TECNOLÓGICO NACIONAL DE MÉXICO

Instituto Tecnológico Superior de Teziutlán

Diseño de seguridad perimetral para la infraestructura de red del H. Ayuntamiento de Teteles de Ávila Castillo, Pue.

TESIS QUE PRESENTA:

María Elisa Mariano Ramos

N° de control:

19TE0027P

Como requisito parcial para obtener el título de:

MAESTRO EN SISTEMAS COMPUTACIONALES

Fracción I y II S/N, Aire Libre, Teziutlán, Puebla.
Agosto de 2020

TECNOLÓGICO NACIONAL DE MÉXICO

Instituto Tecnológico Superior de Teziutlán

Diseño de seguridad perimetral para la infraestructura de red del H. Ayuntamiento de Teteles de Ávila Castillo, Pue.

TESIS QUE PRESENTA:

María Elisa Mariano Ramos

N° de control:

19TE0027P

Como requisito parcial para obtener el título de:

MAESTRO EN SISTEMAS COMPUTACIONALES

Fracción I y II S/N, Aire Libre, Teziutlán, Puebla.
Agosto de 2020

La presente tesis que lleva por título Diseño de seguridad perimetral para la infraestructura de red del H. Ayuntamiento de Teteles de Ávila Castillo, Pue. Fue realizada bajo la dirección del consejo que a continuación se indica, que a su vez ha sido aprobada por mismo y verificada como requisito para la obtención del título de:

MAESTRO EN SISTEMAS COMPUTACIONALES.

DIRECTOR:

Dra. Adriana Pérez López _____

1er. CO-DIRECTOR:

M.S.C. Héctor Vicenteño Rivera. _____

2o. CO-DIRECTOR:

M.S.C. María Eugenia Carreón Romero _____

Agradecimientos

Agradezco en especial a mi directora de tesis la Doctora Adriana Pérez López por su continua guía y apoyo brindado antes y durante el desarrollo de la presente tesis, a mis co-asesores por brindar su tiempo para guiarme en el proceso del proyecto, a mis padres y hermanas por confiar en mi a pesar de las circunstancias y dejarme vencer.

Resumen

La seguridad perimetral como herramienta y técnica de protección informática tiene como propósito establecer una línea de defensa que se relaciona con la red interna y toda la prolongación que conforma el entorno en el que se encuentra la tecnología de información de la administración. Este establece medidas de protección que previene ataques externos y que a la vez identifica la actividad natural dentro de la propia red, protegiendo y aislando actividades desconocidas o fraudulentas. (Costas Santos, 2006)

La seguridad de la infraestructura es de vital importancia, ya que busca controlar y dar solución a las diferentes vulnerabilidades que surgen a lo largo de una jornada laboral. La estrategia del gobierno digital tiene como objetivo aprovechar al máximo el uso de las TIC en el funcionamiento de las dependencias y entidades en la Administración Pública, para así agilizar los trámites que realizan los ciudadanos, coadyuvar a transparentar la función pública, de tal manera elevar la calidad de los servicios gubernamentales, y en su caso detectar oportunamente prácticas que afecten a las instituciones públicas.

Se requiere de una serie de pruebas, con el objetivo de localizar y conocer las distintas barreras de seguridad que tiene la red, con la intención de probar su efectividad o, al contrario, demostrar y actuar contra la vulnerabilidad de la infraestructura. Un firewall o Cortafuegos establece secciones de confianza y barreras entre los dispositivos controlados y considerados de confianza. Obteniendo una buena seguridad perimetral mediante la resistencia a ataques externos, la identificación de ataques sufridos y alertar de ellos, aislar y segmentar los distintos servicios y sistemas en función de su exposición a ataques, filtrar y bloquear el tráfico, permitiendo únicamente aquel que sea absolutamente necesario.

La seguridad es primordial, los ataques por red y pérdidas de información ocasionan un gran trastorno y no solo la imagen si no también el funcionamiento y progreso de la administración se ven afectados. Se dice que una plataforma robusta para el control de accesos y protección de los servicios informáticos garantiza un correcto aprovechamiento de la infraestructura y con ello garantiza la integridad y confidencialidad de la información.

