.2 Enfoque de la investigación 25
2.2.1 Deductivo 25
2.2.2 Analítico- sintético 25
2.3 Tipos de investigación 26
2.3.1 Descriptiva.....26
2.4 Técnicas de investigación 26
2.4.1 Encuesta 26
2.4.2 Entrevista 26
2.5 Instrumentos de investigación.....27
2.5.1 Cuestionario 27
2.5.2 Guía de la entrevista 27
2.6 Validez de instrumentos.....27

2.7. Población y muestra 28
2.7.2. Muestra 28
2.8. Tablas y Grafos....28
2.8.1. Encuestas realizadas al personal del Distrito de Salud 13D05 de El Carmen. 28
2.9. Entrevista....34
2.10. Triangulación de los resultados 37
CAPITULO lll 38
3 PROPUESTA....38
3.1 Antecedentes....38
3.2 Misión 39
3.3 Visión....39
3.4 Objetivo de estudio 39
3.4.1 Objetivos Específicos 39
3.5 Informe de auditoría de la red del Distrito de Salud 13D05. 41
3.5.1 Objetivos 41
3.5.2 Personal relacionado....41
3.6 Controles de seguridad aplicados 41
3.6.1 Norma ISO/IEC 27033....41
3.6.1.1 Procesos de la norma ISO/IEC 27033 41
3.6.1.2 Controles sugeridos por la norma ISO/IEC 27033....42
3.6.2 Estándar IEEE 802.10 43
3.6.2.1 Procesos del Estándar 43
3.6.3 Alcance 43
3.1. Hallazgos 47

3.1.1. Cumplimiento general de las políticas sobre la seguridad en la red. 47

3.2. Análisis de gráficos por segmentos 48

3.2.1. Amenazas a la red y configuración de las herramientas. 48

3.2.2. La seguridad en la red y las medidas que se deben tener en cuenta en su ordenador. 50

3.2.3. Norma ISO/IEC 27033 y Estándar IEEE 802.10 51

3.3. Situación Actual 52

3.4. Características del Proyecto 52

3.4.1. Naturaleza del Proyecto 52

3.4.2. Importancia 52

3.4.3. Localización 52

3.5. Estudio técnico 52

3.5.1. Recursos Humanos 52

3.5.2. Recursos Tecnológicos 53

3.6. Factibilidad 54

3.6.1. Técnica 54

3.6.2. Operativa 54

3.6.3. Económica 54

3.6.4. Conclusión del estudio 55

4 Herramientas de seguridad para la red del Distrito de Salud 13D05. 56

4.1 Instalación de herramientas y comprobación de vulnerabilidades. 56

4.1.1 Instalación de Nmap y análisis de red 56

4.1.2 Ejecución y pruebas de Nessus 59

4.1.3 Tinywall 62

4.2 Resolución del estudio 64

4.3 Resultados obtenidos 64
4.3.1 Mecanismos utilizados para la seguridad 64
4.3.2 Creación de usuarios y contraseñas.....65
4.3.3 Pruebas de bloqueo y protección con TinyWall 65
4.3.4 Análisis de las herramientas utilizadas para la protección de la red de datos del Distrito 13D05 El Carmen. 67
5 CONCLUSIONES 68
6 RECOMENDACIONES.....69
7 Bibliografía.....70
8 ANEXOS.....74

ÍNDICE DE ILUSTRACIONES

Ilustración 1 DMZ DUAL 14
Ilustración 2 DMZ de una sola 14
Ilustración 3 tabulación de resultados generales de la Auditoria 46
Ilustración 4resultados generales.....47
Ilustración porcentaje 5 de resultados generales 47
Ilustración 6 tabulación de amenazas a la red 48
Ilustración 7 porcentaje de amenazas a la red 49
Ilustración 8 seguridad en la red 50
Ilustración 9 norma ISO 51
Ilustración 10 porcentaje de Norma y Estándar.....51
Ilustración 11 instalación de Nmap 56
Ilustración 12 finalización de Nmap.....56
Ilustración 13 análisis de la IP.....57
Ilustración 14 escaneo de Host 57
Ilustración 15 detección de sistema 58
Ilustración 16 Puertos y servidores 58
Ilustración 17 resultados de la IP 58
Ilustración 18 topología 58
Ilustración 19 Puertos abiertos.....59
Ilustración 20 descarga de Nessus 59
Ilustración 21 registro en Nessus 60
Ilustración 22 Selección de opciones 60
Ilustración 23 Detección de Malware 61
Ilustración 24 Análisis de Bloqueo 61
Ilustración 25 iniciamos la instalación 62

Ilustración 26 servicios de aplicaciones 62
Ilustración 27 modos de acceso.....63
Ilustración 28 detección de aplicaciones.....63
Ilustración 29 creación de administrador y contraseña.....65
Ilustración 30 cambio de modo a administrador 65
Ilustración 31 protección de páginas con malwares 66
Ilustración 32 bloqueo de aplicaciones.....66
Ilustración 33 comprobación de bloqueo de aplicación 67
Ilustración 34 matriz de la encuesta.....80

ÍNDICE DE CUADROS

Tabla 1 Tabulación de encuesta 33
Tabla 2 Tabulación de entrevista 36
Tabla 3 Parámetros de Seguridad de la Norma ISO/IEC 2703 43
Tabla 4 recursos Humanos 52
Tabla 5 Recursos Tecnológicos.....53

ÍNDICE DE ANEXOS

anexo 1 Asignación de Tutor 74

anexo 2 Certificado de Auditoría 75

anexo 3 Resultados de URKUND 76

anexo 4 Encuesta 78

anexo 5 Entrevista 82

anexo 6 Ficha aplicada en la Auditoria bajo la norma ISO/IEC 27033 84

Anexo 7 resolución de entrevista 85

Anexo 8 revisión de entrevista 85

Anexo 9 pruebas de Nmap y Nessus 85

Anexo 10 instalación de Nessus y Nmap 85

Anexo 11 ejecución de herramientas de protección Autor: Carlos Valdez.....85

Anexo 12 análisis de la red 85

Anexo 13 Análisis y protección en Talento Humano Autor: Carlos Valdez 85

Anexo 14 Instalación de herramientas en el dpto. Talento Humano.....85

RESUMEN

La seguridad en redes se ha convertido en un factor de suma importancia debido a la presencia constante de intrusos en la red ya que son elementos que afectan la calidad de servicio por lo que es de vital importancia proteger los equipos de las vulnerabilidades y afecciones que se ven expuestos los usuarios día a día, ya sea por la falta de conocimiento de herramientas que permiten analizar y proteger la información de diferentes tipos de ataques, y que a medida que la tecnología va a avanzando se crean nuevos métodos de penetración y hackeo de redes aprovechándose de las vulnerabilidades de una red sin protección. Con estos antecedentes, el objetivo de la presente investigación fue realizar un estudio de seguridad en redes para la información sanitaria en la "Dirección Distrital de Salud 13D05 El Carmen – zona 4."

Se realizó una investigación cuantitativa, con un enfoque deductivo y analítico sintético, el tipo de investigación utilizada fue el descriptivo. Para la recolección de información se utilizó las técnicas de la encuesta y entrevista información que sirvió para determinar la aplicabilidad de las herramientas de seguridad de redes en el presente estudio. La población objeto de estudio fueron los empleados del Distrito de Salud 13D05, cuya muestra fue de 20 empleados. Se realizó una entrevista al responsable del Departamento de TIC. Resultado de la presente investigación fue un informe de auditoría sobre la seguridad en la red, la misma que determinó el uso de herramientas que tendrán como objetivo el proteger la red del Distrito de Salud 13D05.

SUMMARY

The Security in networks has become a very important factor due to the constant presence of intruders in the network as they are elements that affect the quality of service so it is of vital importance to protect computers from vulnerabilities and conditions that are exposed to users every day, either by the lack of knowledge of tools that can analyze and protect information from different types of attacks, and that as technology advances new methods of penetration and network hacking are created taking advantage of the vulnerabilities of an unprotected network. With this background, the objective of the present investigation was to carry out a network security study for health information in the "Dirección Distrital de Salud 13D05 El Carmen - zona 4.

Regarding the method used in the present investigation, we will find the quantitative one, with a deductive and analytical synthetic approach, the type of research used was the descriptive one. For the collection of information, the techniques of the survey and information interview were used to determine the applicability of the network security tools in the present study. The population under study was the employees of the 13D05 Health District, whose sample was 20 employees. An interview was conducted with the head of the TIC Department. The result of the present investigation was an auditory report on network security, which determined the use of tools that will have the objective of protecting the network of the 13D05 Healthcare District.

INTRODUCCIÓN

En la actualidad el crecimiento de redes y la cantidad de información disponible en estás ha llegado a ser casi ilimitada a nivel mundial, dando como resultado a ser inseguras debido a que cualquier usuario que tenga acceso a internet puede obtener información acerca de las vulnerabilidades las mismas que se encuentran con mayor facilidad; los usuarios de las redes van ganando cada vez más experiencia, provocando así que más personas las conozcan, volviéndose cada vez más inseguras y por lo tanto muy vulnerables a ataques y robos de información o dejar temporalmente inhabilitada la red que ha sido afectada.

En el Ecuador las empresas, organizaciones y cualquier persona que utiliza una computadora envía y recibe correos electrónicos, comparte información de manera local o fuera de este, realiza transacciones, ofrece servicios y encuentra soluciones de acuerdo a sus necesidades. Es así que la información se vuelve algo muy preciado tanto para los usuarios como para los Hackers. Es por eso que se utilizan mecanismos de seguridad o herramientas como Nessus que cuenta con un estándar a nivel nacional y mundial para la prevención de ataques de red, identificación de vulnerabilidades y detección de problemas de configuración que utilizan los hackers para entrar en la red con el objetivo de brindar mayor seguridad en la red evitando así que alguien no deseado filtre información.

El presente estudio de seguridad está enfocado a la red del Distrito de salud 13D05 con el fin de detectar los problemas acerca de las vulnerabilidades de redes, tiene como objetivo proponer varias soluciones o herramientas de acuerdo a los resultados obtenidos para fortalecer la seguridad de la red, enfocando su estudio a los equipos con los que se trabaja, los sistemas operativos y programas, aplicar en base a las pruebas realizadas de detección de amenazas y análisis, información que sirvió para la respectiva documentación en base a la propuesta que nos permitirá la detección y prevención de problemas de seguridad a corto y largo.

En el presente trabajo se dará a conocer la importancia de la seguridad en las redes por lo que se realiza dicho estudio el cual tiene como objetivo proteger la información de las amenazas que existen en las redes, el mantener los datos libres de cualquier tipo de ataque y de la misma manera resguardar la información que se transmita dentro del Distrito de Salud 13D05, mediante la instalación de herramientas de seguridad en redes las mismas que se encargan del análisis y protección de la red, por lo que se presenta una auditoria en base la norma ISO/IEC 27033 la misma que se utilizó los parámetros de seguridad que esta ofrece.

El método a utilizar en esta investigación es el cuantitativo, con un enfoque deductivo los mismos que ayudaran a la deducción de los problemas de seguridad que se encuentren en el estudio y el analítico que será aplicado para la revisión y distinción los elementos encontrados, el tipo de investigación utilizada fue el descriptivo el mismo que se utiliza para describir el problema al cual se quiere darle solución. Para la recolección de información se utilizó las técnicas de la encuesta y entrevista información que sirvió para determinar la aplicabilidad de las herramientas de seguridad de redes en el presente estudio, la muestra será discrecional por lo que no será necesario aplicar la técnica de muestreo, se han considerado 3 herramientas de prevención y seguridad para redes, la técnica a utilizar es la encuesta la que se va a aplicar a los 20 empleados del Distrito de Salud 13D05 y la entrevista al encargado del departamento de TIC.

CAPÍTULO I

1 MARCO TEÓRICO

1.1 Seguridad en Redes

1.1.1 La seguridad en redes

La seguridad en redes es de lo cual muchas empresas y organizaciones se preocupan en la actualidad, el mantener la información libre de cualquier tipo de ataque y de la misma manera proteger los recursos de dicha empresa u organizaciones, En términos generales, la seguridad puede entenderse como aquellas reglas técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial. Es muy importante citar que la seguridad informática es parte tanto de las empresas, instituciones o compañías así también como de sus miembros o usuarios, para lo cual, si se habla de seguridad informática, se debe tener responsabilidad y dar el conocimiento oportuno respecto de todas las normas y políticas de seguridad, como grupo. (Stallings, 2014)

1.1.2 Aspectos generales de la seguridad en redes

En muchos casos la perdida de información o robo de datos suelen ser de alto costo para la empresa internamente debido a los percances o daños de información que suelen ser de uso privado, tanto de la empresa como también de los altos miembros que la conforman dejándolos vulnerables a un acoso o amenaza por parte de los delincuentes informáticos. (Costas, 2014)

Los conocidos como hackers o intrusos expertos en vulnerar las redes suelen obtener acceso al ordenador por las vías y métodos sencillos o sofisticados que comprometen el software y hardware convirtiéndolos en vulnerables, donde muchos usuarios suelen registrarse con sus datos personales tanto como nombres y sus contraseñas siendo estas fáciles de acceder permitiéndoles a los piratas informáticos obtener datos e información sumamente valiosa para la empresa como para los usuarios de la red. (Moguel, 2005)

1.1.2.1 Amenazas externas

Este tipo de amenazas son las que a diario muchas entidades u organizaciones se ven afectadas debido a que muchas personas sin autorización pueden acceder a la red o al sistema mediante enlaces engañosos o formularios que piden ingresar datos personales y empresariales. (Arantes, 2015)

1.1.2.2 Amenazas Internas

Las vulnerabilidades internas son las más comunes en cualquier organización debido a que las personas que manipulan la red conocen la información o los datos privados pertenecientes a dicha organización. En muchos casos también se da que las personas sin tener el conocimiento llegan a insertar cualquier tipo de virus transfiriéndolo desde fuera de la organización, por lo que afectaría directamente a afectar la red interna , esta es una de las mayores amenazas que las empresas se ven considerablemente afectadas y una de las que menos se tiene precaución, muchas organizaciones suelen invertir cantidades considerables de dinero en seguridad externa cuando la mayoría de la sustracción de información se la da por la ingeniería social. (Costas, 2014)

1.1.3 Cortafuegos

Es más conocido como firewall ya que su nombre se identifica como un componente de protección fundamental en los sistemas operativos y redes aun así este mecanismo no es lo suficiente como para poder tener protegidas toda la red, como también los equipos que se encuentran conectados en ella. (Alonso, 2013)

Lo recomendable para una red de ordenadores es contar con un cortafuegos de esta manera evitara el acceso no autorizado a la red local rechazando oportunamente el intento de ingreso a la información privada, en varios casos existen dispositivos de red como los Router´s que cuentan con este particular mecanismo de cortafuegos, un cortafuego analiza el tráfico por completo de una red todo lo que entra y sale a la vez de esta ya que este se encuentra en el límite de la red. (Gonzales, 2014)

1.1.3.1 Firewall de Redes

El firewall de red ofrece componentes de control de datos entre la red que accede al Router o cualquier dispositivo que funcione como el control del tráfico de la red, protegiéndola de cualquier persona o malwares maliciosos impidiéndoles que estos se puedan colar en la red y de esta forma evitar el robo de información. (Gonzales, 2014)

1.1.3.1.1 Tinywall

Es una herramienta de cortafuego intuitivo, con una interfaz amigable con el usuario, protección instantánea, sin avisos molestosos en ventanas emergentes, además incluye una serie de combinaciones de características que lo diferencia de los demás firewall gratis y comerciales. (Costas, 2014)

Características fundamentales de Tinywall

- Tinywall no molesta al momento de estar trabajando con ventanas emergentes como otros firewalls, lo que lo convierte en una herramienta fácil de manejar y agregar excepciones al firewall.
- Tinywall bloquea en tiempo real cientos de virus, troyanos y gusanos, no requiere conocimiento de puertos y protocolos.
- Tinywall evita generalmente que esos programas maliciosos en la red modifiquen o dañen archivos como también el firewall del Sistema Operativo.

1.1.3.2 Firewall de Equipo

Este ámbito está referido a la función de firewall implementada en un computador y que tiene como finalidad aplicar los módulos de control en los datos intercambiados entre el equipo y la red. (Costas, 2014)

Este tipo de firewall es el más conocido por todos los usuarios que tienen acceso a un ordenador, el análisis que realiza el firewall tiene como finalidad inspeccionar y comprobar las normas de seguridad entre un equipo u ordenador con la red. Entre las reglas más comunes se conoce como la selección de puertos la que les permite el paso de datos a una serie de puertos respectivo a la información que se esté enviando o receptando, se lo

conoce también como un proceso de reconocimiento denominado filtrado el cual cumple con la tarea de dejar pasar dicha información o rechazarla. (Musser, 2017)

1.1.4 Listas de Control ACL

A través de la interfaz del Router´s se crean estas listas de condiciones siendo las condiciones que viajan a través de este por su interfaz, se crean dependiendo del protocolo o el puerto al que se le va a filtrar. Las listas de acceso se crean necesariamente para que el Router´s pueda detectar que paquetes este pueda aceptar sin tener ningún inconveniente con toda la información que viaja a través de la red, de la misma saber que paquetes de datos este pueda rechazar ya sea en la entrada de la interfaz lo que limitaría de cierta manera el tráfico en la red mejorando el rendimiento de la misma (Gasco, 2015)

En los tipos de ACL encontramos las conocidas como estándar donde solo se tiene que especificar la dirección de origen es decir la dirección IP o de host, rango de direcciones, de la misma manera denegando y permitiendo el acceso a la red configurándola en modo global asiéndose la asignación a la interfaz de red que corresponda. Las ACL extendida son las direcciones de origen y destino, son más comunes por lo tanto son las más utilizadas ofreciendo un control mayor que la estándar porque verifican las direcciones tanto de origen como también la de destino los protocolos y números de puertos. (Costas, 2014)

1.1.5 Redes Inalámbricas

Hoy en día es muy usual y/o común el uso de las redes inalámbricas en el mundo, en la mayoría de los casos se utiliza en los dispositivos móviles los cuales son hechos necesariamente para este tipo de redes, con el avance de la tecnología existen un sin número de dispositivos que ya cuentan con acceso a redes inalámbricas como el internet de las cosas, también nos encontramos con los puntos que de acceso que controlan el acceso, las tarjetas Wireless que permiten la conexión de las computadoras personales tanto internas como externas. (Costas, 2014)

Los cables que suelen utilizar para construir lo que conocemos como redes locales son los más comunes conocidos como el cable coaxial, la fibra óptica

entre otros, en la actualidad las nuevas edificaciones de grandes empresas que son construidas se les realiza la instalación en el proceso de construcción evitando el gasto de recursos económicos, el daño de algún dispositivo o del mismo cableado a utilizarse en el proceso de instalación evitando así a futuro una serie de gastos innecesarios para la empresa. (Costas, 2014)

1.1.5.1 Interferencias

Las interferencias más comunes que se conocen hoy en día son generadas por ruidos de maquinarias pesadas, por radios o las ondas que estas producen las que ocasionan distorsión de la red. Por esta razón actualmente las operadoras de red ofrecen internet por medio de fibra óptica ya que estas no sufren ningún problema de alteración de datos que viajan a través de este asiéndolos como el medio de transmisión más seguro de internet. En las organizaciones siempre se suelen ver más estos casos de los cuales se suelen aprovechar ciertas personas maliciosas con el fin de obtener beneficio proprio perjudicando a la empresa. (Salvador, 2014)

1.1.6 Vulnerabilidades de los servicios en Red

La comunicación es de fácil uso y libre a la vez de la manera en que cada usuario es libre de usarla de acuerdo a sus necesidades, puede ser para comunicarse con seres queridos desde el otro lado del continente, para jugar un juego online y hasta para gestionar el trabajo haciéndolo de manera más fácil, pero estas comunicaciones siempre van a estar expuestas a los riesgos de conexión o inseguridad en la red, es por esto que se basan las redes en el modelo OSI con cada una de sus capas definidas en orden de manera que cada una cumplen con sus funciones asignadas. (Gómez, 2013)

La redes de comunicación que se usan a diario como medio de comunicación se basan en el funcionamiento en un modelo de conocido como el modelo OSI el cual es el modelo de interconexión de todos y cada uno de los equipos de comunicación, este modelo está definido en siete capas u niveles siendo cada nivel definido para la comunicación mediante una interfaz la que está diseñada precisamente para facilitar la comunicación por cada uno de los niveles desde inferior o superior de los cuales está compuesto el modelo ya mencionado, aun

así existen vulnerabilidades en cada uno de estos niveles las cuales si no se tiene el debido cuidado o precaución serán las puertas para que cualquier atacante se aproveche de esas vulnerabilidades adquiriendo información personal o empresarial. (Gasco, 2015)

1.1.7 Monitorización

La monitorización es fundamental realizarla en cada red que se encuentre operando ya que no importa que se tenga el mejor hardware si la red está fallando debido a las amenazas que la afectan, esta permite también identificar si se está haciendo el uso correcto del consumo del ancho de banda. El monitoreo es primordial en las redes informáticas debido a los cambios que tienen que enfrentarse con el pasar de los días, en esos cambios se encuentran principalmente debido a que los usuarios quienes interactúan en los diferentes dispositivos se encuentran navegando, enviando información a través de las redes sociales o correos, descargando cualquier tipo de información en los ordenadores los cuales los hace vulnerables a ciertas amenazas que no se pueden detectar a simple vista. (Costas, 2014)

El que una red funcione de maravilla brindando un excelente servicio al principio de su instalación, con el tiempo que a medida que pasen estos le afectaran de cierta forma perjudicando de cierta forma la vida útil de la red como la de los equipos con los que trabaje dicha red, en ciertas ocasiones uno de los principales causantes de estas afecciones suelen ser los conocidos Malware maliciosos que afectan al ordenador con muchas finalidades, una de ellas es la extracción de información personal, cuentas, dinero, etc. de forma ilegal de la misma forma ocasionar una colisión en la red. (Gasco, 2015)

La utilización de nuevas aplicaciones en la red o la cantidad de usuarios son perjudicialmente para la red, partes del hardware cuando estos se encuentran en estados defectuosos por lo tanto no solo basta una implementación de red con la mejor tecnología de punta, como requisito se debe monitorear y proteger la red de estas amenazas con las herramientas adecuadas se podrá corregir estos problemas a los que se encuentran expuestas las redes. (Martínez, 2014)

- **Port mirroring**. Conocido como método de monitoreo el cual consiste en la configuración de dispositivos quienes son los conductores de toda la información que pasa por la red.
- **Network tap.** Es una forma diferente a la anterior con este método se utiliza un dispositivo que accede a todo el tráfico de la red que le llega al dispositivo para así poderlos analizar de la mejor manera.

1.1.7.1 Herramientas de monitorización

En el mercado actual existen muchas herramientas de monitoreo creadas con el fin de monitorear y examinar las redes libres o comerciales, estas herramientas fueron creadas debido a las vulnerabilidades que una red está expuesta ya sea por la falta de cuidado o el poco conocimiento de lugares maliciosos que se aprovechan de dichas vulnerabilidades, las publicidades engañosas que no son más virus o Malware acortando la vida útil de la red de datos, cabe mencionar algunas de las herramientas de monitoreo a continuación : Wireshark, Ntop, Nagios, PandoraFMS, Zabbix, Ettercap. Etc. (Gasco, 2015)

1.1.7.2 Herramientas de seguridad de redes

La red esta una gran parte expuesta a muchas vulnerabilidades de seguridad de software, sean aplicaciones o software, de cierta forma esto incita a la creación de nuevos virus, malware, worm, que son los más comunes y los cuales se aprovechan de ciertas vulnerabilidades en la red, por esta razón se han desarrollado ciertas herramientas de seguridad de redes las cuales se encargan de la protección de la misma ante las amenazas ya mencionadas algunas de estas herramientas pueden ser: (Orueta, 2014)

1.1.7.2.1 Nmap

Es una herramienta muy conocida por ser Open Source (código abierto) permite escanear los puertos de las redes, realiza auditorias de seguridad, detecta que versión y que tipo de sistema operativo usan los hosts, corta fuego muy útil a la hora de realizar actualizaciones de servicios, el inventario de las redes calcula en tiempo en el que el host estuvo activo, este además utiliza direcciones IP como paquetes los que ayudan a determinar que host están disponibles. (Costas, 2014)

1.1.7.2.1.1 Características de Nmap

Su propósito principal de esta maravillosa herramienta Nmap es que la red de todos al momento de navegar o interactuar en ella, brindando seguridad tanto para usuarios como los administradores de las redes, a los auditores para estar alerta ante las amenazas que a diario se ven amenazada las redes, está disponible para cualquier sistema Operativo es gratuito en la actualidad trae como ayuda para los usuarios la modalidad de poder modificar el código fuente según los términos de sus políticas de esta forma poder redistribuirlos. (Orueta, 2014)

- **Flexible. -** se la conoce como flexible por que admite ciertas metodologías actualizadas para analizar y proteger redes con IP´S llenas de filtros, enrutadores, firewalls, host entre otros. Por lo que contiene muchos componentes de escaneo de puertos, descubrimiento de Sistema Operativo y sus versiones, limpiezas etc.
- **Compatibilidad. -** Es el más utilizado para el escaneo de grandes redes las cuales cuentan con un sinnúmero de ordenadores, es compatible con la mayoría de los Sistemas Operativos, entre los más conocidos están: Microsoft Windows, Linux, Solaris, Sun OS etc.
- **Popular. –** es una de las herramientas más descargadas diariamente en las diferentes versiones de los sistemas Operativos que se encuentra disponible, siendo su objetivo principal ayudar a que al navegar se tenga mayor seguridad.

1.1.7.2.2 Nessus

Es una herramienta muy versátil de excelente rendimiento cuenta con un potente escáner el cual le permite poder realizar una examinación completa con el objetivo de proteger el sistema, detectando todas y cada una de las vulnerabilidades del sistema evitando daños en la red o infecciones en la misma. (Stallings, 2014)

Las características con las que más se la conoce a Nessus son:

- **Análisis en profundidad.** La herramienta Nessus analiza a una velocidad extremadamente alta por encima de cada programa examinado. Una de sus grandes ventajas es que se pueden lanzar varios tipos scanner en las diferentes redes de dicha organización. Otra ventaja es que se puede insertar un sin número de direcciones IP porque no tiene limitaciones siendo capaz de utilizar DNS en caso de que las direcciones IP sean dinámicas, puede completar una auditoria en la red con 100 host en poco tiempo. (Alvira, 2011)
- **Auditoria de dispositivos móviles.** Esta característica se aplica o se integra con Apple Pro-file Manager y con Microsoft Exchange como directorio activo, con el propósito de detectar aquellas vulnerabilidades de la empresa como también el estado en el que se encuentran los dispositivos. (Costas, 2014)
- **Auditorias antivirus, de botnets y procesos maliciosos.** tiene la capacidad de detectar procesos en tiempo real dañinos para los ordenadores con cualquier Sistema Operativo, ayudando a mejorar la eficiencia del antivirus, analizando y estudiando las amenazas encontradas las que pueden ser APTS (Amenaza Persistente Avanzada). Buscando amenazas e identificándolas todas aquellas amenazas que ponen en riesgo la red infecciones conocidas como botnets y los servidores Web con contenidos infectados con contenido malicioso. (Gasco, 2015)
- **Integración de parches de seguridad.** Nessus cuenta con productos típicos de gestión como de actualizaciones como el Gerente de Punto Final Tivoli (TEM) o el Windows Server Update Services (WSUS). (Orueta, 2014)

1.1.7.2.3 John the Ripper

Es un software muy eficaz de acuerdo para lo que lo necesitemos ya sea para la protección de ciertas amenazas o para realizar algún tipo de ataque en alguna red.

1.1.8 Proxies

Este tipo de servicio es de los más usuales por cada y para cada usuario que navegan a diario en la red, como lo es un proxy web que son los que se encuentran en el modelo OSI, su uso habitual es permitir la conexión o acceso a internet en los ordenadores de las organizaciones ofreciendo una capa de seguridad a los clientes que se conecten a la red, ya que se encarga de realizar las peticiones de los clientes y es el encargado de realizar las comunicaciones dando como resultado la petición realizada. (Gascó & Serrano, 2015)

En la mayoría de los temas se ha visto al proxy como un dispositivo el cual sirve para ocultarse sin poder ser detectado razón por la cual la mayoría de hackers los utilizan para la obtención de información beneficiándose así mismo o a quien los contrato, además permiten los proxies son los que permiten el acceso a la red de redes a cada uno de los diferentes equipos que se encuentren conectados cuando en si solo se puede conectar el proxy, siendo el principal conector entre la red y los equipos que desee acceder a la red lo que permite a la vez proporcionar una capa de seguridad con el objetivo de proteger la conexión a la red. (Orueta, 2014)

La capa de seguridad de las proxies es fundamental en la comunicación porque cuando un dispositivo o equipo en una estación de trabajo desea quiera acceder a los equipos que contienen la información que deseen buscar es en base al proxi que se realiza dicha conexión y una vez realizado el pedido se envía la información solicitada. (Costas, 2014)

1.1.8.1 Gestión unificada de amenaza

En la actualidad existen una gran cantidad de dispositivos de seguridad los cuales se los conoce como UTM (Gestión Unificada de Amenazas) estos dispositivos combinan varias metodologías de protección de redes como por ejemplo, antivirus, antispam, cortafuegos, la protección a redes privadas de curiosos etc., todos y cada uno de estas metodologías de protección en un solo dispositivo. (Urbina, 2016)

Es por este motivo que la mayoría de los usurarios optan por estos dispositivos en pequeña, grandes y medianas empresas son los más utilizados por su facilidad de uso y protección que estos brindan, sobre todo en varias empresas donde no se puede invertir en softwares de seguridad debido a sus altos costos y tiempo de desarrollo. Así como tiene sus ventajas de la misma manera tiene sus desventajas, el hecho de que tenga varios sistemas de seguridad no significa que sean siempre eficaces, suelen presentarse ocasiones donde habrá dificultades de rendimiento, si llega a fallar el dispositivo todos los sistemas de protección fallaran dejando a la red vulnerable. (Gasco, 2015)

1.1.9 Zonas desmilitarizadas

Las zonas desmilitarizadas permiten a la red interna como la externa conectarse mediante estas zonas siendo estas las que actúan como intermediarias de las empresas y las red del exterior, pero estas solo acceden a establecer conexión con la red externa prohibiendo conexiones entrantes a la red interna, de esta forma la DMZ puede iniciar conexiones con dispositivos o equipos de red externos, debido a que es el nivel de seguridad es bajo la DMZ no permite estas conexiones internas. (Costas, 2014)

Las zonas desmilitarizadas tienen como objetivo permitir la conexión solo con la red externa como su principal función prohibiéndole la entrada a la red interna, pero la red puede establecer conexión ya sea interna o externa. (Gómez, 2013)

1.1.9.1 DMZ Dual

Es una de las configuraciones más utilizadas debido a que es una de las que cuentan con mayor seguridad de cortafuegos. Las DMZ o Zonas Desmilitarizadas dual cuentan con dos cortafuegos un interno y un externo, el interno es el que interactúa o se encuentra en medio de quienes manipulan los ordenadores en este caso lo usuarios como también de los servidores, el cortafuego exterior es todo lo contrario como su nombre lo indica este se encuentra en la parte externa de la red y de los servidores , se la conoce por la más segura por la seguridad que brinda a las empresas si un delincuente informático accede a la DMZ este no tendrá acceso a los usuarios por que se encuentran protegidos por los cortafuegos, en caso que llegue a fallar alguno de

estos cortafuegos la red no quedaría vulnerable ante ninguna amenaza. (Toro, 2015)

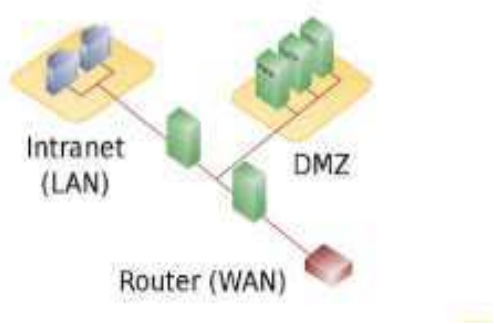


Ilustración 1 DMZ DUAL

Autor: Jiménez y Toro

1.1.9.2 DMZ de una sola pata

Las zonas desmilitarizadas de una sola pata se las conoce por ser una de las configuraciones de un inferior precio a diferencia de otras, debido a que en estas DMZ se realiza una separación de los servidores como también de los usuarios, encontrándose el cortafuego en medio de las tres zonas: servidores, usuarios y la red, en este caso se crea una capa que separa a los servidores de las demás zonas de manera que para que los usuarios puedan acceder a internet o a los servidores deben primero pasar por el cortafuego , por lo tanto si el único cortafuego llega a fallar la red por completa quedara totalmente expuesta a amenazas. (Toro, 2015)

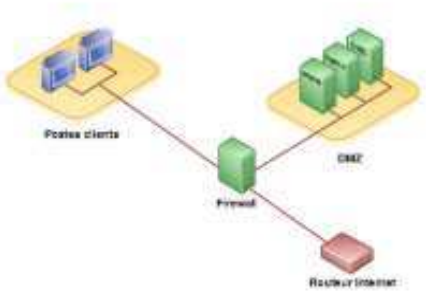


Ilustración 2 DMZ de una sola

Toro: Jiménez y Toro

1.1.10 Criptografía

La criptografía son métodos de protección de datos para grandes organizaciones con el fin de no ser manipuladas, a ese método de transformación se le conoce como inteligible y cifrado, un mensaje cifrado consta de una clave el cual solo

puede tener acceso el emisor y el receptor a quien va dirigido el mensaje, además en la criptografía se encuentran métodos como la autenticación que no es más que la comprobación de la identidad de quien envía el mensaje. (Santos, 2014)

1.1.10.1 Criptografía Simétrica

Este tipo de cifrado es uno de los más comunes usados por los usuarios su método de cifrar es un tanto sencillo brindando facilidad tanto para el emisor como para el receptor porque con la misma clave que se cifra se puede descifrar el mensaje sin necesidad de utilizar otros métodos, simplemente se le envía la clave al destinatario y este una vez que llegue el mensaje cifrado insertara la misma clave con la que fue cifrado el mensaje lo descifrará automáticamente. (Alonso, 2013)

Este tipo de cifrado por muy sencillo que parezca tiene sus contras o vulnerabilidades debido a que como se mencionó antes para poder descifrar el archivo es necesario enviar la clave del cifrado al receptor y mediante el envío cualquier atacante se puede aprovechar obteniendo la clave o unas posibles combinaciones que le ayudarían a descifrar más rápido la clave. (Costas, 2014)

1.1.10.2 Criptografía de claves Asimétricas

Este tipo de criptografía se divide en diferentes tipos de claves:

- Clave privada: este tipo de clave solo es conocida por su creador y solo él será quien sepa siendo el único a la vez que lo puede descifrar.
- Clave pública: como su nombre lo indica es conocida de manera pública por todos los usuarios.

Son los tipos de claves más comunes siendo el caso que si una cifra solo puede ser descifrada por la siguiente repitiéndose de forma como un bug, este tipo de clave se sacan la mayoría con los métodos matemáticos, a diferencia de las claves públicas que se pueden obtener mediante los números primos lo cual resulta bastante complicada de obtener. (Santos, 2014)

1.2 Información Sanitaria

1.2.1 La información sanitaria

La información sanitaria es la que se trasfiere comenzando con la administración y los expertos a los interesados o usuarios. Esta información contiene contenidos de motivo epidémico, de salud pública, acciones preventivas las cuales son necesarias anticiparlas antes de que cumplan su ciclo, los procesos de asistencia de cada departamento, el tener acceso tanto de servicios y dispositivos asistenciales los cuales son de utilidad. Los Sistemas de Información Sanitaria (SIS) son las herramientas de las que dispone la administración sanitaria para conocer los problemas de salud de la población, sus determinantes, y para la correcta toma de decisiones eficientes en la protección y mejora de la salud y en el control de las enfermedades en nuestra población. La calidad de la asistencia sanitaria o la eficacia de la planificación sanitaria y la formulación de políticas dependen de la disponibilidad de información precisa y oportuna para apoyar la toma de decisiones. (Vallés, 2014)

1.2.2 Procesos de la obtención de la información

La información es lo principal para cada usuario o paciente al momento de recibir cualquier tipo de noticia respecto algún problema de salud el cual tenga que afrontar, el comportamiento que tomen estos después de recibir la información inesperada así como también la de sus familiares o más allegados siendo esto un cambio en la rutina o vida acostumbrados a llevar, es por este motivo que la información sanitaria debe ser dada solo por personal profesional. (Grifols, 2014)

En la actualidad existen una gran cantidad que justifica el por qué es necesaria la información sanitaria, desde el comienzo se puede notar la importancia que tiene el principio bioético que no son más que la manera o se desenvuelve cada ser humano y todos los seres vivos en el ambiente al cual deben adaptarse, cabe destacar la importancia de los Derechos Humanos, la salud es lo importante en cada ser vivo por lo tanto es necesario la participación de la persona afectada, de esta manera es de suma importancia tener un mayor conocimiento sobre todas las afecciones de las condiciones de salud las cuales van a afectar a diario en la vida cotidiana, los cambios a los cuales tendrá que adaptarse debido a que

la condición de salud no le permitiría seguir viviendo con normalidad o como el individuo lo hacía antes de sufrir cualquier tipo de enfermedad, por este motivo es necesario que cada ser humano debe recibir clases de formación continua. Con el propósito de vincularlos con el medio mediante programas de capacitaciones y formaciones como también deberá recibir apoyo con el objetivo de mejorar la calidad de vida tanto psicológico como físico, una enfermedad no es fácil llevarla a diario muchas personas suelen renunciar a la vida debido a estas afecciones de la salud más aún cuando las enfermedades no tienen cura como cáncer, sida, enfermedades del corazón las cuales se tratan mediante tratamientos a largo plazo por lo que no es fácil sobre llevarlas con la vida diaria a la que estaban acostumbrados anteriormente. (Andrés, 2014)

Por este motivo que es fundamental para cada individuo aprender a entender la información sanitaria en lo más posible que sea y de la misma manera el tomar decisiones; los profesionales quienes están a cargo de dicha información tienen que saber dar una información concreta porque esta será utilizada en todos los casos de las diferentes enfermedades que se presenten. (Grifols, 2014)

1.2.3 Información de la enfermedad y tratamiento

Cada ciudadano o usuario tiene por derecho conocer acerca de la información sanitaria ya sea esta verídica o alterada por ética profesional, aunque parezca algo tan obvio sin que el usuario pueda darse cuenta de lo que se le puede venir o de lo que en verdad le puede llegar a suceder en su salud. Sin duda darle una noticia que afectará a la situación y la calidad de vida siendo esta la que se verá afectada totalmente, no es nada fácil darle una noticia a un desconocido por lo que muchos médicos o quienes dan el parte médico deben ser siempre profesionales ante una noticia de tal magnitud, esta no debe afectarlo ante el paciente. (Grifols, 2014)

El conocimiento que tienen los que están a cargo del paciente lo ayudaran a este a determinar un diagnóstico previo a lo que podría ocurrir con este y de alguna u otra forma se determinara la relación de cómo se llevara a cabo todo el proceso siguiente. En base a todos estos procesos se hace posteriormente un levantamiento de información de como se ha obtenido el proceso desde un inicio donde fue dada la información.