Índice general

1.1 Introducción 12

1.2 Planteamiento del problema 13

1.4 Justificación 14

1.5. Hipótesis e identificación de variables 15

1.6. Objetivo general 15

1.6.1 General: 15

1.6.2 Específicos 15

1.7 Alcances 16

1.8 Limitaciones 16

1.9 Estado del Arte 17

2.1. Fundamentos Teóricos 12

2.1. Sistemas de información (general) 12

2.1.1. Seguridad 12

2.1.2. Política de seguridad 16

2.1.3. Medidas de seguridad avanzada 17

2.1.8. SmoothWall 21

2.1.9. IPFire 21

2.1.11. Redes 23

2.1.11.1. Infraestructura de red 23

2.1.12. LAN 25

2.1.13. MAN 25

2.2 Metodología de la Investigación 30

2.3 Metodología de desarrollo 33

3.1 Análisis de datos 42

3.2 selección de pruebas estadísticas 52

3.3. Realización de análisis (Interpretación) 53

3.4. Comprobación de la Hipótesis 55

Diseño y configuración de Smoothwall 57

4.1 Resultados 69

4.2 Conclusión 78

Dedicatoria

Dedico este logro a mis padres por apoyarme, forjarme y guiarme como la persona y profesional que soy en la actualidad; la mayoría de mis logros se los debo a ustedes entre los que incluyo a este nuevo logro. Desde pequeña me han formado con valores, reglas y motivación para seguir adelante.

Gracias por ser parte de este nuevo logro en mi vida profesional.

Índice de Ilustraciones

Ilustración 1 Fortinet 20
Ilustración 2 Región 03 de Puebla 32
Ilustración 3 División de regiones de Puebla 32
Ilustración 4 Organigrama Ayuntamiento de Teteles de Ávila Castillo 34
Ilustración 5 Módem 34
Ilustración 6 Copiadora en red 34
Ilustración 7 Cableado 35
Ilustración 8 Equipos informáticos 35
Ilustración 9 Equipo de cómputo 35
Ilustración 10 Módem 2 35
Ilustración 11 Simbología croquis de infraestructura 37
Ilustración 12 Recursos informáticos piso 1 ayuntamiento 37
Ilustración 13 Recursos informáticos piso 2 ayuntamiento 38
Ilustración 14 Recursos informáticos Unidad del DIF Teteles 38
Ilustración 15 Cuestionario de Diseño de Infraestructura de red (Usuario) 42
Ilustración 16 Gráfica 1: Formación 43
Ilustración 17 Gráfica 2: Identificación 43
Ilustración 18 Gráfica 3: Riesgos 44
Ilustración 19 Gráfica 4: Streaming 45
Ilustración 20 Gráfica 5: Prevención 45
Ilustración 21 Gráfica 6: Calidad de los servicios 46
Ilustración 22 Gráfica 7: Cursos de orientación 46
Ilustración 23 Gráfica 8: Amenazas 47
Ilustración 24 Gráfica 9 Rendimiento 48
Ilustración 25 Gráfica 10: Control 48
Ilustración 26 Gráfica 11: Sistema de seguridad de datos 49
Ilustración 27 Gráfica 12: Instalaciones de red y comunicación 50
Ilustración 28 Gráfica 13: Funcionamiento 50
Ilustración 29 Gráfica 14: Actualización 51
Ilustración 30 Gráfica 15: Medidas de seguridad 52
Ilustración 31 Idioma del teclado 57
Ilustración 32Solicitudes entrantes open 58
Ilustración 33 Tarjeta Green-Red 58
Ilustración 34 Menú configuración de red 58
Ilustración 35 Asignación tarheta Green 58
Ilustración 36 Asignación tarjeta Red 58
Ilustración 37 Interface Green 59
Ilustración 38 Interfaz Red 59
Ilustración 39 Configuración servidor DHCP 59
Ilustración 40 Password admin 60

Ilustración 41 Password root 60
Ilustración 42 Ingreso como usuario root 60
Ilustración 43 Finalización de instalación 60
Ilustración 44Ingreso a Smoothwall 60
Ilustración 45 Home Smoothwall 61
Ilustración 46 Web proxy 61
Ilustración 47 Configuración PuTTY 61
Ilustración 48 Conexión segura PuTTY 62
Ilustración 49Descargar Urlfilter 62
Ilustración 50 Descomprimir Urlfilter 62
Ilustración 51 Instalar Urlfilter 62
Ilustración 52 Advanced proxy 63
Ilustración 53Activación url filter 64
Ilustración 54Filtrado por categorías 64
Ilustración 55 Lista negra 64
Ilustración 56Lista blanca 64
Ilustración 57 Filtrado expresiones regulares 65
Ilustración 58 Contenido de filtrado avanzado 65
Ilustración 59 Actualización automática 65
Ilustración 60 Configuración de ancho de banda 66
Ilustración 61Monitoreo tráfico interno 67
Ilustración 62 Ancho de banda Green 67
Ilustración 63Bloqueo página Teteles 69
Ilustración 64 Bloqueo facebook 69
Ilustración 65Bloqueo twitter 69
Ilustración 66 Bloqueo Megafire 70