La información que se trasmitirá sin dudarlo es lo más difícil aun cuando es una mala noticia o si no se conoce al paciente en algunos casos suelen ser pacientes con historial dentro de la institución por lo cual resulta más fácil darle a conocer la información o ellos mismos ya suponen una respuesta ya sea esta alentadora o una información negativa, pero cuando no se conoce al paciente es totalmente distinto no se sabe cómo reaccionara este de qué manera tomara aquella información muchos tienen a quitarse la vida por no poder soportar tal noticia que afectara su vida cotidiana . (Grifols, 2014)

Es por esa razón que cada profesional debe ser profesional al momento de dar dicha información teniendo que comprenderla de la manera más sutil para llegar a comunicarla a cada paciente de manera concreta dependiendo siempre del paciente o el diagnostico que este padezca. (Gasco, 2015)

1.2.4 Adaptación e individualización de la información

La Informacion es un proceso e herramienta de ayuda para cada usuario obligando de cierta forma a los profesionales a plantearse, como en cualquier actividad que este desempeñandose ya sea de cualquier ámbito, por esta razon la informacion sanitaria debe tener cuidado de cierta forma evitando errores importantes (Grifols, 2014)

La informacion sanitaria tiene como finalidad el reducir errores sean importantes para cada ciudadano o paciente esto ocurrira siempre y cuando el paciente sepa controlarse, cuidarse como tambien tratarse llevando un control medico en su beneficio, si se llevan estos controles como debe ser reducira cualquier riesgo en la salud, aun asi se cometen errores en este tipo de informacion en los pacientes muchos de ellos se olvidad del trato y el cuidado que deben estar juntos, debido a eso pacientes en su mayoria se dedican solo al cuidado dejando de un lado el control es por que lo conocemos como error de información, al dejar de consumir algo no significa que se este haciendo lo correcto para su salud al contrario al dejar a un lado el control es lo mas perjudicial afectandose de manera directa todo por una mala información sanitaria. (Vallés, 2014)

1.2.4.1 Contenidos y manera de informar

El saber comunicar a los pacientes es lo más importante para ellos poder continuar su vida diaria, en muchos casos se ha dado que se utiliza el parámetro normalidad cuando no es realmente lo que se debe informar una vez que un paciente sufre alguna lesión o una enfermedad que lo alejara de su vida que este estaba acostumbrado ya no será ni podrá llevar una vida normal como muchas veces suelen informarle, esto se debe a que en la mayoría de casos se utiliza el termino no con el objetivo de mentirle al paciente todo lo contrario de animarlo que podrá continuar su vida cotidiana, aun así el paciente sabe que nada será igual ni tampoco tendrá esa normalidad con la que contaba anteriormente. (Grifols, 2014)

1.2.5 Utilidad de la informacion sanitaria

Desde el punto de vista profesional la informacion sanitaria se demuestra de forma que la persona participe positivamnete en el proceso del tratamiento y atencion. De esta manea se puede decir que ofrecer la informacion veraz es de mucha ayuda siempre y cuando sea veridica siendo comprendida por los usuarios . (Vallés, 2014)

A continuacion destacamos que la informacion sanitaria correctamente utilizada es de mucha ayuda tanto para el paciente como para los profesionales debido a que una perosona o paciente bien informado correctamente tendra la disponibilidad de trabajar voluntariamente para su beneficio con el objetivo de recuperarse en el tiempo establecido por los profesionales, cabe mencionar que no siempre el tratamiento es placentero en muchos pacientes es muy dificil seguirlos como se les ordena debido a que no estan acostumbrados a esa vida al inicio le costara adaptarse a ese nuevo estilo de vida. (Andrés, 2014)

1.2.5.1 Toma de decisiones

La toma de decisiones es fundamental en cada uno de los seres humanos siendo esta la que permite el elegir la mejor decisión con responsabilidad de la vida. El saber comunicar, dar a conocer información verídica es la mejor herramienta que puede llevar a elegir una buena decisión para cualquier paciente o usuario. (Vallés, 2014)

1.2.5.2 Control

El conocer la información real sobre lo que padece el paciente afecta como también ayuda directamente a poder entender lo que este padece, las afecciones que causa padecer una enfermedad lo que genera de lo que hoy se conoce como el control lo que resulta beneficioso para el paciente ayudándole a una mejor adaptación de lo que será su vida diaria, el paciente es el único que podrá tomar el control acerca de sus cuidados, en ciertos casos el saber el diagnóstico acerca de lo que le sucede no siempre ni todo paciente podrá tomar el control de lo que está sucediendo en su salud esto ha generado abandonos de sí mismo como de los familiares. (Grifols, 2014)

1.2.5.3 Seguridad

El conocer acerca de la información o diagnostico como ya se ha mencionado ayuda a la toma de decisiones como el poder controlar la situación en la que se encuentre el paciente, lo que también genera seguridad de la forma que si el paciente sabiendo lo que padece y que el tratamiento que este llevara será el adecuado para su pronta recuperación produce que este se sienta seguro confiando en plenitud total que será la mejor decisión seguir el proceso que los profesionales le han de recomendar. (Andrés, 2014)

1.2.6 Participación de la familia en la información

Uno de los aspectos considerados como los más importamtes por parte de los usuarios ha sido el papel de los familiares, el rol de acompañar es por parte de los familiares, esto se debe a que en muchos casos la informacion que se reciva pueda ser masiva la que pueda darse en una consulta, para esto la familia tiene el papel de apoyo y soporte. (Salvador, 2014)

1.2.6.1 Acompañar

Este rol es de suma importancia ya que los familiares son por lo general quienes realizan este papel sin tener en cuenta el papel que desempeña acompañar a un familiar muchos carece de errores al tomar decisiones importantes de los pacientes por el hecho de ser familiares o allegados, es por esto que el acompañamiento no es sustituir al paciente al contrario en muchas ocasiones cuando el paciente no es capaz de resistir tal noticia dependiendo de la gravedad

de la noticia recibida, es aquí donde los familiares o allegados sirven de ayuda de soporte debido a la magnitud de la información recibida ya sea está a la cantidad o a las malas noticias. (Grifols, 2014)

1.2.6.2 Ayuda a tomar decisiones

El tomar decisiones es uno de los roles más importantes para un paciente que no esté preparado para asimilar tal diagnóstico, es por esto que los familiares son fundamentales a la hora de recibir este tipo de noticias que afectan de manera directa a los pacientes llevándolos a perder las ganas de luchar ante aquel diagnóstico, es por esto que los familiares son los que por lo general se hacen cargo de lo sucedido, realizan preguntas acerca del diagnóstico con el fin de buscar información u obtener otras opiniones hasta asegurarse de que el diagnóstico es correcto de esta forma poderlo afrontarlo con ayuda profesional. (Andrés, 2014)

1.2.7 Información de los resultados de los hospitales

Los hospitales por lo general contienen una alta demanda de uso de información de calidad privada siendo de esta forma limitada para algunos usuarios o aspectos, dejándolos en una posición de anticipación a diferencia de otros niveles de asistencias con el fin de generar ideas verídicas permitiendo de esta forma poder compartir la información y la vez asemejar los resultados recabados. (Salvador, 2014)

1.2.7.1 Información del sistema

Se lo conoce como el esfuerzo arrojado del conjunto de varios sistemas informáticos los que tienen como referencia los profesionales en los hospitales, los que buscan mejorar la calidad de información siendo este el esfuerzo en conjunto de todos los profesionales que buscan perfeccionar la calidad como también la cantidad de información que se esté utilizando en el registro de alta de la misma manera de los profesionales que diagnostican la información sanitaria con los procedimientos más relevantes. (Grifols, 2014)

1.2.7.2 Registros

Los registros en la información son fundamentales en un sistema mediante a este el paciente podrá acceder desde su historial clínico hasta conocer sus diagnósticos. (Salvador, 2014)

- Variables con la que se identifican los pacientes: serie de números relacionados a su tarjeta de identificación sanitaria, sexo, fecha, numero del historial clínico.
- Variables relacionadas con el proceso: es conocida como la unidad de servicios donde se presentan características del sistema sanitario, las fechas de ingreso y salidas del paciente.
- Variables clínicas: se las conoce como el análisis y serie de pasos que son codificados de acuerdo como se los clasifique en el sistema, como la Clasificación Internacional de Enfermedades (CIE) de la misma Organización Mundial de la Salud (OMS).

1.2.7.3 Indicadores de seguridad y calidad clínica

Existen indicadores de calidad internacionales que los emplean para comparar los resultados que van asociados con la calidad además la de la seguridad en los hospitales, esto se debe a el seguimiento de indicadores de los responsables quienes se encuentran a cargo de calcular la actividad del sistema sanitario como tambien de varios expertos asistenciales. (Andrés, 2014)

1.2.8 Las arquitecturas de los sistemas sanitarios

Existen seis agentes principales, las cuales sus interacciones determinan las arquitecturas de cada régimen de salud. En los hospitales los proveedores tienen como objetivo convertir el dinero en los servicios de la misma manera motivar a los medicos, enfermeros como tambien al personal que conforma el hospital vincular y coordinar los medios materiales de tecnología e instalaciones donde se realizan la práctica profesional diaria. (Vallés, 2014)

1.2.8.1 Modelos de reembolso

En este tipo de reembolso como es de costumbre el paciente asegurado por decreto elije en qué lugar quiere ser atendido sea público o privado como también el médico que lo va a atender, para lo cual tendría que abandonar los servicios que ofrecen los proveedores, reenviando la factura para que esta sea devuelta parcial o completa. Este modelo de reembolso se lo da principalmente en los seguros privados como los de voluntariado, pero también tiene algunos problemas e inconvenientes como la tendencia moral de los usuarios es decir el mal uso de los pacientes. (Salvador, 2014)

1.2.8.2 Modelos de contratos

Este sistema de contrato se lo conoce como la solución inmediata a la problemática que presenta el modelo anterior de reembolso, se caracteriza principalmente por que los aseguradores realizan los respectivos acuerdos con varios hospitales, clínicas, asociaciones de médicos los que prestan servicios en condiciones acordadas , es decir que si el paciente se enferma ya no tiene la potestad de elegir el medico de su preferencia o el sitio donde quiere este que sea atendido sino realizarse la respectiva ajuste a lo que su asegurador tenga disponible minimizando la capacidad de elección. (Andrés, 2014)

1.2.9 Condicionantes del modelo sanitario

El modelo exploratorio sanitario, es una consecuencia social de los grupos que lo pugnan como resultado de intereses. Los intereses de estos grupos constan de varias formas de los cuales se han identificado unos cincuenta y siete modelos sanitarios disímiles. Por lo que lo hace importante determinar cuales son los que forman parte de esos grupos asociados deduciendo las caracteristicas fundamentales del modelo sanitario los que estan divididos en cuatro grupos que son: ciudadanos, gestores y propietarios, los intereses fundamentales y por último los suministradores de salud. De esta manera cabe mencionar que los ciudadanos los cuales son seguros colaboradores tienen que tener derecho a no esperar, ser informados (Grifols, 2014)

En toda situación, confiaza en el sistema, no truncarse con la asistencia, al usar el sistema sanitario los pacientes como son los padres pueden actuar actuando bajo un patrón u orden que se les dicte como que se acueste, callese etc.

- Para el individuo. Las personas por lo general son las principales causantes de su propia salud de acuerdo al estilo de vida que este llevando siendo el mas inlfuyente.
- Para el médico. Teniendo como su mayor influencia el autocontrol haciendolo una persona con la moral alta aumentando su heterocontrol anhelando la perfección y teniendo en cuenta que la negligencia es sancionada.

1.2.10 Planificacion y gestion del modelo sanitario

Una vez que cualquier modelo sanitario se cumpla adecuadamente con todas y cada una de sus funciones sera aceptado por parte de los grupos quienes lo evaluan y este debera estar debididamente gestionado y planificado. La planificacion debe basarse en calcular lo que necesita una sociedad determinada para que esta sea antendida correctamente. (Andrés, 2014)

1.2.10.1 Necesidad

La necesidad que hace que sea comprensible y el elevado coste mayor al 60% de los gastos sanitarios, calculo que será puesto directamente al sistema del hospital ajustando las cifras en todo el modelo sanitario, para computar la insuficiencia hospitalaria se utilizaría una medida que podría ser la cama hospitalaria, aunque este no solo realice funciones de un hospital a las que debe dedicarse generalmente. (Salvador, 2014)

1.2.10.2 Eficacia

La otra característica común de un sistema sanitario necesaria que debe aplicarse es la eficacia, la que consiste específicamente en realizar el cálculo de cada una de las instituciones hospitalarias que dan servicio en situaciones frecuentes con una fórmula expuesta anteriormente. (Vallés, 2014)

CAPITULO II

2 DIAGNÓSTICO.

2.1 Método de Investigación

2.1.1 Cuantitativo

La investigación cuantitativa busca medir un fenómeno. Es más estructurada, objetiva. Se enfoca en el comportamiento de una persona respondiendo preguntas como cuántas, con qué frecuencia y en qué medida. (Jaramillo, 2010)

Este método de investigación es una de las metodologías más utilizados en investigaciones de estudio, por tal motivo se lo utiliza en la recolección de información por medio de las técnicas e instrumentos aplicados los mismo que permiten obtener datos de diferentes puntos de vista de los encuestados.

2.2 Enfoque de la investigación

2.2.1 Deductivo

Es un procedimiento donde el investigador combina la reflexión con la observación, en el posterior estudio a realizar, con este método se pretenderá darle soluciones al problema que se ha planteado, también realiza la comprobación de la hipótesis deducidos asemejándolos con la experimentación (Cegarra, 2004) .

El cual se utilizó para la elaboración del capítulo tres en los procedimientos que ayudaron a la deducción e inducción del estudio en el uso de las herramientas de seguridad de redes con el fin de obtener resultados para lograr cumplir con el estudio.

2.2.2 Analítico- sintético

Este método se implementó al momento de desarrollar el marco teórico de la investigación para poder analizar ideas de los diferentes autores y de esta forma obtener nuevos conocimientos los cuales permitirán sintetizar los conceptos necesarios propios acerca de los temas a investigar (Moguel, 2005).

Este método es el que se encargara de analizar y revisar todos los elementos de forma ordenada de cualquier fenómeno por lo que así se analizara el funcionamiento de las herramientas de seguridad en redes.

2.3 Tipos de investigación

2.3.1 Descriptiva.

Este tipo de investigación es uno de los más utilizados teniendo como objetivo principal y único el poder describir detalladamente el problema al cual se pretende darle solución de manera directa durante el proceso del estudio analizando y englobando la información del tema inicial como lo son sus características, la configuración como también los procesos que serán necesarios llevar a cabo para el respectivo estudio e implementación de las herramientas de seguridad en la Red.

2.4 Técnicas de investigación

2.4.1 Encuesta

La encuesta es una herramienta de obtención de información ordenada, la forma en la que más se la utiliza es en plantear una serie de preguntas con el fin de obtener las ideas o pensamientos de los encuestados acerca de lo que se pretende solucionar (Alvira, 2011).

Esta técnica se la realizó al personal que conforma el Distrito de Salud, con el objetivo de obtener la información necesaria, las que aportarán a la investigación.

2.4.2 Entrevista

La entrevista es útil al momento de analizar un problema, conocerlo a profundidad por las personas a las que se les realizará la entrevista, es una breve interrogación sobre lo que conoce, piensa y de alguna forma cree el entrevistado (Jaramillo, 2010) .

La entrevista fue aplicada al encargado del departamento de TIC siendo el individuo responsable del control de toda la red de dicho lugar, método clave para recabar información para continuar con este estudio investigativo.

2.5 Instrumentos de investigación

2.5.1 Cuestionario

Un cuestionario es, por definición, el instrumento estandarizado que utilizamos para la recogida de datos durante el trabajo de campo de algunas investigaciones cuantitativas, fundamentalmente, las que se llevan a cabo con metodologías de encuestas (Valverde, 2015).

De esta forma se lo conoce también como una herramienta eficaz que permite al investigador realizar un conjunto de preguntas las que serán aplicadas a una muestra determinada utilizando el método cuantitativo

2.5.2 Guía de la entrevista

Se logra mostrar que la entrevista se guía por ciertos argumentos limitadas por el investigador, no obstante, hay una ventaja muy significativa, la cual es ofrecer ciertas conformidades para aclarar, pulir o ilustrar las preguntas, no solamente en eso sino profundizar aún más la investigación a través de las respuestas adquiridas por el entrevistado (Martínez, 2014).

2.6 Validez de instrumentos.

La validez se refiere a los resultados de una prueba y no a la prueba misma. Por tanto, si tenemos la prueba ABC de habilidades sociales, los resultados de la prueba podrían ser válidos para medir la interacción social en adolescentes. Hablamos de validez solo a la luz de los resultados de una prueba. Tenga presente que la validez de un instrumento a menudo se define dentro del contexto de como se está usando la prueba. La validez muestral se refiere a que el instrumento contenga una muestra representativa del universo de la materia de interés (Namakforoosh, 2012).

2.7. Población y muestra

2.7.1. Población

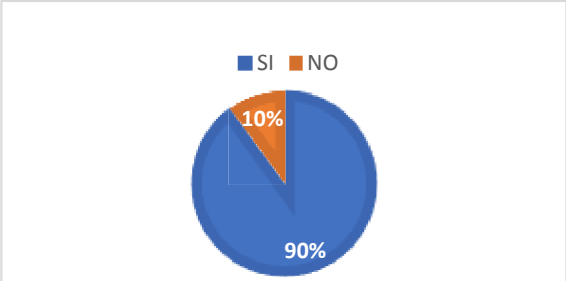
La población que será la base para la presente investigación se ha considerado a los empleados de la “Dirección Distrital de Salud 13D05 El Carmen” con un total de 20 empleados en general los cuales laboran en el mismo y hacen uso de la red de dicho lugar.

2.7.2. Muestra

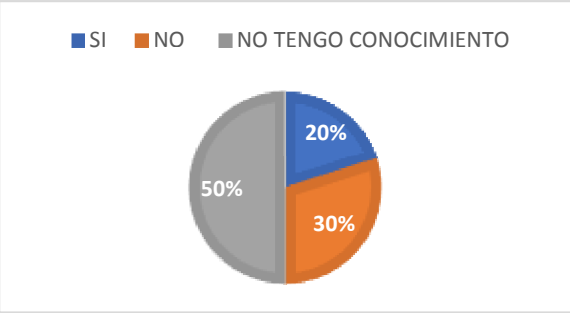
Debido a que la población es mínima la muestra será discrecional por tal motivo no será considerada aplicar la técnica de muestreo, por lo consiguiente se investigó a todos los empleados que laboran en la “Dirección Distrital de Salud 13D05 El Carmen” los cuáles serán objeto del presente estudio. Para la entrevista se consideró al responsable del Departamento de TIC.

2.8. Tablas y Grafos

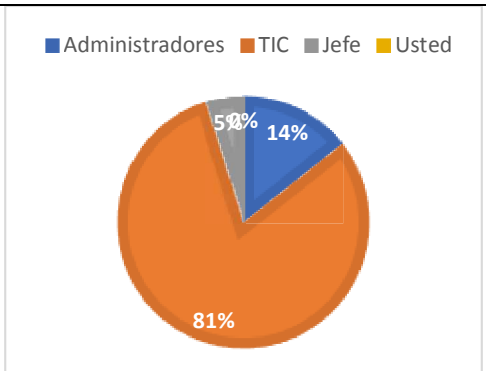
2.8.1. Encuestas realizadas al personal del Distrito de Salud 13D05 de El Carmen.

Preguntas	Gráficas	Análisis
¿Cuenta usted con un usuario y clave para acceder a su ordenador?		Como se puede observar la mayoría cuenta con un usuario y contraseña en su ordenador.

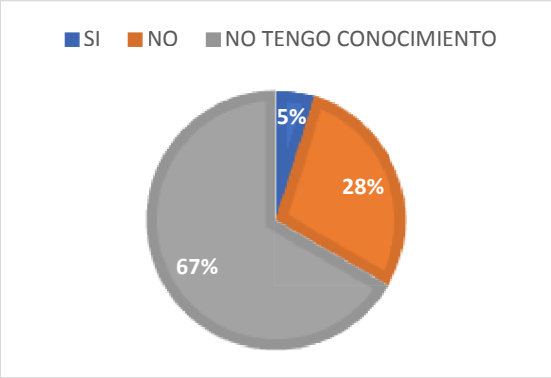
Pregunta	si	no
n.º 1	18	2

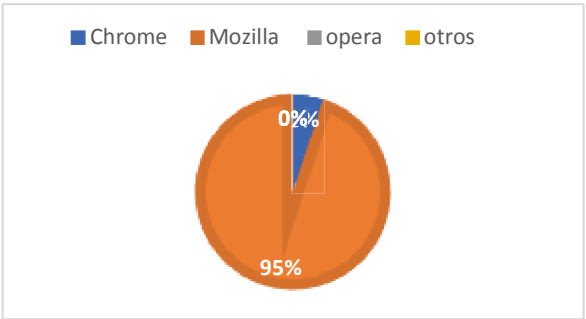
Preguntas	Gráficas	Análisis
¿Conoce usted las herramientas de seguridad de redes como son: Nessus, pandora, Nagios, ¿Nmap? etc.? ¿Su computador cuenta con alguna herramienta de seguridad de redes?		De acuerdo a los resultados obtenidos de los encuestados podemos notar que un gran porcentaje desconoce acerca de las herramientas de seguridad

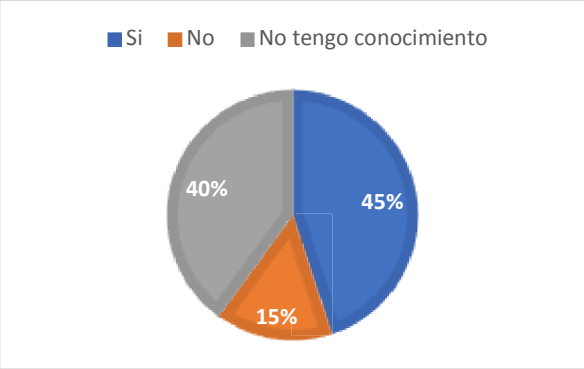
Pregunta	si	no	No tengo conocimiento
N.º 2	2	18	
N.º 3	4	6	10

Preguntas	Gráficas	Análisis
¿Quiénes están a cargo de instalar software de seguridad en su computador?		La encuesta nos arroja que para la población Distrital de Salud los encargados de instalar son del departamento TIC

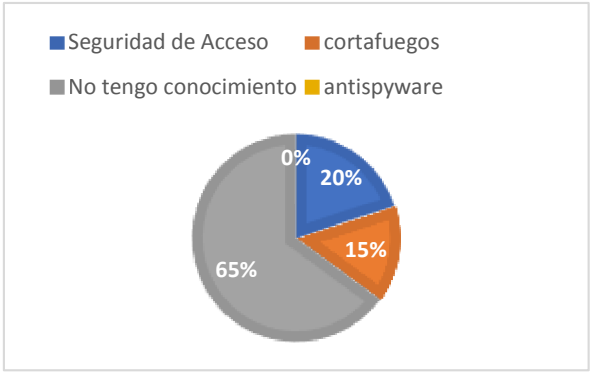
Pregunta	Administrador	TIC	Jefe	Usted
N.º 4	3	16	1	0

Preguntas	Gráficas	Análisis
¿Su sistema Operativo se encuentra actualizado a la última versión?	 Pregunta / Si / No / No tengo conocimiento N.º 5 / 1 / 6 / 13	Según los resultados obtenidos se analiza que la mayoría de la población desconoce acerca de las actualizaciones de su SO.

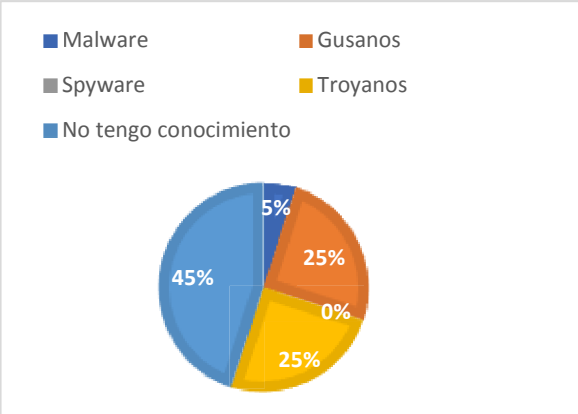
Preguntas	Gráficas	Análisis
¿Qué navegador web utiliza regularmente en su ordenador?	Pregunta / Chrome / Mozilla / Opera N.º 6 / 1 / 19 / 0 	Según los resultados nos indica que la mayoría de los usuarios utiliza Mozilla como su navegador confiable.

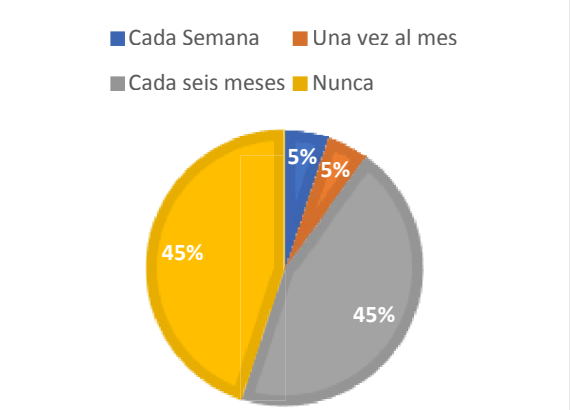
Pregunta	Gráficas	Análisis
¿Se ha encontrado con problemas de seguridad en la red de datos donde se ha visto comprometida la información de los usuarios?		Podemos denotar que los usuarios afirman que se ha visto comprometida su información personal en la red. Y otra parte desconoce los hechos.

Pregunta	Si	No	No tengo conocimiento
N.º 7	9	3	8

Pregunta	Gráficas	Análisis
¿Qué tipo de seguridades tiene en su ordenador?		Existe una similitud en la seguridad de acceso y el cortafuego, aun así, la mayoría no conoce con qué tipo de seguridad cuenta.

Pregunta	Seguridad de acceso	cortafuegos	No tengo conocimiento
N.º 8	4	3	13

Pregunta	Gráficas	Análisis
¿Ha tenido usted algún inconveniente con virus llamados:	 Pregunta / Malware / Troyanos / Gusanos / No tengo conocimiento N.º 9 / 1 / 5 / 5 / 9	El mayor porcentaje no tiene conocimiento haber tenido problemas de virus, una gran parte asegura que si han tenido un Malware.

Pregunta	Gráficas	Análisis
¿Actualmente realizan mantenimientos periódicos sobre la seguridad de redes en las computadoras?	 Pregunta / Cada Semana / Cada Mes / Cada. 6 meses / No tengo conocimiento N.º 10 / 1 / 1 / 9 / 9	Se puede denotar que el mantenimiento a la red y ordenadores no es periódicamente dato que será tomado en cuenta.

<table>
<tr><th>Pregunta</th><th>Gráficas</th><th>Análisis</th></tr>
<tr>
<td>¿Realizan capacitaciones acerca de la seguridad de redes hacia los usuarios?</td>
<td>


<table>
<tr><td>Pregunta</td><td>Si</td><td>No</td><td>A veces</td><td>No tengo conocimiento</td></tr>
<tr><td>N.º 11</td><td>2</td><td>16</td><td>0</td><td>2</td></tr>
</table>
</td>
<td>Según los resultados nos muestra que una gran cifra no ha sido capacitada acerca de las amenazas que hay en la red.</td>
</tr>
</table>

Tabla 1 Tabulación de encuesta
Autor: Carlos Valdez

De acuerdo a los resultados obtenidos en la encuesta se menciona que un cierto porcentaje de usuarios si tienen seguridad de acceso a su ordenador lo que hacen que estos equipos estén más seguros, de la misma manera se hace referencia que una gran proporción de los encuestados no conoce al menos ningún tipo de herramienta de seguridad de las que se ha planteado por lo que se desconoce si sus ordenadores tienen alguna de estas u otras, el desconocimiento de acerca de quienes están a cargo de instalar software y darme el respectivo mantenimiento como la actualización del sistema operativo generan ciertas inseguridades dentro del equipo y lugar de trabajo. Como se puede notar la mayoría de los usuarios afirma que se ha visto afectada la información ya sea esta por virus o el desconocimiento de herramientas que brindan seguridad a los ordenadores, se puede notar que el mantenimiento a los ordenadores no es oportuno como debería ser para un mejor funcionamiento de los equipos de trabajo.

2.9. Entrevista

Esta entrevista fue realizada al encargado y jefe del departamento de TIC (Tecnología de la Información) en el Distrito de Salud 13D05.

Preguntas	Respuestas
1. **¿Con que tipo seguridad lógica cuentan los ordenadores de quienes trabajan en el Distrito de Salud?**	El Distrito 13D05- Salud El Carmen cuenta con ordenadores de software libre y Windows, no contamos específicamente ningún software de protección.

2. ¿Qué herramientas de protección a la red tienen los ordenadores del Distrito de Salud 13D05?	El único software de protección con el que se cuenta es el antivirus y su firewall tanto de Linux como de Windows.
3. ¿En caso de un ataque a la red con qué plan anti-fallas cuentan?	Actualmente no se cuenta con un plan en caso de un ataque a nuestra red.
4. ¿Cada que cierto tiempo realiza mantenimientos de seguridad en la red y en los ordenadores?	El distrito de salud y TIC están al pendiente de todos los centros de Salud y sus equipos lo que lo hace un tanto complicado realizar mantenimiento periódicamente por lo que se lo realiza cada seis meses.
5. ¿Cuál es el tipo de amenaza en la red que se detectan con mayor frecuencia en la Institución?	Spam de la Web, códigos maliciosos lo que suele encontrarse en Linux, en Windows virus los más conocidos.
6. **¿Considera usted que se deba realizar capacitaciones acerca de las amenazas que existen a los usuarios quienes laboran en la institución? ¿Y por qué**?	Si, por que ayudaría el mejoramiento a los usuarios en su trabajo laboral.

7. **¿Cree usted que la red del Distrito de Salud se utiliza solamente para el trabajo o también para otros fines?**	Considero y creo que solo se utiliza para el trabajo, pero es común usarla para hacer diferentes fines, como transacciones, mensajería etc.
8. **¿Cree usted que al tener Antivirus en las máquinas están libres de ataques y virus en la red?**	No, el contar con un Antivirus es importante, pero este no protege por completo el ordenador por lo que siempre estaremos expuestos.
9. **¿Considera usted que es importante que se deba tener el sistema Operativo actualizado, para protegerlos de las nuevas amenazas?**	Si es importante el tenerlo actualizado debido a los beneficios que este ofrece en cada actualización, pero aun así seguiremos expuestos a las amenazas en las redes.
10. **¿Se han presentado inconvenientes en los equipos que tienen acceso a la red tanto personales como del trabajo algún índice de robo de información?**	¡Personalmente no me ha sucedido, pero si al personal de trabajo de dicho lugar ya mencionado!
11. **¿Cree usted que es importante contar con herramientas de seguridad que se encarguen del monitoreo y protección de ataques, virus en la red? ¿Y por qué?**	Si, Ayudaría a manejar un sistema de red confiable para los usuarios y eficaz en su manejo.

Tabla 2 Tabulación de entrevista
Autor: Carlos Valdez

Analizando las respuestas expuestas por el entrevistado, se puede concluir que actualmente el distrito 13D05 no cuenta con una herramienta de análisis y detección de amenazas en la red, las máquinas u ordenadores solo tienen como escudo de protección de amenazas el firewall de seguridad del sistema operativo que estas utilicen ya sea Linux o Windows, por las respuestas de dicha entrevista también se puede notar que algunos tienen usuario y contraseña en sus ordenadores con el objetivo de evitar el acceso de intrusos.

2.10. Triangulación de los resultados

En base a los resultados del análisis que se ha obtenido de la encuesta realizada al personal de trabajo que lo conforman el Distrito 13D05 de Salud El Carmen, se dio a conocer como resultado que un mayor porcentaje cuenta con usuario y contraseña en su ordenador con el fin de evitar el acceso de personas no autorizadas en su equipo de trabajo de uso particular, en la pregunta 1 de la entrevista con la 2 y la 3 de la encuesta se puede notar que el personal de trabajo del distrito no conoce ninguna de las herramientas de protección de seguridad en redes que se proponen en la encuesta.

Además, en la entrevista la respuesta número 5 y la 9 se ha encontrado anomalías en Windows más conocidos como virus los que afectan el rendimiento como también la perdida de información valiosa, entre ellos se mencionó a los virus conocidos como troyanos, gusanos y malware los que por lo general son detectados con mayor frecuencia en las redes, en Linux se encuentran ciertas vulnerabilidades más conocidos Spam de Web, códigos maliciosos.

Como parte de los resultados recabados cabe mencionar que una gran parte de la población encuestada afirma en la pregunta 11 de la encuesta que el personal de trabajo no ha sido capacitado acerca de los riesgos informáticos a los cuales se ven expuestos a diario, al no conocer sobre el tema son los principales afectados debido a las amenazas en la red, al igual que no se les da el respectivo mantenimiento periódicamente ni a la red como tampoco a los ordenadores información que será corroborada en la pregunta diez de la encuesta y cuatro de la entrevista.

CAPITULO III

3 PROPUESTA

Realizar un estudio de seguridad enfocado a la red del Distrito de salud 13D05 El Carmen-Zona 4 con el fin de detectar los problemas debido a las vulnerabilidades que afectan a la misma y proponer varias soluciones de acuerdo a los resultados obtenidos.

3.1 Antecedentes

Nuestra misión es 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.

Sus atribuciones y responsabilidades son:

- Dirigir la aplicación de las políticas de Salud, en el ámbito de su competencia.
- Organizar y conducir la red de servicios de salud pública y complementaria del nivel distrital y los entes administrativos sujetos a su jurisdicción.
- Aprobar el plan anual de la política pública del nivel distrital y los entes administrativos sujetos a su jurisdicción;
- Conducir gerencialmente las unidades de planificación, técnica y administrativa financiera orientando a un trabajo técnico, objetivo e integral de salud.
- Disponer la elaboración del plan de fortalecimiento de las capacidades institucionales del nivel distrital, para la implementación del Modelo de Atención Integral, Familiar, Comunitario e Intercultural en la red de servicios de salud.

3.2 Misión

Ejercer como Autoridad Sanitaria Nacional, la rectoría, regulación, planificación, coordinación, control y gestión de la Salud Pública ecuatoriana a través de la gobernanza, vigilancia de la salud pública, provisión de servicios de atención integral, prevención de enfermedades, promoción de la salud e igualdad, investigación y desarrollo de la ciencia y tecnología y la articulación de los actores del sistema, con el fin de garantizar el derecho a la Salud.

3.3 Visión

Será la Institución que ejerce plenamente la gobernanza del Sistema Nacional de Salud, con un modelo referencial en Latinoamérica que priorice la promoción de la salud y la prevención de enfermedades, con altos niveles de atención de calidad con calidez, garantizando la salud integral de la población y el acceso universal a una red de servicios, con la participación coordinada de organizaciones públicas, privadas y de la comunidad.

3.4 Objetivo de estudio

Realizar un estudio de seguridad en redes para la información sanitaria en la "Dirección Distrital de Salud 13D05 El Carmen – zona 4."

3.4.1 Objetivos Específicos

- Fundamentar teóricamente sobre seguridad en redes e información sanitaria.
- Recopilar información sobre el funcionamiento de la red de datos del Distrito de Salud 13D05.
- Realizar un informe de auditoría de la red de datos del Distrito de Salud 13D05.
- Sugerir herramientas de seguridad para la red de datos del Distrito de Salud 13D05.

INFORME DE AUDITORÍA SOBRE LA SEGURIDAD EN LA RED DE DATOS DEL DISTRITO DE SALUD 13D05

Realizado por: Carlos Daniel Valdez Toral

El Carmen, enero 2020

Colaboradores del Distrito

De Institución evaluadas: 1

Personal: 20

3.5 Informe de auditoría de la red del Distrito de Salud 13D05.

En el presente informe se nos muestra los resultados de la auditoria informática que se realizó cumpliendo con los parámetros necesarios para la seguridad de la red en el Distrito de Salud, el cual fue aplicada a los ordenadores de cada uno de sus colaboradores quienes desempeñan sus labores diarias en dicha entidad la cual se encuentra ubicada en el Cantón el Carmen, este análisis se enfoca en demostrar el cumplimiento de la norma propuesta y del estándar IIEE, demostrando al final una manera de las muchas que podemos encontrar para poder prevenir ciertos ataques la red.

3.5.1 Objetivos

Verificar la utilización de los estándares y normas que garantizan la seguridad en la red Distrito de Salud El Carmen.

3.5.2 Personal relacionado

Para poder realizar este presente trabajo de investigación acerca de la seguridad de la red, oportunamente se pudo obtener la información necesaria gracias a la colaboración y disponibilidad de los colaboradores del Distrito de Salud 13D05.

3.6 Controles de seguridad aplicados

3.6.1 Norma ISO/IEC 27033

El propósito de la norma ISO / IEC 27033 es proporcionar una guía detallada sobre los aspectos de seguridad de red, el funcionamiento y el uso de redes de sistemas de información y sus interconexiones. Las personas dentro de una organización que se encargan de la seguridad de información en general y seguridad de la red, en particular, deben ser capaces de adaptar el material en esta norma para satisfacer sus necesidades específicas. (Ramos, 2011)

3.6.1.1 Procesos de la norma ISO/IEC 27033

3.6.1.1.1 Análisis de riesgos y selección de medidas

Esta sección trata de la identificación de riesgos de la red e identificación de los controles de seguridad.

3.6.1.1.2 Identificación de Controles

Estos controles pueden ser a la vez técnicas y administrativas y se dan con el fin de implementar la seguridad en la red y mantener las medidas de apoyo.

3.6.1.1.3 Identificación de Arquitectura Técnica de Seguridad y Controles

El contenido de esta etapa del proceso es establecer la arquitectura de seguridad de la red técnica adaptables a las necesidades de la empresa de los objetivos planteados.

3.6.1.1.4 Desarrollo, implementación, puesta a prueba, verificación y medición.

El contenido de esta etapa del proceso consiste en "desarrollar, implementar, probar, verificar y medir la solución a desarrollarse.

3.6.1.2 Controles sugeridos por la norma ISO/IEC 27033

Red de Área Local
Proporcionar manual de la utilización de parámetros a aplicar.
Hardware y Software
Instalar software que detecte cualquier amenaza a la red y que permita controlar cualquier tipo de ataque a la misma.
Desactivar páginas web para evitar el contagio de contenido no deseado.
Procedimientos
Realizar controles de seguridad con el mantenimiento adecuado a los ordenadores
Crear cuenta de administrador para cada usuario y eliminar softwares obsoletos

Se recomienda documentar la configuración e instalación de los softwares de seguridad para usarlas en las nuevas estaciones de trabajo
Garantizar la protección de la red y que las contraseñas sean cambiadas periódicamente.
Probar vulnerabilidades de todos los dispositivos conectados a internet.