Índice de tablas

Tabla 1 Recursos informáticos **¡Error! Marcador no definido.**

CAPÍTULO I

GENERALIDADES DEL PROYECTO

1.1 Introducción

En el presente proyecto se consideran diversos ámbitos de la seguridad perimetral, aquella que va adquiriendo y tomando fuerza con el aumento de volumen de información y que requiere de la máxima seguridad para su resguardo y utilización.

Hoy en día, la utilización de estrategias para realizar de manera eficiente las actividades y tareas que corresponden al área gubernamental, se han vuelto una necesidad y exigencia por parte de la sociedad. La innovación y modernización de las Tecnologías de la Información y la Comunicación (TIC) incitan a la mejora y renovación de los mecanismos gubernamentales que apoya a generar un cambio de panorama, el cual se vea reflejado en la seguridad y paradigma del Gobierno Digital.

A continuación, se propone el diseño de seguridad perimetral para la infraestructura de red del H. Ayuntamiento de Teteles de Ávila Castillo, Pue., que permitirá generar mayor confianza, seguridad y efectividad en los procesos internos y externos. La detección de vulnerabilidades y el monitoreo de los sistemas de información son esenciales para el funcionamiento de la administración y sus usuarios. Es ahí donde surge la necesidad de diseñar una herramienta que genere la protección informática; con el fin de establecer una línea de defensa conformada por la red interna y todo el entorno que conforma la administración. (Costas Santos, 2006)

A lo largo del proceso de desarrollo del diseño del sistema de seguridad en el ayuntamiento, se logran conocer claramente las necesidades que surgen dentro de la organización, es estado actual de los recursos informáticos y la infraestructura de red de datos. A su vez se reflejan los resultados de cuestionarios realizados hacia los usuarios de dicha organización gubernamental, en donde los mismos dan a conocer sus puntos de vista, las necesidades de contar con mejores recursos informáticos y las ventajas de aplicar un mecanismo de seguridad en la infraestructura de red de datos.

1.2 Planteamiento del problema

El tema de la seguridad informática como una disciplina del conocimiento busca cerrar la brecha de los distintos eventos inesperados como contraseñas débiles, software infectado de virus, falta de cifrado de datos, Bugs, etc., los cuales pueden perjudicar a los activos de una organización, por ello es necesario contar con estrategias para avanzar ante cualquier eventualidad como la divulgación de datos confidenciales, propagación de virus, intrusión de piratas informáticos, el robo de información, entre otros. Se requiere de diseños, procesos y procedimientos que salvaguarden la información y datos confidenciales. Estos procesos se estructuran con el uso de estándares, normas, protocolos y metodologías para mitigar y minimizar los riesgos asociados a la infraestructura tecnológica.

Este proyecto está dirigido hacia el H. Ayuntamiento de Teteles de Ávila Castillo, Puebla, donde se busca diseñar un mecanismo de seguridad perimetral en su infraestructura de red, ya que no cuenta con todos los servicios protegidos y modernización. Es por ello que el municipio requiere de un cuarto de telecomunicaciones, donde se almacene y genere la seguridad de la información, que a su vez otorgue una mejor calidad en los servicios hacia la ciudadanía y exista un control en el manejo de los recursos informáticos por parte de los usuarios internos y externos. Un sistema robusto que protege datos sensibles, históricos que son parte de la ciudadanía y administraciones anteriores.

Actualmente no cuenta con técnicas o protocolos de seguridad en su infraestructura, es por ello que se busca dar inicio a la implementación de técnicas y procesos que generen un panorama positivo y vanguardista. Para llevar los riesgos de seguridad informática a su mínima expresión, es necesario un mecanismo especializado, que transforme la seguridad en un proceso continuo y dinámico.