Tabla 3 Parámetros de Seguridad de la Norma ISO/IEC 2703
(Andrade, 2012)

3.6.2 Estándar IEEE 802.10

Este estándar especifica la asociación de seguridad de gestión y administración de claves, así como el control de acceso, confidencialidad de los datos y la integridad de los datos.

3.6.2.1 Procesos del Estándar

- Enfoque en el aspecto de seguridad de las redes empresariales de tamaño reducido.
- permite operar en una serie de redes e incorpora métodos de autenticidad y encripta miento.

3.6.3 Alcance

El presente estudio es la obtención final de la información recabada donde se aplicaron ciertos parámetros de obtención de información como es el de este caso una ficha el cual tenía como objetivo determinar cierto nivel de conocimiento por parte de los empleados del Distrito de Salud el Carmen sobre ciertas herramientas de análisis y protección de seguridad en redes, que como objetivo principal tiene cumplir con los estándares y normas de seguridad de la red del distrito.

Por lo que en esta auditoria se verifico la aplicación de los parámetros de seguridad que establece la norma ISO/IEC 27033 que se destina a la gestión de la seguridad, aplicaciones de servicios y/o redes, seguridad de los dispositivos de red y a la seguridad de información, parámetros que se deben cumplir para que la red sea segura ayudando a tomar las medidas o métodos que sean necesarios. Por lo que también se tuvo considerar el Estándar 802.10 de

seguridad el cual menciona que es un estándar que opera sobre una variedad de redes e incorpora métodos de autenticación y encripta miento, este estándar está compuesto por normas que incluyen dentro de ellas horarios de funcionamiento, denegaciones, restricciones a varios lugares en la red, planes de emergencia y todo lo que se necesita para que una red tenga un buen nivel de seguridad.

Una vez analizadas la norma y el estándar sobre la seguridad en redes para información sanitaria se procedió a realizar un método de obtención de información, el cual permitió recolectar los datos necesarios para llevar a cabo este trabajo donde fue necesario realizar un total de 30 preguntas mismas que están compuestas de SI y NO las que son conocidas como preguntas cerradas, conformándolo a este método en 3 partes importantes el cual se distribuye de la siguiente forma; las primeras 10 preguntas van dirigidas a las amenazas que afectan a la red y la configuración de las herramientas, las 10 siguientes preguntas hacen referencia a la seguridad en la red y medidas que se deben tener en cuenta en su ordenador, las últimas 10 pertenecen a los parámetros establecidos como lo son las normas ISO/IEC 27033 y el Estándar/IEEE 802.10 de seguridad.

Para poder realizar la recolección de la información de los trabajadores se procedió a realizar una matriz en Excel con un total de 30 preguntas las que una vez aprobadas se las procedió a ejecutarlas y así determinar los problemas a los que se ven afectados los usuarios en la red para poder cumplir con los estándares de calidad que ofrece la norma ISO/IEC 27033, para obtener cierta información se le asigno a cada empleado T1 (trabajador 1) hasta llegar al T20.

0	PREGUNTAS	RESPUESTAS																			
		T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	T16	T17	T18	T19	T20
	AMENAZAS QUE AFECTAN A LA RED Y CONFIGURACIÓN DE LAS HERRAMIENTAS.																				
1	¿ Usted ha recivido ayuda en caso de perdida de información por contaminación de su equipo?	0	0	0	0	0	1	0	0	1	1	0	1	0	0	0	0	0	0	1	1
2	¿ Su equipo se encuentra protegido ante los ataques informáticos y virus?	1	0	0	0	0	1	0	1	0	1	0	0	0	1	0	1	0	0	1	0
3	¿conoce usted alguna herramienta de análisis y protección de redes?	0	0	1	1	0	1	1	1	1	1	1	1	0	1	0	1	0	1	0	1
4	¿Sabe usted que hacer en caso de una contaminación de su ordenador de trabajo ?	0	0	0	1	0	1	0	1	1	1	0	1	0	1	0	1	1	0	1	0
5	ha recibido capacitaciones sobre las amenazas a las que esta expuesta una red.	1	0	1	0	0	0	1	0	0	1	0	1	0	0	1	0	1	0	1	0
6	tiene idea usted de lo que pueden causar ciertas amenzas de redes a su ordenador	1	1	1	0	1	1	0	1	1	1	0	1	1	0	0	1	1	0	0	1
7	sabe usted como proteger su equipo con herramientas de analisis y protección	1	0	1	0	0	1	0	1	0	0	1	0	0	0	1	0	0	1	0	0
8	ha instalado y configurado herramientas de protección de virus en su ordenador	1	0	0	0	0	1	0	1	0	0	0	1	0	0	1	0	0	1	0	1
9	su equipo cuenta con una conexión segura a la red	1	1	1	0	0	1	1	1	0	0	1	0	1	1	0	1	0	0	1	0
10	alguien le hablado sobre las amenazas que existen en las redes.	1	0	1	0	1	0	1	1	1	1	1	1	1	0	1	0	1	0	1	0
	LA SEGURIDAD EN LA RED Y LAS MEDIDAS QUE SE DEBEN TENER EN CUENTA EN SU ORDENADOR	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	T16	T17	T18	T19	T20
11	sabe usted cuales son los tipos de seguridad que debe contener su ordenador	0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	1	0	1
12	su ordenador tiene contraseña de inicio de sesión	1	1	0	1	1	0	1	0	1	1	1	1	1	0	0	1	0	1	0	0
13	sabe usted de que caractéres debe contener su contraseña de inicio.	1	0	1	1	1	0	1	0	1	1	0	1	0	1	0	0	1	1	1	1
14	su contraseña esta compuesta solo de números	0	0	0	1	0	1	0	1	1	0	0	0	1	0	1	0	1	0	1	0
15	su contraseña esta conformada de lestras y números	1	1	1	0	1	0	1	0	0	1	0	1	0	1	0	0	0	1	0	0
16	su contraseña esta conformada con datos personales	1	1	0	1	1	0	1	0	1	0	0	0	0	1	0	1	0	0	1	0
17	cree usted que su ordenador tiene medidas de seguridad adecuada	1	0	1	0	1	1	0	1	0	1	0	1	1	0	1	1	0	0	0	1
18	cree usted que su equipo está actualizado a la ultima versión	1	1	0	1	0	1	0	1	0	1	0	1	0	1	1	0	1	0	1	1
19	sabe usted si su equipo cuenta con un firewall	1	0	0	1	0	1	0	0	0	1	0	1	0	1	0	0	1	0	1	0
20	sabe usted de la importancia que es tener un firewall en su ordenador	1	0	1	0	1	0	1	0	1	0	1	1	0	1	1	0	1	0	1	0

1

	NORMA ISO 27033 Y ESTANDAR 802.10	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	T16	T17	T18	T19	T20
21	¿Sabe usted si realizan periódicamente análisis en la red con el objetivo de prevenir cualquier perdida	0	0	1	0	1	0	0	0	0	1	0	1	0	1	0	1	0	1	0	1
22	¿La red de trabajo esta libre para el acceso al público?	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
23	ha recibido orientación sobre laidentificación y análisis de riesgos de seguridad en la red	1	0	0	1	0	0	0	1	0	0	0	0	1	0	1	0	0	1	0	0
24	se he enfrentado con problemas de perdidas de informacion	1	1	1	0	1	0	1	0	1	1	0	1	0	1	0	1	0	0	1	0
25	usted realiza periodicamente algun tipo de respaldo de información	1	0	1	1	0	1	0	1	0	1	0	0	1	0	0	0	1	0	1	0
26	¿ha visto la necesidad de instalar un software de análisis y protección de red para evitar ciertas amena	0	1	0	1	1	1	0	1	1	0	1	0	1	0	1	1	0	1	1	1
27	¿cree usted que tener un software de protección para la red siendo este confiable reduce ciertos riesgos	1	0	1	0	1	1	1	1	0	1	0	1	0	1	0	1	0	1	0	1
28	su equipo tiene restricciones a ciertas páginas Web con el objetivo de prevenir de algún virus malicios	1	0	1	0	1	0	1	0	1	1	0	1	1	0	1	0	0	1	1	0
29	su equipo es seguro con los métodos de protección que tiene ante ciertas amenazas de red.	0	1	0	1	0	1	0	0	0	1	0	0	1	0	1	0	1	0	1	0
30	cree usted que la red carece de ciertos protocolos de seguridad.	1	0	1	0	1	0	1	1	0	1	0	1	1	1	0	1	1	1	0	1

Ilustración 3 tabulación de resultados generales de la Auditoria

Autor: Carlos Valdez

2

3.1. Hallazgos

Una vez realizado el instrumento de recolección de información basado en la seguridad y el análisis de redes se ejecutó con el objetivo de analizar si se cumple con las normas, parámetros y estándares de seguridad, la misma que fue aplicada a los trabajadores quienes se encargan de la operatividad de la información en el Distrito de Salud 13D05 por lo que se pudo encontrar lo siguiente de acuerdo a los conocimientos que ellos poseen.

3.1.1. Cumplimiento general de las políticas sobre la seguridad en la red.

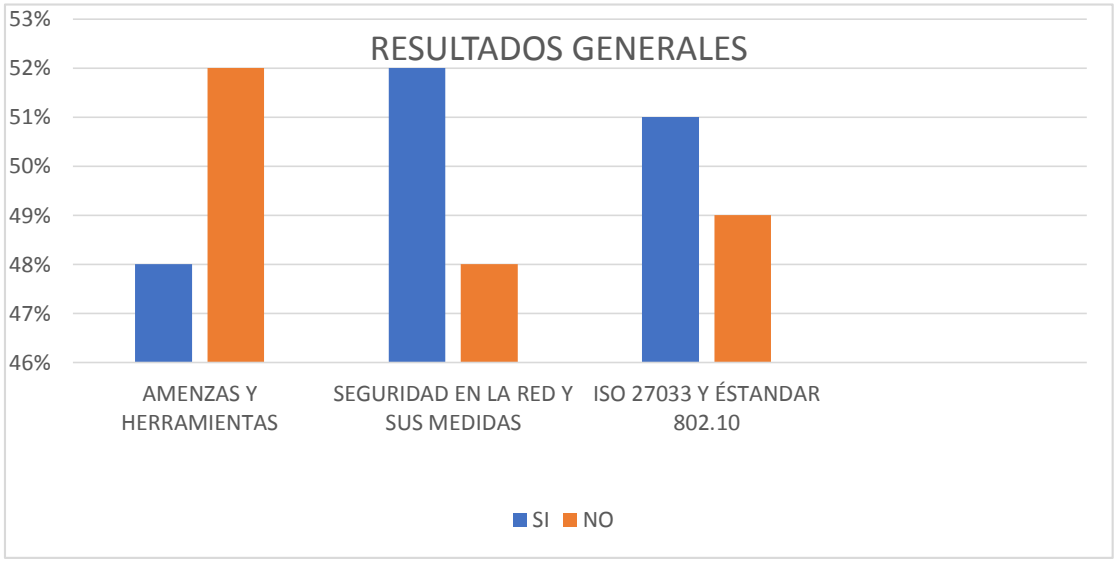


Ilustración 4resultados generales

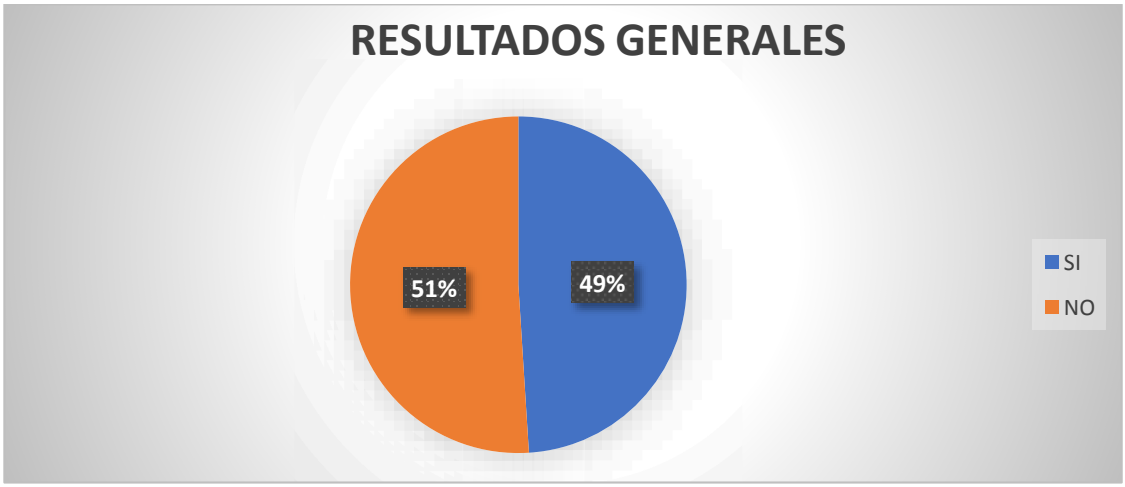


Ilustración porcentaje 5 de resultados generales

Una vez obtenido los resultados se pudo determinar con respecto a ciertas medidas y parámetros si estas se cumplen o no proyectando como resultados los valores aproximados que se encuentra dentro del 49% y 51% demostrando así de cierta forma una falta de conocimiento acerca de las herramientas de análisis y protección de red siendo este el mayor problema a la hora de manejar cierta información dentro de la institución.

Se realizo el análisis a 20 colaboradores utilizando el instrumento que sirvió para obtener información donde se realizaron ciertas preguntas de acuerdo a las normas y estándares de protección de la red , el mismo que determinó que la capacidad de conocimiento acerca de seguridad y de herramientas de protección es muy poco, también existen parámetros donde se exige la protección contra intrusos, los caracteres que debe poseer una clave para que esta sea segura los cuales son desconocidos por los colaboradores de la entidad.

3.2. Análisis de gráficos por segmentos

De las 30 que se realizaron se dividieron en 3 grupos para su mayor entendimiento y apreciación de los resultados lo cuales fueron:

3.2.1. Amenazas a la red y configuración de las herramientas.

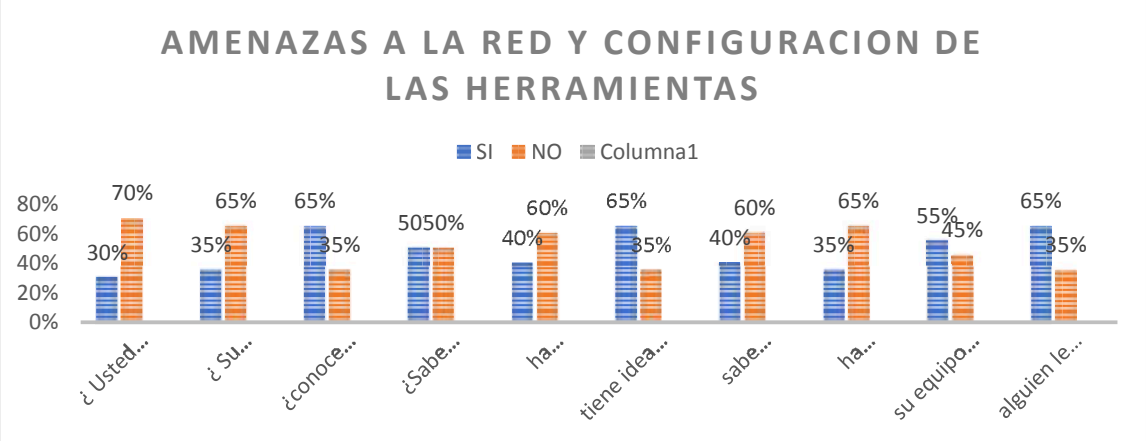


Ilustración 6 tabulación de amenazas a la red

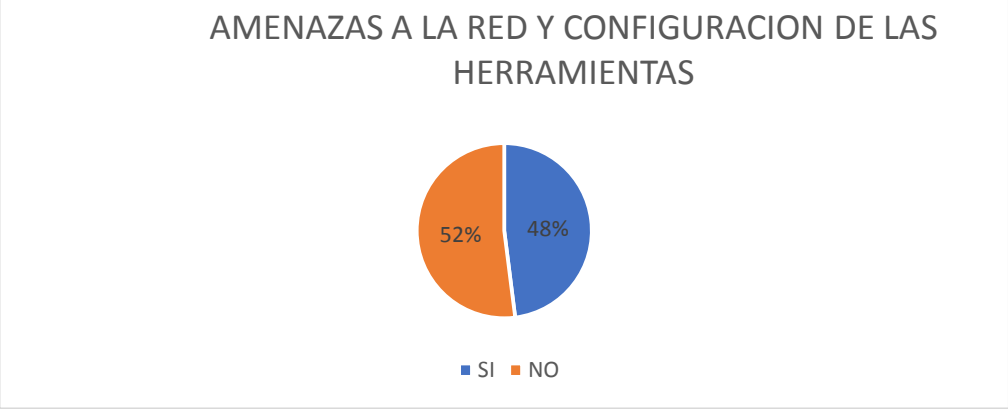


Ilustración 7 porcentaje de amenazas a la red

Con el instrumento de recolección aplicado a los 20 colaboradores se determinó que el 52% desconoce ciertos parámetros de seguridad que se deben tener en cuenta en la red en base a la seguridad ya sea esta por falta de capacitaciones por parte de los directivos sobre los riesgos a los que está expuesta una red que contienen información sanitaria.

Una vez analizados los resultados de forma individual se llegó a determinar que no cumplen con los parámetros de seguridad, por lo que se deberían aplicar para mejorar la seguridad en la red, se puede notar a simple vista que el 52% tiene y ha tenido dificultades a la hora de proteger la información que operan ya sea por falta de conocimiento o indolencia por parte de los encargados de llevar la seguridad en la red.

Los problemas más comunes son:

- Falta de capacitación a los empleados.
- Desconocen cómo proteger la red de las amenazas de virus
- Falta de conocimiento en caso de contaminación de virus, malware.

3.2.2. La seguridad en la red y las medidas que se deben tener en cuenta en su ordenador.

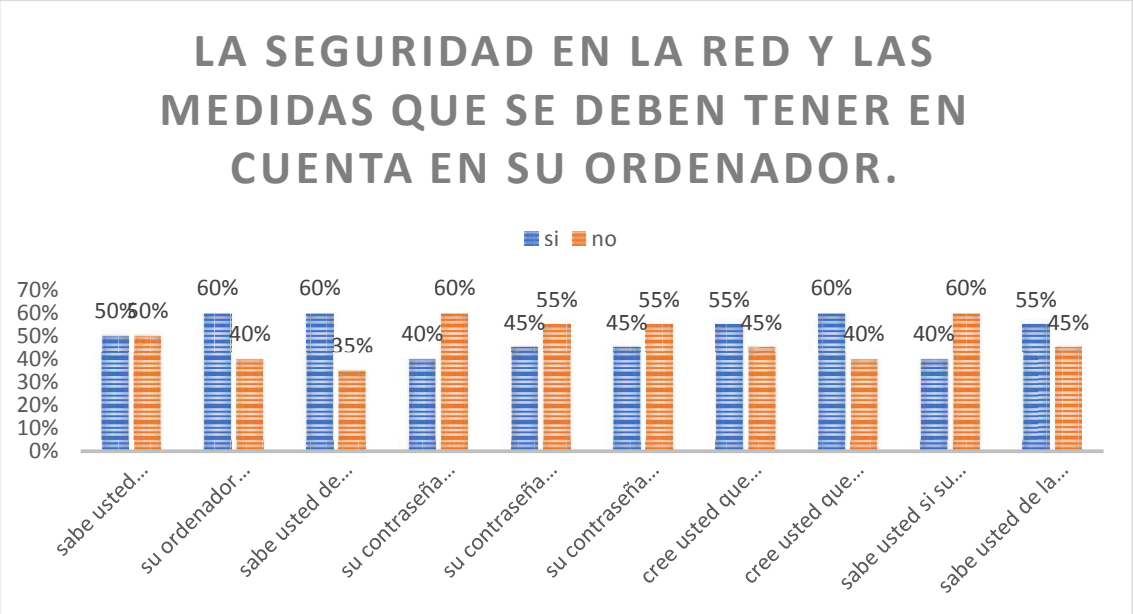


Ilustración 8 seguridad en la red

En la ficha de este instrumento aplicado se notó que el 60% conoce los parámetros de seguridad sobre los caracteres que debe contener una contraseña de seguridad para su ordenador mientras que el otro 40% desconoce tales parámetros, así mismo un 50% conoce los diferentes parámetros de las normas de seguridad que se deben tener en su ordenador para brindarle mayor seguridad según los parámetros de seguridad en redes.

Por lo consiguiente se llegaron a determinar ciertos inconvenientes de seguridad los mismo que son los siguientes:

- Falta de configuración adecuada del firewall de equipo.
- El poco conocimiento de la importancia sobre el firewall de equipo.
- No tener conocimiento sobre las actualizaciones del equipo.

3.2.3. Norma ISO/IEC 27033 y Estándar IEEE 802.10

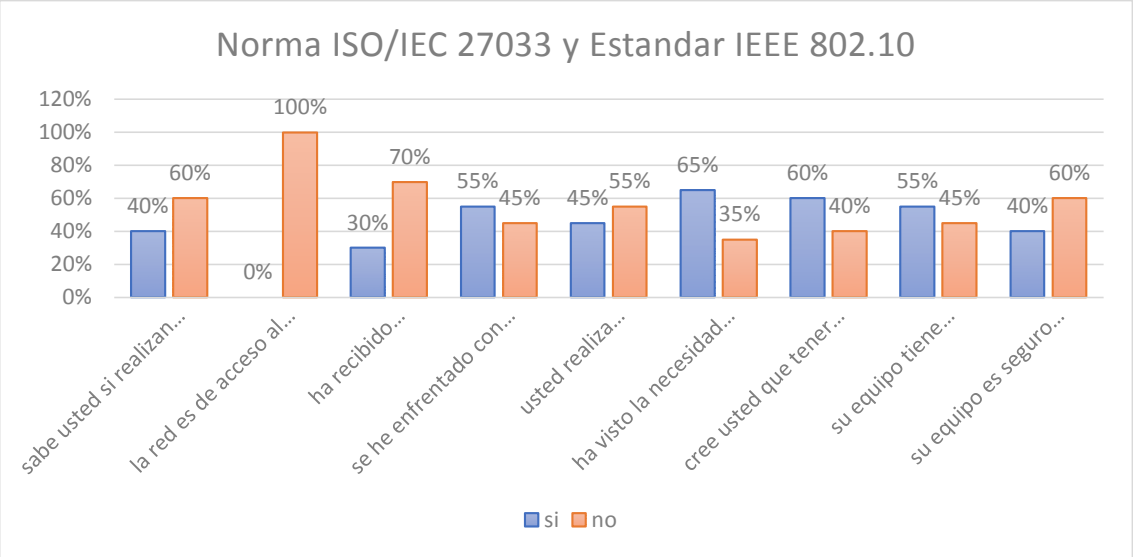


Ilustración 9 norma ISO

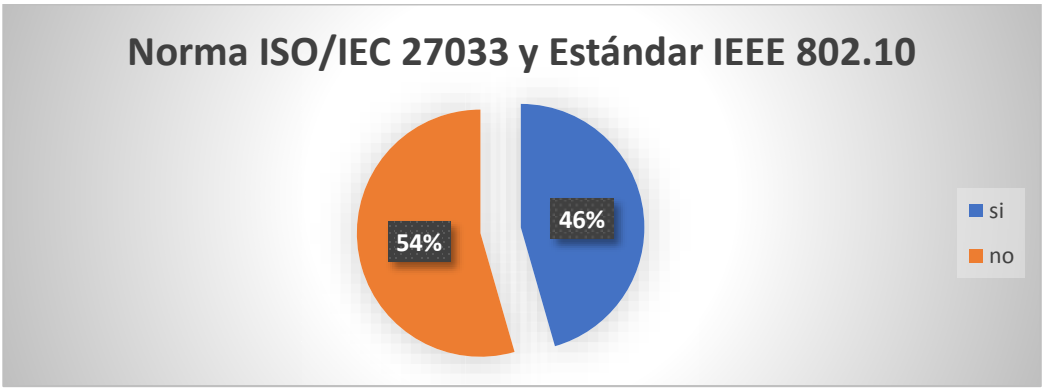


Ilustración 10 porcentaje de Norma y Estándar

Los resultados que se obtuvieron con el instrumento aplicado sobre los estándares de seguridad proporcionaron que el 46% de los empleados en un rango promedio sobre la seguridad de la red, y un 54% demuestra que no se aplican ciertos aspectos de seguridad de redes.

Sobre los resultados acerca del estándar IEEE 802.10 de las medidas que se deben establecer existe tan solo el 54% que se cumple con ciertos parámetros de seguridad de red de la población respectiva analizada.

3.3. Situación Actual

Sabemos que la tecnología va creciendo y que las inseguridades a través de las redes se hacen cada vez más frecuente por lo que se debe implementar medidas de seguridad para evitar los riesgos que afectan a la red y las vulnerabilidades que existen como el hurto, robo de información, duplicidad o la fuga del activo más importante de la institución que es los datos.

Para conocer cómo se encuentra la situación actual del Distrito de Salud 13D05, se debe analizar el entorno de la información y las medidas de seguridad que se emplean en ella, de acuerdo con eso se utilizaron herramientas para mejorar el rendimiento o respaldar dicha información, justificando de esta manera el estudio de la seguridad de red dentro del Distrito 13D05 de Salud.

3.4. Características del Proyecto

3.4.1. Naturaleza del Proyecto

En el presente trabajo lo que se quiere lograr es realizar un estudio de viabilidad con el objetivo principal de comprobar si existen riesgos y vulnerabilidades que afecten la red en el Distrito de Salud 13D05.

3.4.2. Importancia

Es importante Implementar herramientas de seguridad de redes que ayuden a respaldar dicha información dentro del distrito de Salud 13D05.

3.4.3. Localización

El presente trabajo fue aplicado en el Distrito de Salud 13D05 El Carmen Zona-4

3.5. Estudio técnico

3.5.1. Recursos Humanos

Autor	Valdez Toral Carlos Daniel
Tutor de tesis	A.S. Javier Zambrano Quiroz

Tabla 4 recursos Humanos
Autor: Carlos Valdez

3.5.2. Recursos Tecnológicos

Recursos	Características
Computadora portátil con un procesador Intel i3 8th Generación, 4GB RAM, Disco duro 1TB, Windows 10 Profesional.	• Instrumento principal para elaboración y redacción de la tesis • Prueba y recopilación de información de las herramientas aplicadas.
Nmap	• La mayoría de los sistemas operativos son compatibles • Permite escanear los puertos de las redes, realiza auditorias de seguridad • admite docenas de técnicas avanzadas para trazar redes llenas de filtros IP, firewalls, enrutadores y otros obstáculos
Nessus	• Identifica las vulnerabilidades que requieren atención con un escaneo preciso. • Rentable para empresas de todos los tamaños.
Tinywall	• bloquea activamente cientos de troyanos, virus y gusanos. • evita que los programas maliciosos modifiquen la configuración del Firewall de Windows

Tabla 5 Recursos Tecnológicos
Autor: Carlos Valdez

3.6. Factibilidad

3.6.1. Técnica

En este estudio de seguridad de redes su mayor y principal objetivo está el análisis y protección de la red con herramientas de seguridad las mismas que protegerán en tiempo real la red del Distrito de Salud, además se recolectara toda la información necesaria para llevar a cabo este estudio.

3.6.2. Operativa

Este estudio permite conocer al Distrito sobre los tipos de vulnerabilidades a los que se encuentran expuestos, por lo que fue necesario aplicar instrumentos de recolección de información para determinar la importancia que tiene la aplicación de estas herramientas de análisis y protección de redes, las que estarán bajo la supervisión del departamento de TIC una vez ejecutadas.

3.6.3. Económica

La realización de este estudio es factible económicamente porque en este no se generan gastos excesivos para llevarlo a cabo, las herramientas tienen su versión gratuita por un determinado tiempo de 15 días, por lo que si se utiliza la versión completa brindara mayor seguridad, además se utilizó una laptop para el análisis como también el levantamiento de información y material de apoyo para los respectivos instrumentos de recolección de información.

Descripción	Costo aproximado
Laptop Asus Core i3 8th Generación	$500
Material de apoyo (copias de encuestas y entrevista)	$ 3.00

Nesus (herramienta de análisis y protección)	$8.011.50

3.6.4. Conclusión del estudio

Si es factible dicho estudio porque se realizaron los respectivos análisis y protección en la red con las herramientas ya propuestas de la cuales se obtuvieron resultados de vulnerabilidades, uno de los más encontrados fueron los conocidos como malwares en la red del Distrito de Salud 13D05, con el cumplimiento de los estándares de calidad y el previo uso de las herramientas instaladas estarán protegidos de este tipo de amenazas en los diferentes sistemas operativos como también la información de los usuarios.

4 Herramientas de seguridad para la red del Distrito de Salud 13D05.

4.1 Instalación de herramientas y comprobación de vulnerabilidades.

4.1.1 Instalación de Nmap y análisis de red

- Una vez descargada la herramienta se procederá a instalarla aceptando los términos de usos, se nos creará un icono en el escritorio.

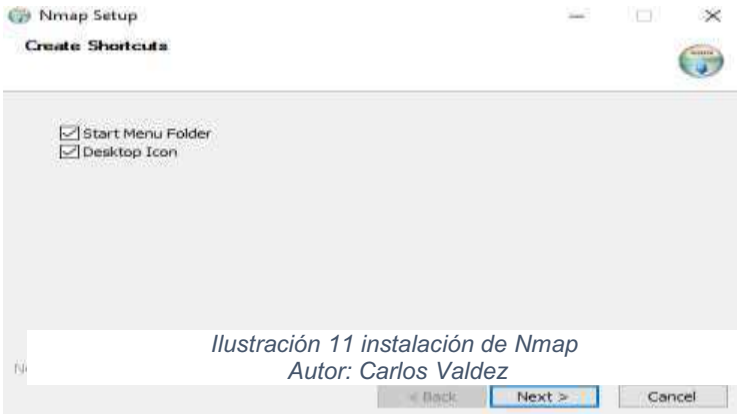


Ilustración 11 instalación de Nmap
Autor: Carlos Valdez

- Una vez aceptada las opciones de instalación se procederá a instalar dicha herramienta

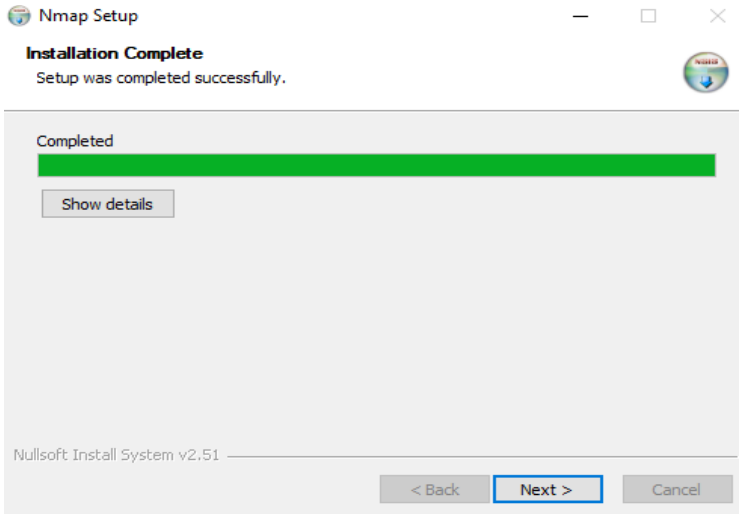


Ilustración 12 finalización de Nmap
Autor: Carlos Valdez

- Como se puede notar en el primer escaneo de Nmap bajo su entorno gráfico se procedió a realizar el respectivo análisis en la dirección IP

192.168.20.16 de las maquinas del Distrito de Salud 13D05 obteniendo como resultado lo siguiente.

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-18 11:00 Hora est. Pacífico, Sudamérica
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 11:00
Completed NSE at 11:00, 0.00s elapsed
Initiating NSE at 11:00
Completed NSE at 11:00, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 11:00
Completed Parallel DNS resolution of 1 host. at 11:00, 0.10s elapsed
Initiating SYN Stealth Scan at 11:00
Scanning 192.168.20.116 [1000 ports]
Discovered open port 135/tcp on 192.168.20.116
Discovered open port 139/tcp on 192.168.20.116
Discovered open port 445/tcp on 192.168.20.116
Discovered open port 5357/tcp on 192.168.20.116
Completed SYN Stealth Scan at 11:00, 0.81s elapsed (1000 total ports)
```

Ilustración 13 análisis de la IP
Autor: Carlos Valdez

- Escaneara 4 servicios es decir 1 host de la dirección IP de la máquina que se está realizando la detección. Se puede ver que el host este activo con una latencia de 0.000097 segundos y 965 puertos cerrados que no se muestran.

```
Initiating Service scan at 11:00
Scanning 4 services on 192.168.20.116
Completed Service scan at 11:00, 11.12s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against 192.168.20.116
Retrying OS detection (try #2) against 192.168.20.116
Retrying OS detection (try #3) against 192.168.20.116
Retrying OS detection (try #4) against 192.168.20.116
Retrying OS detection (try #5) against 192.168.20.116
NSE: Script scanning 192.168.20.116.
Initiating NSE at 11:00
Completed NSE at 11:01, 30.22s elapsed
Initiating NSE at 11:01
Completed NSE at 11:01, 0.04s elapsed
Nmap scan report for 192.168.20.116
Host is up (0.000097s latency).
Not shown: 996 closed ports
```

Ilustración 14 escaneo de Host
Autor: Carlos Valdez

- En esta parte del escaneo se puede ver el sistema Operativo que se está utilizando y los servicios que se ejecutaron en la red en los puertos TCP 135 msrpc,139 netbios,445 microsoft-ds,5357 http.

```
Host is up (0.000097s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
```

```
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.70%E=4%D=7/18%OT=135%CT=1%CU=39507%PV=Y%DS=0%DC=L%G=Y%TM=5D3097
OS:D6%P=i686-pc-windows-windows)SEQ(SP=106%GCD=1%ISR=10C%TI=I%CI=I%II=I%SS=
OS:S%TS=U)OPS(O1=MFFD7NW8NNS%O2=MFFD7NW8NNS%O3=MFFD7NW8%O4=MFFD7NW8NNS%O5=M
OS:FFD7NW8NNS%O6=MFFD7NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF
OS:70)ECN(R=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A
OS:=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=
OS:Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%R
OS:D=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=
OS:0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U
OS:1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DF
OS:I=N%T=80%CD=Z)
```

Ilustración 15 detección de sistema
Autor: Carlos Valdez

- la distancia de red que se nos muestra en esta parte es de 0 saltos, los resultados que la dirección IP escaneada fue en 195.47 segundos.

```
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2019-06-27 08:22:38
|_  start_date: N/A