La detección de vulnerabilidades y el monitoreo de los sistemas de información son imprescindibles para el funcionamiento de la organización y sus usuarios. De aquí parte la necesidad de diseñar un mecanismo de seguridad perimetral en la infraestructura de red, que monitoree, recolecta, notifique y analice el tráfico de la red y sistemas.

1.4 Justificación

La protección de datos y la infraestructura informática o de red son elementos que merecen mayor prioridad e importancia en el caso de las administraciones gubernamentales, que forman parte de enormes masas de información y comunicación.

El presente proyecto hace referencia a la importancia de la seguridad informática que debe tomarse en cuenta en las instituciones de gobierno, conocer las distintas amenazas y vulnerabilidades a la que está expuesta. El H. Ayuntamiento de Teteles de Ávila Castillo requiere lograr una eficiente administración de sus activos físicos y lógicos que a su vez deben ser rápidos, seguros y eficientes, que ayude a obtener un sistema de seguridad, que fortalezca al máximo la seguridad de su infraestructura y disminuir los riesgos posibles a los que se enfrenta día con día.

Contribuyendo en gran parte a la protección de los sistemas, información almacenada, procesos y servicios que conforman la infraestructura de red, mediante el seguimiento de procedimientos que aseguren un control de acceso, roles, limitación de diversos servicios como el streaming o redes sociales, donde la mayoría de las veces se generan tiempos muertos, ya que en ocasiones los usuarios no disponen su tiempo al 100% en sus actividades y responsabilidades diarias.

El mecanismo de seguridad, permitirá ser una solución a corto plazo para el H. Ayuntamiento de Teteles de Ávila Castillo y a mediano o largo plazo para otros ayuntamientos que carezcan de una adecuada infraestructura, con la salvedad de adaptar dicho sistema a la infraestructura tecnológica que requiera cada administración, logrando ser implementado de manera más rápida y segura.

De tal manera aportar calidad en los diversos servicios que se otorgan a la ciudadanía, obteniendo un control en el uso de los recursos o sistemas informáticos, ejerciendo políticas de seguridad, filtrando los accesos a la red y a su vez bloquear el acceso a personas ajenas o no autorizadas. Generar mayor coordinación entre los diferentes departamentos y, por lo tanto, proteger de la información dentro de la administración. Es necesario poner en práctica mejores técnicas de seguridad, diseñando la infraestructura bajo estándares y

protocolos que mejor se adecuen a la institución. El impacto que ejerce en las tecnologías de la información es ampliamente fuerte y que en la actualidad tiene mayor peso en el desarrollo de las organizaciones gubernamentales, la comunicación y los nuevos modelos de administración, que buscan fortalecer al crecimiento y desarrollo de los servicios que se ofrecen a la ciudadanía en general. Acercando el gobierno con la ciudadanía mediante los servicios públicos, alcanzando calidad y eficiencia en los servicios.

1.5. Hipótesis e identificación de variables

El diseño de un mecanismo de seguridad perimetral, contribuirá positivamente en la administración de los sistemas de información en el H. Ayuntamiento de Teteles de Ávila Castillo, Pue

1.6. Objetivo general

1.6.1 General:

Diseñar un mecanismo de seguridad perimetral en la infraestructura de red del H. Ayuntamiento de Teteles de Ávila Castillo, Puebla, con base en metodologías de seguridad open source, con la finalidad de contribuir positivamente en la administración de los sistemas de información.

1.6.2 Específicos

- ✔ Desarrollar un proceso de recolección de información en cuanto el ambiente físico y virtual en la actual administración.

- ✔ Registrar el respectivo levantamiento de servicios informáticos, aplicaciones, redes y sistemas de información.
- ✔ Diseñar el esquema de seguridad perimetral
- ✔ Establecer políticas de seguridad capaces de estandarizar procesos transversales, la seguridad en acceso y permisos

1.7 Alcances

- Establecer diversas políticas de bloqueo que limiten el servicio de streaming y entretenimiento.
- Asegurar mayor rendimiento en el servicio de red e internet.
- La obtención de mayor eficiencia en la consulta y manipulación de información.
- Llevar a cabo un control de acceso que defina los permisos que posee el usuario dentro del sistema.
- Controlar la descarga masiva de aplicaciones o archivos ajenos a la institución, evitando la portación de virus o la vulneración del sistema.

1.8 Limitaciones

- El esquema de seguridad no garantizará el aumento de la frecuencia o ancho de banda de la conexión de internet.
- Una de las posibles limitantes podría ser la falta de personal capacitado para el manejo y administración del esquema de seguridad.