NSE: Script Post-scanning.
Initiating NSE at 08:23
Completed NSE at 08:23, 0.00s elapsed
Initiating NSE at 08:23
Completed NSE at 08:23, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 195.47 seconds
           Raw packets sent: 1080 (51.090KB) | Rcvd: 2195 (97.460KB)
```

Ilustración 17 resultados de la IP
Autor: Carlos Valdez

- Puertos y servidores se nos muestra a continuación los que fueron analizados

Salida Nmap | Puertos / Servidores | Topología | Detalles del servidor | Escaneos

Puerto	Protocolo	Estado	Servicio	Versión
135	tcp	open	msrpc	Microsoft Windows RPC
139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445	tcp	open	microsoft-ds	
5357	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

Ilustración 16 Puertos y servidores
Autor: Carlos Valdez

- La topología de la red es ponderada como se muestra gráficamente

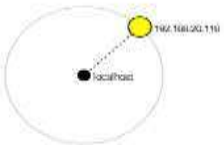


Ilustración 18 topología
Autor: Carlos Valdez

- Por último, tenemos los detalles del servidor con sus puertos abiertos y los cerrados ya mencionados anteriormente.

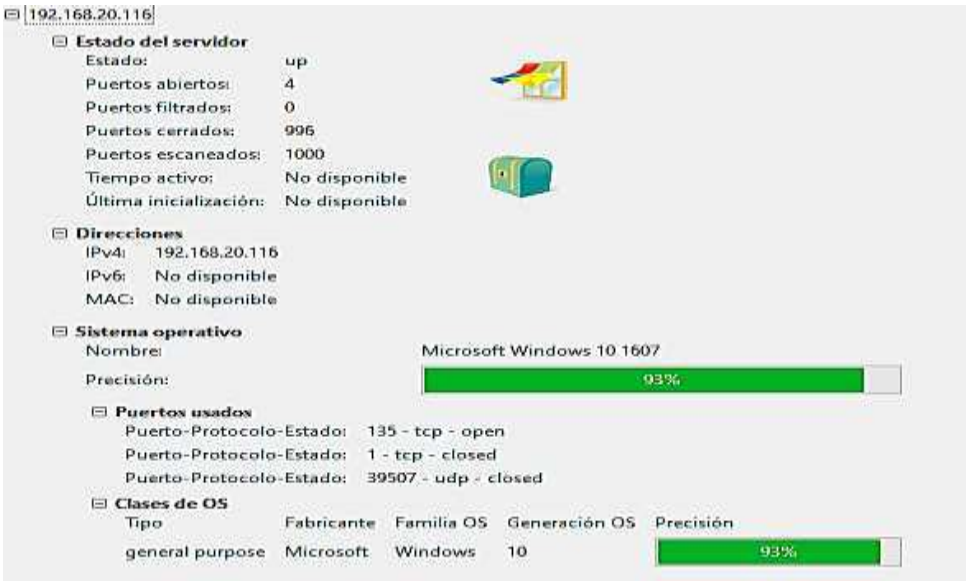


Ilustración 19 Puertos abiertos
Autor: Carlos Valdez

4.1.2 Ejecución y pruebas de Nessus

- Como podemos ver en esta imagen encontramos en diferentes versiones de sistemas Operativos, también existen varias versiones de esta herramienta.

Ilustración 20 descarga de Nessus
Autor: Carlos Valdez

- Una vez descargado, nos registramos para obtener una clave de activación, después accederemos en el navegador en la dirección de https://localhost:8834/#/ rellenamos los datos de inicio de sesión y después esperamos a que se descarguen todos los paquetes o componentes de Nessus para su completo funcionamiento.

Ilustración 21 registro en Nessus
Autor: Carlos Valdez

- En esta herramienta existen ciertas clases de análisis y protección, entre las cuales tenemos Escaneo de malware y detección de bloqueo de información las mismas que utilizamos para el respectivo estudio.

Ilustración 22 Selección de opciones
Autor: Carlos Valdez

- Los componentes utilizados de esta herramienta fue la detección de malware para verificar si estas tenían estas vulnerabilidades en la red y sus equipos dando como resultado 10 vulnerabilidades, una de nivel crítico y de nivel alto por lo tanto queda demostrada la eficiencia de dicha herramienta detectando el peligro en la red.

Ilustración 23 Detección de Malware
Autor: Carlos Valdez

- Se realizó una respectiva búsqueda en la opción de análisis de bloqueo donde se encuentran los controles remotos y locales para CVE2016-2018, donde se encontraron dos vulnerabilidades de información.

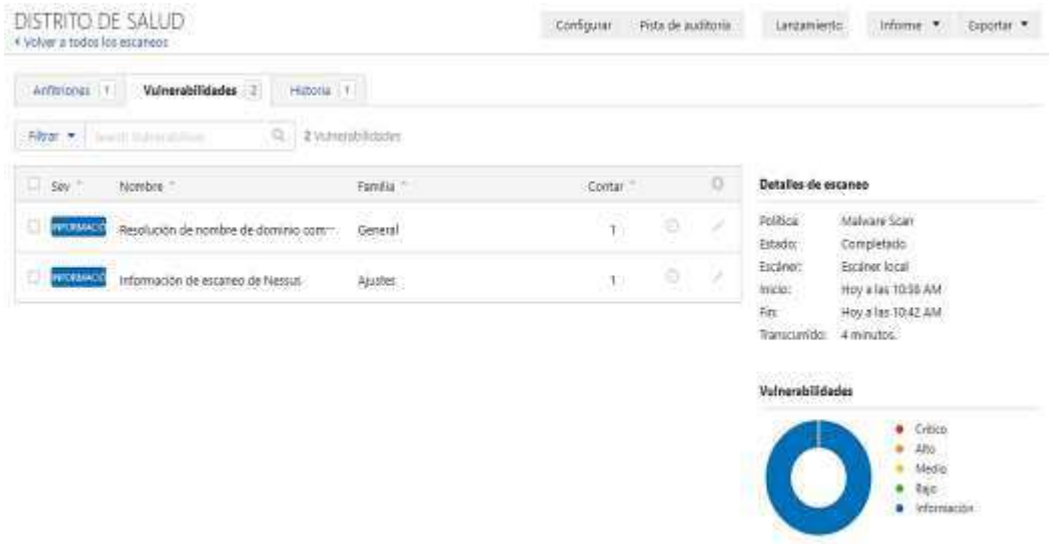


Ilustración 24 Análisis de Bloqueo
Autor: Carlos Valdez

4.1.3 Tinywall

- Herramienta de seguridad la encontramos desde su sitio web oficial https://tinywall.pados.hu/, siendo esta una de las mejores herramientas de protección en tiempo real que refuerza y a la vez controla el firewall en los sistemas actuales dando mayor seguridad al usuario mientras trabaja.

- Iniciamos la instalación

Ilustración 25 iniciamos la instalación
Autor: Carlos Valdez

- Estos son los servicios y aplicaciones las que se pueden seleccionar para darle un mejor funcionamiento a la herramienta de acuerdo al usuario como desee utilizarla.

Ilustración 26 servicios de aplicaciones
Autor: Carlos Valdez

- A la misma vez también se puede realizar un análisis de las aplicaciones que tendrán acceso a la red y los modos a los que tenemos acceso.

Ilustración 28 detección de aplicaciones
Autor: Carlos Valdez

-

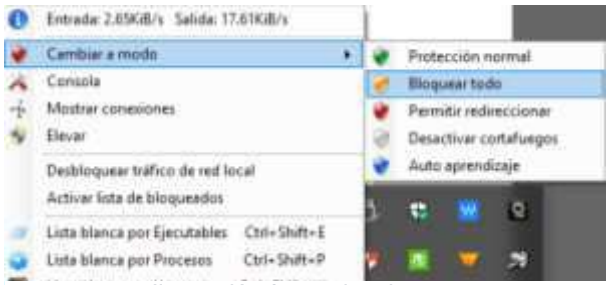


Ilustración 27 modos de acceso
Autor: Carlos Valdez

4.2 Resolución del estudio

Ante la comprobación que hemos realizado dentro de las herramientas y revisado las vulnerabilidades que existen tanto de virus o bloqueos de información hemos llegado a la conclusión de que se necesitan ciertas herramientas que garanticen la prevención de las vulnerabilidades a las que esta expuesta la red y el correcto análisis de la misma.

4.3 Resultados obtenidos

4.3.1 Mecanismos utilizados para la seguridad

Con el propósito de detectar y proteger se utilizaron las herramientas de Nmap y Nessus en la cual se encontraron ciertas amenazas como lo son los malware, bloqueos de información en la red, que para prevenir y corregir estas vulnerabilidades se llegó a determinar la necesidad de instalación de dichas herramientas, de la misma manera la creación de usuarios con su respectiva contraseñas con el objetivo de resguardar el ingreso y utilización del computador de personas no autorizadas evitando el robo de información o la perdida de la misma.

Como herramienta de prevención y corrección se utilizó TinyWall la misma que se encargara y/o tendrá como función principal bloquear el ingreso de malware a las computadoras por medio de páginas web con contenidos de infiltración o aplicaciones de que contengan algún virus además esta evitara que programas alteren la configuración del firewall dándole a este una configuración segura, cuenta también con una interfaz fácil de utilizar donde se podrá configurar que aplicaciones instaladas en los equipos podrán tener acceso a la red controlando la entrada y salida de datos además de poder bloquear el tráfico o el acceso de a la red mientras no se esté utilizando el computador, cuenta además con una lista blanca la misma que se utiliza para las aplicaciones que son necesarias que tengan acceso a la red.

4.3.2 Creación de usuarios y contraseñas

- En esta sección se procedió a crear el usuario de administrador con una contraseña segura la que tendrá símbolos, letras y caracteres especiales.

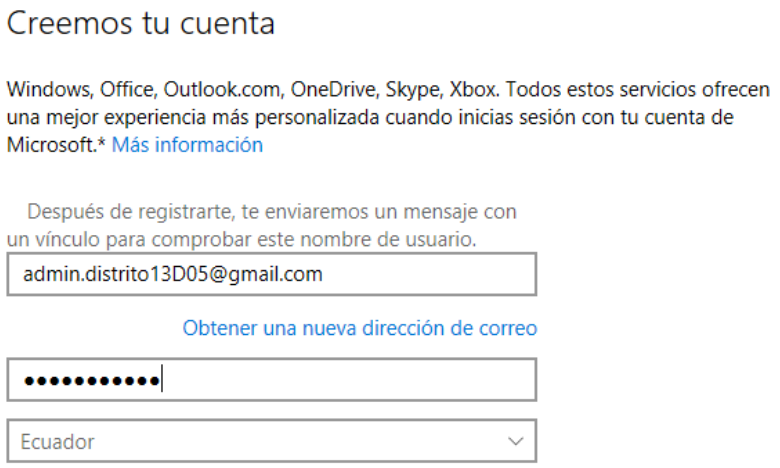


Ilustración 29 creación de administrador y contraseña
Autor: Carlos Valdez

- Cambiamos a administrador de usuario estándar, así el equipo de cada usuario estará protegido de ser manipulado por terceros.

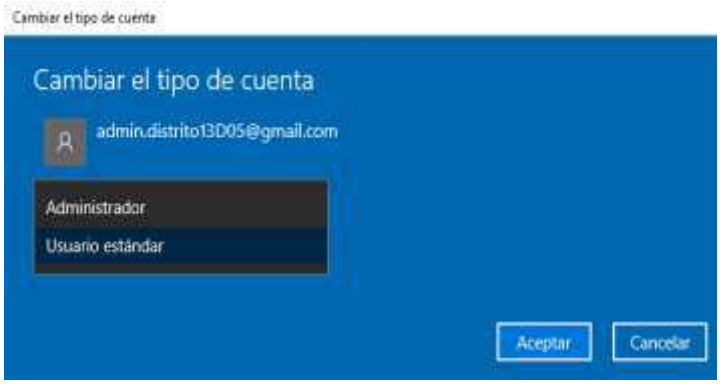


Ilustración 30 cambio de modo a administrador
Autor: Carlos Valdez

4.3.3 Pruebas de bloqueo y protección con TinyWall

Para esta prueba se utilizó una de sus configuraciones que tiene la herramienta como método de protección donde se intentó ingresar a una página web de las que contienen malwares por lo que se pudo obtener como resultado el bloqueo inmediato de dicha página evitando y corrigiendo el ingreso a este tipo de páginas, TinyWall por ser unos de los firewalls más seguros ofrece el bloqueo de aplicaciones por completo es decir no necesariamente habría que bloquear cada una de sus extensiones de las aplicaciones, sino que lo aria totalmente.

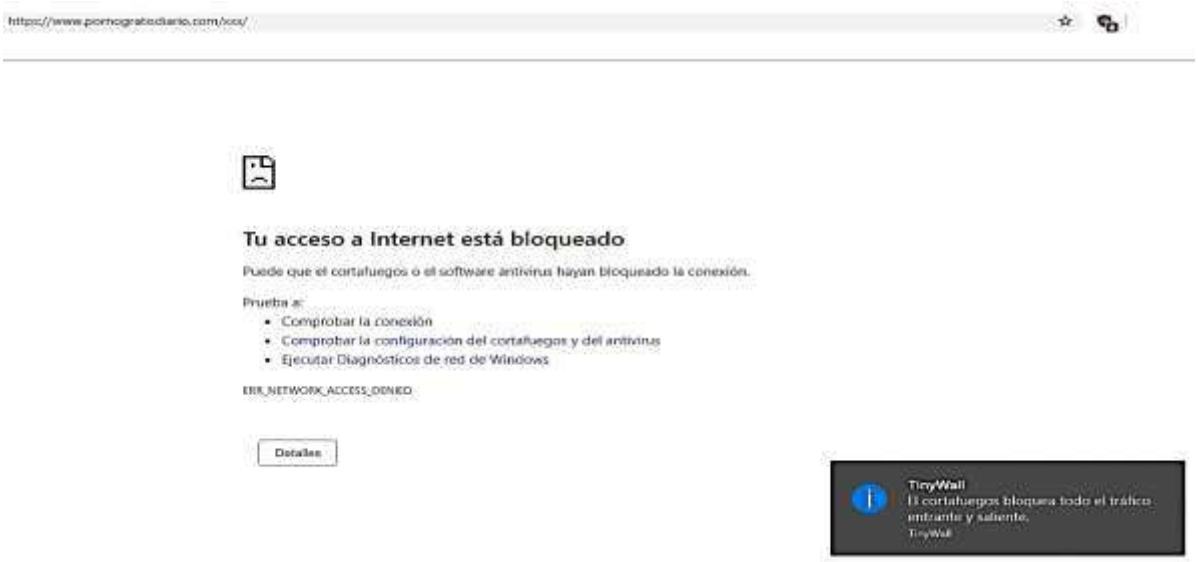


Ilustración 31 protección de páginas con malwares
Autor: Carlos Valdez

- TinyWall además ofrece la protección y bloqueo de aplicaciones a la cual se las puede restringir de tener acceso a la red, bloquear el tráfico a la misma o permitirles tener acceso solo ah algunos puertos específicos.

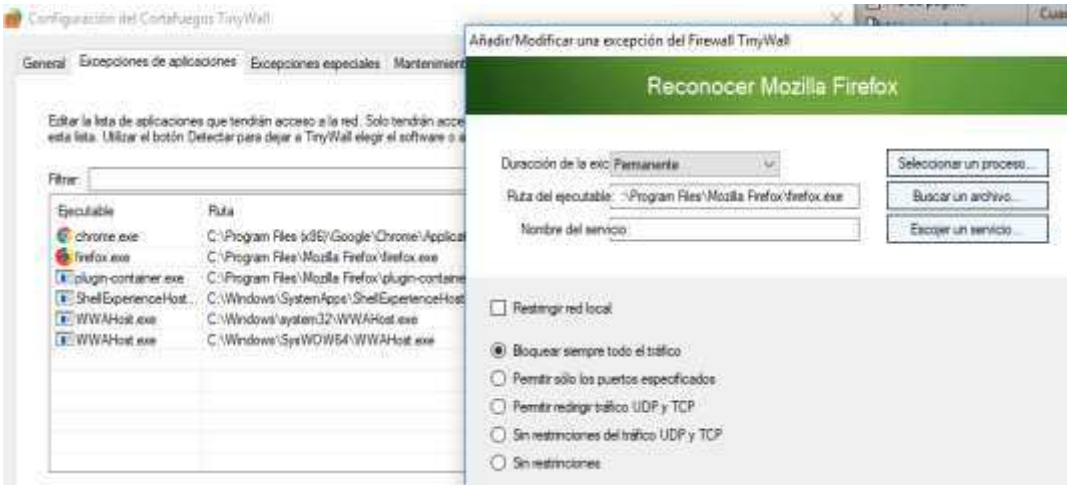


Ilustración 32 bloqueo de aplicaciones
Autor: Carlos Valdez

- para esta prueba se ha escogido la aplicación de Mozilla Firefox la misma que se utilizó para comprobar la eficacia de esta herramienta a la que se le bloqueo todo el tráfico de red dejándola sin acceso a la red.

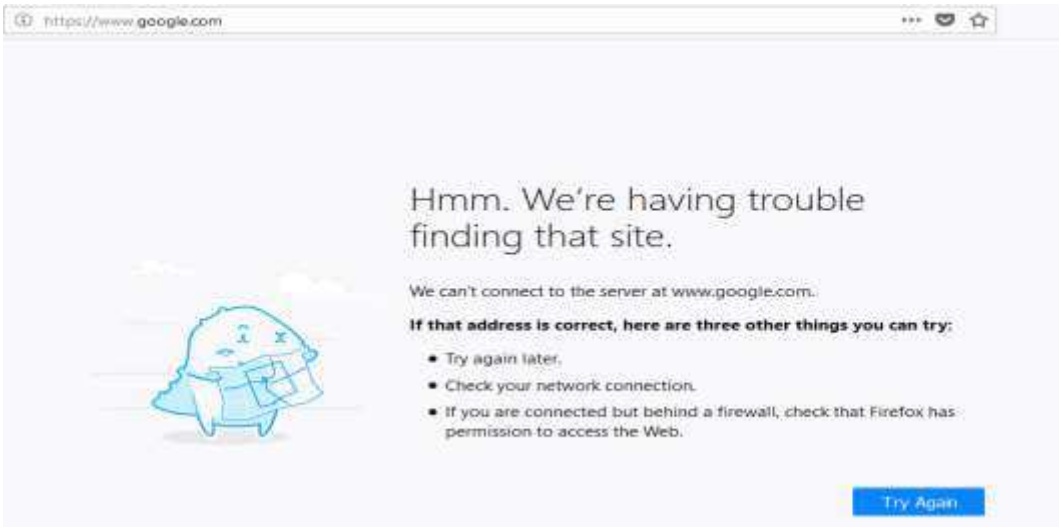


Ilustración 33 comprobación de bloqueo de aplicación
Autor: Carlos Valdez

4.3.4 Análisis de las herramientas utilizadas para la protección de la red de datos del Distrito 13D05 El Carmen.

Las herramientas utilizadas en este estudio son las más eficaces al momento de analizar y asegurar la calidad en la red, entre las más comunes destacamos a Nessus que inicia escaneando los puertos con Nmap uno de los escaneadores de vulnerabilidades más utilizado en el mundo, estas herramientas son adaptables a cualquier tipo de empresas con el mismo objetivo de brindar seguridad y detección de vulnerabilidades utilizada por los expertos en seguridad informática cuando tienen que realizar auditorías y como herramienta de prevención y corrección se utilizó TinyWall la misma que se encargara y/o tendrá como función principal bloquear el ingreso de malware a las computadoras por medio de páginas web con contenidos de infiltración o aplicaciones de que contengan algún virus además esta evitara que programas alteren la configuración del firewall dándole a este una configuración segura.

5 CONCLUSIONES

- Según los resultados obtenidos se determina que la información fue satisfactoria para la fundamentación teórica la que permitió conocer más sobre la seguridad de la red e información sanitaria.

- La recopilación de información mediante las técnicas de la encuesta y entrevista permitieron encontrar que los empleados del Distrito de Salud se sienten seguros con la implementación de las herramientas de seguridad de redes. Sin embargo, debido a la falta de mantenimiento adecuado estas se volverán obsoletas.

- La realización de la autoría permitió gestionar las vulnerabilidades que pudieran estar presentes en el sistema, además de conocer la situación exacta de la que está expuesta la información en cuanto a protección, control y medidas de seguridad, se mostró el funcionamiento actual de la red la misma que no cumple con los parámetros de seguridad bajo ciertas normas de seguridad como lo es la ISO/IEC 27033.

- Al sugerir las herramientas de seguridad de redes se dio a conocer la importancia que es contar con estas herramientas de redes para la protección de la misma, obteniendo como resultado respuestas aceptables al realizar los análisis, la detección de vulnerabilidades y protección de dichas afecciones en la red.

- La implementación de las herramientas de análisis y seguridad de redes ayudaran a todos los empleados del Distrito 13D05 de SALUD-El Carmen a detectar y proteger fácilmente los equipos de los usuarios de las amenazas que asechan en la red.

6 RECOMENDACIONES

- En cuanto al análisis realizado sobre el estudio de seguridad en redes e información sanitaria se sugiere que se implementen estos tipos de herramientas para mejorar y fortalecer la seguridad de la red en posteriores estudios de seguridad que se realicen en cualquier institución.

- La utilización de herramientas de seguridad es necesarias e importantes en cuanto a la protección en redes por lo que es recomendable que se tengan en los equipos de trabajo de cualquier empresa.

- Para tener una mejor gestión en la red se debe tener en cuenta el elaborar un plan estratégico el cual este basado en la seguridad de redes, para poder implementar de cada uno de los controles basados en la ISO/IEC 27033 acorde a las necesidades prioritarias como lo es proteger la información.

7 Bibliografía

Musser, G. (2017). BioKIDS - Rodent. *Britannica*, 10.

Alfau Ascuasiati, A. (2012). *Plagas domésticas.* España: Palibro.

Alonso, N. O. (2013). *Redes de comunicaciones industriales.* Madrid: ISBN.

Alvira, M. F. (2011). *La encuesta: una perspectiva general metodológica.* Madrid: consejo.

Andrés, J. M. (2014). *Gestión sanitaria: Calidad y seguridad de los pacientes.* : diaz de santos.

Arantes, S. C. (2015). *Gestión de redes telemáticas.* España: Elearning S.L .

Bishop, R. (2007). *Mechatronic Systems, Sensors, and Actuators.* Texas: Francis Group.

Bonnefoy, X., Kampen, H., & Swweney, K. (2008). *Public Health Significance of Urban Pests.* Word Health.

Buckle, A., & Smith, R. (2015). *Rodent Pests and their Control.* Boston: CABI.

Cegarra, S. J. (2004). *Los métodos de investigación.* Madrid: Ediciones Díaz de Santos.

Cerdá Filiu, L. M. (2014). *Instalaciones eléctricas y automatismos.* Madrid: Paraninfo, S.A.

Chambers, L., Lawson , M., & Lyn , H. (2006). Control biológico de Roedores- el caso para el. 28.

Coates , R., & Estrada, A. (1986). *Identificación de campo de los mamíferos de la Estación de Biología "Los Tuxtlas.* Mexico: UNAM.

Corona Ramírez, L. G., Abarca Jiménez, G. S., & Mares Carreño, J. (2014). *Sensores y actuadores aplicaciones con arduino.* Mexico: Patria S.A.

Costas, S. J. (2014). *Seguridad Informatica.* Madrid, España: RA-MA.

Daneri, P. (2008). *PLC Automatizacion y Control Industrial.* Buenos Aires: Hispano Americana S.A.

Everett, H. (2010). *Sensors for Mobile Robots.* California: CRC Prees.

Gasco, G. E. (2015). *Seguridad informatica.* Madrid: Macmillan.

Gascó, G. E., & Serrano, M. R. (2015). *Seguridad Informatica.* Madrid: Macmillan Iberia, S.A.

Gómez, J. A. (2013). *Servicios en Red.* Madrid: editex.

Grifols, V. (2014). *La informacion sanitaria y la participacion activa de los usuarios.* Barcelona: Graficas Hisper.

Haus, J. (2010). *Optical Sensors: Basics and Applications.* Germany: WILEY-VCH.

Jaramillo, I. D. (2010). *Método y conocimiento: metodología de la investigación : investigación.* Colombia: fondo editorial.

Krebs, C. (2013). *Population Fluctuations in Rodents.* Chicago: University of chicago.

Landete Castillejos, T., & Cerro Barja, A. (1998). *La Rata de Alcantarilla: Ecologia, comportamiento y control.* Cuenca: Universidad de Castilla-La Mancha.

Linares Gonzales, V. (2015). *Diagnosis de averias y mantenimiento correctivo de sistemas de automatizacion industrial.* Malaga: IC Editorial.

Maloney, T. (2006). *Electronica Industrial Moderna.* Mexico: Pearson.

Mandado Pérez , E., Acevedo, J., Silva, C. F., & Aresto Quiroga, J. I. (2009). *Automata programables y sistemas de automatizacion.* Barcelona : MARCOMBO, S.A.

Martínez. (2014). *tecnicas e instruemntos de recogida y Analisis de Datos.* España: Edit- S.A.

Martínez, M. C. (2014). *Tecnicas e Intrumentos de recogida y Análisis de datos.* España: Edit- S.A.

Moguel, E. A. (2005). *Metodología de la Investigación.* Mexico: tabasco.

Namakforoosh, M. N. (2012). *Metodología de la investigación.* Mexico: limusa.

Onwubolu, G. (2005). *Mechatronics principles and Applications.* Oxford: Elsevier.

Orueta, G. D. (2014). *Procesos y herramientas para la seguridad de redes .* Madrid: Uned .

Pérez Garcia, M. A. (2014). *Instrumentación electrónica.* Madrid: Parainfo, S.A.

Quesenberry, K., & Carpenter , J. (2012). *Ferrets, Rabbits and Rodents.* ELSEVIER.

Ramos, M. d. (2011). *Seguridad Informatica ED.* Madrid: Paraninfo S.A.

Rossini, L., Guharay, F., & Zamora, N. (2003). *Estrategia sostenible para el control de los roedores.* Managua: Pascal Chaput.

Salvador, J. C. (2014). *Transparencia del sistema sanitario.* Madrid: Diaz de Santos.

Santos, J. C. (2014). *Diseño de redes telemáticas.* Madrid, España: RA-MA.

Schiller, J., Douang Boupha , B., & Bounnaphol, O. (2011). Rodents in Agriculture in the Lao PDR — a Problem with an Unknown Future. 16.

Stallings, W. (2014). *Fundamentos de seguridad en redes: aplicaciones y estándares.* Madrid: pearson.

Toro, J. A. (2015). *UF1874 - Mantenimiento de la infraestructura de la red de comunicaciones.* España: Elearning S.L.

Torrente Artero, O. (2013). *Arduino curso practico de formación.* Madrid: RC Libros.

Urbina, G. B. (2016). *Introducción a la seguridad informática.* Mexico: Ebook.

Vallés, B. (2014). *Necesidades de información de los usuarios de Servicios Sanitarios de atencion primaria de salanca.* España: Universidad de Salamanca.

Valverde. (2015). *Metologias de la Investigacion .* Madrid: R-ma.

Wodzicki, K. (2010). Prospects for biological control of rodent populations. *Bull. Org. mond. Sant* , 6.

Wolff, J., & Sherman, P. (2007). *Rodent Societies: An Ecological and Evolutionary Perspective.* Chicago: The university of chicago.

8 ANEXOS

	NOMBRE DEL DOCUMENTO: NOTIFICACIÓN DE DESIGNACIÓN DE TUTORES	CÓDIGO: PAT-01-F-007
Uleam	PROCEDIMIENTO: TITULACIÓN DE ESTUDIANTES DE GRADO	REVISIÓN: 1.
		Página 1 de 8

COMISIÓN ACADÉMICA
CARRERA DE INGENIERÍA EN SISTEMAS

MEMORANDUM No. 036-CA-2019

PARA: A.S. Javier Zambrano Quiroz, Msc.
DE: Ing. Milton Zambrano Rivera, Msc.
ASUNTO: **Designación para desarrollar tutorías de titulación**

FECHA: El Carmen a 11 de octubre de 2019

En cumplimiento a la distribución de la carga horaria dispuesta dentro de la planificación académica de esta unidad y considerando los artículos 76 y 77 del proceso de titulación del Reglamento de Régimen Académico, la Comisión Académica de la Carrera de Ingeniera en Sistemas de la Extensión el Carmen ha considerado que, de acuerdo con su experticia en el área de conocimiento asignado, usted deberá dirigir y verificar el desarrollo del trabajo de titulación de la siguiente estudiante:

Estudiante/s	Nivel	Modalidad de Titulación	Tema de investigación
VALDEZ TORAL CARLOS DANIEL	Primera Prorroga	Proyecto de Investigación	Estudio de seguridad en Redes para la información sanitaria en el Distrito de Salud 13D05 El Carmen

Cabe señalar que este trabajo deberá ser presentado según el calendario 2019(2) para titulación y en forma mensual se deberá reportar a Comisión Académica las tareas realizadas en dicho trabajo.

Particular que se informa para los fines consiguientes.

Atentamente,

Ing. Milton Zambrano Rivera
Presidente Comisión Académica
Correo Electrónico Institucional: milton.zambrano@uleam.edu.ec

cc. Sr. VALDEZ CARLO DANIEL
Elaborado por: Wladmir Minaya

anexo 1 Asignación de Tutor

UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ
Proyecto de Investigación "Auditoría y Seguridad Informática"

CERTIFICACIÓN

Quien suscribe Ing. Clara Guadalupe Pozo Hernández, Directora del proyecto de Investigación "AUDITORÍA Y SEGURIDAD INFORMÁTICA" tengo a bien CERTIFICAR:

Que el señor **VALDEZ TORAL CARLOS DANIEL** , portador de la cédula de ciudadanía N° **1725120818,** ha realizado el trabajo de investigación:**" ESTUDIO DE SEGURIDAD EN REDES PARA LA INFROMACIÓN SANITARIA EN EL DISTRITO DE SALUD 13D05 EL CARMEN-ZONA 4 "**, como una actividad del proyecto de investigación, "Auditoría y Seguridad Informática" durante el período 2019(1) y 2019(2) según la planificación y documentación que reposa en los archivos del proyecto.

El señor **VALDEZ TORAL CARLOS DANIEL**, puede hacer uso del presente documento en lo que estime conveniente, dentro del marco legal académico establecido.

El Carmen, 06 de enero del 2020

Ing. Clara Guadalupe Pozo Hernández, Mg.
DIRECTORA DEL PROYECTO

anexo 2 Certificado de Auditoría

URKUND

Urkund Analysis Result

Analysed Document:	TESIS PARA URKUND.docx (D61993095)
Submitted:	08/01/2020 4:08:00
Submitted By:	julijairo71@gmail.com
Significance:	0 %

Sources included in the report:

Instances where selected sources appear:

0

anexo 3 Resultados de URKUND

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ
EXTENSIÓN - EL CARMEN

Encuesta

PROBLEMA: -

Debido a que los usuarios dejan sus equipos y cuentas personales sin ningún tipo de protección, al no conocer o tener el conocimiento acerca de los riesgos informáticos en las redes, tener una contraseña en cada ordenador y tener las herramientas que se encargue del análisis y protección ante cualquier amenaza.

1.- Cuenta usted con un usuario y clave para acceder a su ordenador?

Si ☐ no ☐

2.- Conoce usted las herramientas de seguridad de redes como son: Nessus, pandora, Nagios, Nmap. etc.?

Si ☐ no ☐

3.- Su computador cuenta con alguna herramienta de seguridad de redes?

Si ☐ no ☐ no tengo conocimiento ☐

Herramienta .....

4.- Quienes están a cargo de instalar software de seguridad en su computador?

Administradores ☐ personal de TIC ☐fes ☐ted ☐

5. Su sistema Operativo se encuentra actualizado a la última versión?

SI ☐ NO ☐ no tengo conocimiento ☐

6 ¿Qué navegador web utiliza regularmente en su ordenador?

Chrome ☐ Mozilla ☐ Opera ☐ Otros ☐

7. **Se ha encontrado problemas de seguridad en la red de datos donde se ha visto comprometida la información de los usuarios.**

Si ☐ no ☐ no tengo conocimiento ☐

8. ¿Qué tipo de seguridades tiene en su ordenador?

Seguridad de acceso ☐ rtafuego ☐ tispyware n☐ ngo conocimiento ☐

9. Ha tenido usted algún inconveniente con virus llamados:

Malware ☐ gusanos ☐ spyware ☐ troyanos ☐ no tengo conocimiento ☐

10. Actualmente realizan mantenimientos periódicos sobre la seguridad de redes en las computadoras?

Cada semana ☐ una vez al mes ☐ cada seis meses ☐ unca ☐

11. Realizan capacitaciones acerca de la seguridad de redes hacia los usuarios?

si ☐ no ☐ a veces ☐ o tengo conocimiento ☐

El presente instrumento de investigación cumple con los parámetros para ser aplicado en la encuesta que se realizará a los empleados del Distrito de Salud 13D05 El Carmen

A.S Jaime Zambrano Quiroz MG.

Tutor

anexo 4 Encuesta

EN LA TABULACION DE LA ENCUESTA SE PUEDE NOTAR LA EVALUACION DE ACUERDO A LAS RESPUESTAS DE CADA EMPLEADO T1 HASTA LLEGAR A T20 DONDE "x" SERA SI Y LOS "0" NO

TABULACION DE LA ENCUESTA

P°1	¿Cuenta usted con un usuario y clave para acceder a su ordenador?																			
PERSONAL ENCUESTADOS	T1	T2	T3	T4	T5	T6	T7	T8	T9		T11	T12	T13	T14	T15	T16	T17	T18	T19	T20
ITEMS CALIFICATIVOS																				
SI/NO	x	0	x	x	x	0	x	x	x	x	x	x	x	x	x	x	x	x	x	x

					SUMA
SI	18	NO	2		20

P°2	¿Conoce usted las herramientas de seguridad de redes como son: Nessus, pandora, Nagios, ¿Nmap? etc.																			
P/E	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	T16	T17	T18	T19	T20
SI/NO	x	0	0	0	0	0	0	0	0	0	0	0	x	0	0	0	0	0	0	0

					SUMA
SI	2	NO	18		20

P°3	¿Su computador cuenta con alguna herramienta de seguridad de redes?																			
	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	T16	T17	T18	T19	T20
SI/NO	x		x		0	x		0			x		0		0			0		0
NO TENGO CONOCIMIENTO		x		x			x		x	x		x		x		x	x		x	

							SUMA
SI	4	NO	6	NO TENGO C	10		20

P°4	¿Quiénes están a cargo de instalar software de seguridad en su computador?																			
	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	T16	T17	T18	T19	T20
Administradores					x					x									x	
TIC	x	x	x	x		x	x	x	x		x	x	x	x		x	x	x		x
Jefe															x					
Usted																				

total	
3	Suma
16	20
1	
0	

p°5	¿Su sistema Operativo se encuentra actualizado a la última versión?																			
	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	T16	T17	T18	T19	T20
SI/NO	x		0		0	0		0				0					0			
NO TENGO CONOCIMIENTO		x		x			x		x	x	x		x	x	x	x		x	x	x

TOTAL				
SI	1	NO	6	SUMA
13				20

P°6	¿Qué navegador web utiliza regularmente en su ordenador?																			
	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	T16	T17	T18	T19	T20
Chrome				x																
Mozilla	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Opera																				

total	
1	Suma
19	20
0	

p°7	o con problemas de seguridad en la red de datos donde se ha visto comprometida la informació																						
	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	T16	T17	T18	T19	T20		TOTAL	
si/no	x	0	x		x		x		x		x	0			0		x		x	1		SI 9 NO 3	SUMA
NO TENGO CONOCIMIENTO				x		x		x		x			x	x		x		x				8	20
P°8	¿Qué tipo de seguridades tiene en su ordenador?																						
	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	T16	T17	T18	T19	T20		total	
Seguridad de acceso	x				x						x					x						3	Suma
Firewall		x					x							x								4	20
NO TENGO CONOCIMIENTO			x	x		x		x	x	x		x	x		x		x	x	x	x		13	
p°9	¿Ha tenido usted algún inconveniente con virus llamados:																						
	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	T16	T17	T18	T19	T20		total	
Malware				x																		1	Suma
Troyanos		x								x				x			x			x		5	20
Gusanos			x		x		x					x						x				5	
No Tengo conocimiento	x					x		x	x		x		x		x	x			x			9	
p°10	¿Actualmente realizan mantenimientos periódicos sobre la seguridad de redes en las computadoras?																						
	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	T16	T17	T18	T19	T20		total	
cada semana		x																				1	Suma
Cada Mes							x															1	20
Cada 6 Meses	x		x		x			x		x			x			x		x		x		9	
NO TENGO CONOCIMIENTO				x		x			x		x	x		x	x		x		x			9	
P°11	¿Realizan capacitaciones acerca de la seguridad de redes hacia los usuarios?																						
	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	T16	T17	T18	T19	T20		total	
SI		x					x															2	Suma
NO	x		x	x	x	x			x	x	x	x	x	x	x	x	x		x	x		16	20
A VECES																						0	
NO TENGO CONOCIMIENTO								x										x				2	

Ilustración 34 matriz de la encuesta

Autor: Carlos Valdez

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ
EXTENSIÓN - EL CARMEN

ENTREVISTA

Establecida al Ing. Klever Chica encargado del departamento de **TIC** (Tecnología de la Información) en el Distrito de Salud 13D05- El Carmen.

OBJETIVO:

Esta entrevista tiene como finalidad determinar cuales son las medidas de seguridad que se tiene en el Distrito, conocer acerca de las vulnerabilidades a las que esta expuesta la red.

1. ¿Con que tipo seguridad lógica cuentan los ordenadores de quienes trabajan en el Distrito de Salud?

2. ¿Qué herramientas de protección a la red tienen los ordenadores del Distrito de Salud 13D05?

3. ¿En caso de un ataque a la red con qué plan anti-fallas cuentan?

4. ¿Cada que cierto tiempo realiza mantenimientos de seguridad en la red y en los ordenadores?

5. ¿Cuál es el tipo de amenaza en la red que se detectan con mayor frecuencia en la Institucion?

6. ¿Considera usted que se deba realizar capacitaciones acerca de las amenazas que existen a los usuarios quienes laboran en la institución? ¿Y por qué?

7. ¿Cree usted que la red del Distrito de Salud se utiliza solamente para el trabajo o también para otros fines?

8. ¿Cree usted que al tener Antivirus en las maquinas están libres de ataques y virus en la red?

9. ¿Considera usted que es importante que se deba tener el sistema Operativo actualizado para protegerlos de las nuevas amenazas?

10. ¿Se han presentado inconvenientes en los equipos que tienen acceso a la red tanto personales como del trabajo algún índice de robo de información?

11. ¿Cree usted que es importante contar con herramientas de seguridad que se encarguen del monitoreo y protección de ataques, virus en la red? ¿Y por qué?

El presente instrumento de investigación cumple con los parámetros para ser aplicado en la entrevista que se realizará a el encargado del departamento de TIC del Distrito de Salud 13D05 El Carmen.

A S Jaime Zambrano Quiroz MG

Tutor

anexo 5 Entrevista

FICHA DE RECOLECCIÓN

LAS SIGUIENTES PREGUNTAS FUERON REALIZADAS EN ESTE ESTUDIO TOMANDO EN CUENTA LAS CARACTERÍSTICAS DE LA NORMA ISO/IEC 27033 DONDE SE ENFOCA EN LA SEGURIDAD EN LA RED Y EL ESTÁNDAR IEEE 802.10 SEGURIDAD DE LA INFORMACIÓN.

0	PREGUNTAS		
	AMENAZAS A LA RED Y CONFIGURACIÓN DE LAS HERRAMIENTAS.	SI	NO
1	¿Usted ha recibido ayuda en caso de pérdida de información por contaminación de su equipo?		
2	¿Su equipo se encuentra protegido ante los ataques informáticos y virus?		
3	¿conoce usted alguna herramienta de análisis y protección de redes?		
4	¿Sabe usted que hacer en caso de una contaminación de su ordenador de trabajo?		
5	¿ha recibido capacitaciones sobre las amenazas a las que está expuesta una red?		
6	¿tiene conocimiento usted de lo que pueden causar ciertas amenazas de redes a su ordenador?		
7	¿sabe usted cómo proteger su equipo con herramientas de análisis y protección?		
8	¿ha instalado y configurado herramientas de protección de virus en su ordenador?		
9	¿su equipo cuenta con una conexión segura a la red ante cualquier amenaza?		
10	¿alguien le ha dado ha conocer sobre las amenazas y riesgos que existen en las redes?		

0	PREGUNTAS		
	LA SEGURIDAD EN LA RED Y LAS MEDIDAS QUE SE DEBEN TENER EN CUENTA EN SU ORDENADOR	SI	NO
1	¿Sabe usted cuales son los tipos de seguridad que debe contener su ordenador?		
2	¿Su ordenador tiene contraseña de inicio de sesión?		
3	¿sabe usted de que caracteres debe contener su contraseña de inicio?		
4	¿su contraseña está compuesta solo de números?		
5	¿su contraseña está conformada de letras y números?		
6	¿su contraseña está conformada con datos personales?		

7	¿cree usted que su ordenador tiene medidas de seguridad adecuada?		
8	¿Sabe usted si el sistema de su equipo de trabajo está actualizado a la última versión?		
9	¿Sabe usted si su equipo cuenta con un firewall y si este cumple con los parámetros de seguridad?		
10	¿sabe usted de la importancia que es tener un firewall y herramientas que garanticen la protección de los datos en su ordenador?		

0	**PREGUNTAS**		
	NORMA ISO/IEC 27033 Y ESTÁNDAR IEEE 802.10	SI	NO
1	¿Sabe usted si realizan periódicamente análisis en la red con el objetivo de prevenir cualquier perdida o ataque informático?		
2	¿La red de trabajo esta libre para el acceso al público?		
3	¿ha recibido orientación sobre la identificación y análisis de riesgos de seguridad en la red?		
4	¿se he enfrentado con problemas de pérdidas de información o virus de red?		
5	¿usted realiza periódicamente algún tipo de respaldo de información?		
6	¿ha visto la necesidad de instalar un software de análisis y protección de red para evitar ciertas amenazas.?		
7	¿cree usted que tener un software de protección para la red siendo este confiable reduce ciertos riesgos?		
8	¿su equipo tiene restricciones a ciertas páginas Web con el objetivo de prevenir de algún virus malicioso?		
9	¿Cree usted que su equipo es seguro con los métodos de protección que tiene ante ciertas amenazas de red?		
10	¿Cree usted que la red carece de ciertos protocolos de seguridad?		

El presente instrumento de investigación cumple con los parámetros para ser aplicado en la auditoria de seguridad en redes que se realizará a los empleados del Distrito de Salud 13D05 El Carmen.

.....

A.S Jaime Zambrano Quiroz MG.

Tutor

anexo 6 Ficha aplicada en la Auditoria bajo la norma ISO/IEC 27033

Entrevista realizada al administrador de TIC Ing. Klever Chica

Anexo 8 revisión de entrevista
Autor: Carlos Valdez

Anexo 7 resolución de entrevista
Autor: Carlos Valdez

- Instalación de herramientas de análisis y protección de vulnerabilidades en el Distrito 13D05-El Carmen.

Anexo 9 pruebas de Nmap y Nessus
Autor: Carlos Valdez

Anexo 10 instalación de Nessus y Nmap
Autor: Carlos Valdez

- Análisis y pruebas de vulnerabilidades en los ordenadores del Distrito.

Anexo 12 análisis de la red
Autor: Carlos Valdez

Anexo 11 ejecución de herramientas de protección
Autor: Carlos Valdez

Anexo 14 Instalación de herramientas en el dpto. Talento Humano
Autor: Carlos Valdez

Anexo 13 Análisis y protección en Talento Humano
Autor: Carlos Valdez