1.9 Estado del Arte

La revisión del estado del arte acerca de algunos proyectos similares al que cubre este proyecto, en torno a la implementación de seguridad en la infraestructura de red, arrojó información muy relevante y que sirvió de apoyo para la realización y obtención de resultados del trabajo realizado. Los trabajos más destacados se detallan a continuación:

Implementación del control de acceso a la red mediante los protocolos de autenticación, autorización y auditoría. Se trata del diseño e implementación de un sistema de control de acceso a la red que proporciona el servicio de Autenticación, Autorización y Auditoría (AAA) mediante el uso de software libre, en conjunto con protocolos estándar IEEE 802.1x y RADIUS, con base en una infraestructura de clave pública, donde se genera un servicio de directorio centralizado que almacena las políticas de seguridad para los usuarios y una base de datos MySQL en donde se registran cada uno de los eventos de dicho servicio (AAA).

El servidor FreeRADIUS y cada una de las herramientas que permiten implementar una red con el servicio de (AAA) se configuraron en un computador de escritorio de una agencia de publicidad, y que está dividida en distintos puntos (Cali, Bogotá y Medellín), en un entorno de 300 estaciones de trabajo. El equipo se interconecta a los puntos por una red WAN. Configurando el servidor RADIUS en una máquina virtual con sistema operativo Ubuntu versión 10.4. De tal manera se llevaron a cabo los siguientes pasos para que se lograra habilitar este servicio, la Autenticación, la configuración para usar certificados digitales de identificación personal (EAP-TLS) implementando una Autoridad de Certificación mediante la herramienta libreOpenSSL, la configuración para usar nombre de usuario y contraseña con EAP Protegido (PEAP), la configuración para usar nombre de usuario y contraseña empleando EAP dentro de un Túnel Seguro en la Capa de Transporte (EAP-TTLS), Configuración del punto de ejecución de políticas, Punto de ejecución de políticas de tipo inalámbrico, Punto de ejecución de políticas de tipo cableado, Autorización y Auditoría.

Dichos elementos para proveer la red con un sistema AAA se instalaron en una misma máquina, dando la posibilidad de que sea escalable, de tal manera se definieron las siguientes políticas: Asignación de VLAN de acuerdo al perfil del usuario, Restricción del acceso a la red para los visitantes después del horario laboral, Registro en la base de datos

mySQL de los ingresos exitosos y fallidos a la red, Registros en la Base de Datos información relevante de los usuarios autenticados exitosamente. Con todos los sistemas se demostró que era posible hacer uso de los tres esquemas de autenticación disponibles, realizando autenticación mutua entre las partes del proceso AAA, consiguiendo una conexión exitosa, segura y sin inconvenientes. (Arana R, Villa, & Polanco, 2013)

Otra caso de estudio es el llevado a cabo en el Ministerio del Poder Popular para la educación, en Venezuela, donde se diseñó un **sistema de Seguridad para redes de datos**, ésto debido a la carencia de una seguridad de la información que establezca las políticas, normas, procedimientos y la estructura organizacional adecuada; de modo que se busca implementar métodos y mejores prácticas en tecnologías de la información y telecomunicaciones; logrando minimizar y erradicar varios de los problemas de seguridad originados por las amenazas y vulnerabilidades a las redes de datos de esa institución.

Este proyecto hizo uso de tres estándares en materia de seguridad de la información: CobiT, ITIL e ISO/IEC 27002, aunque solo se lograría llegar a una aproximación en el alcance del estudio. Para el diseño del sistema de seguridad se mencionaron los siguientes elementos que lo conforman: Preventivo, Correctivo, De contingencia y recuperación, Gestión del desempeño y la capacidad, Continuidad del servicio. Esta propuesta de seguridad abarca tres aspectos relativos: La prevención de incidentes, la corrección de posibles fallos y la contingencia, a su vez la recuperación en caso de afectación por incidentes de seguridad.

Se menciona que el estudio efectuado en las condiciones y los sistemas de información en general de la institución, da un resultado insuficiente, así que es necesaria la implementación de normas y estándares de seguridad que logren mejorar la situación actual de la institución.

Esta propuesta tiene por finalidad beneficiar los sistemas de información, asegurando los datos existentes, repercutiendo directamente en la mejora de los servicios prestados a los usuarios del sistema. Tomando en cuenta las características que son de tipo: preventivo, correctivo, de contingencia y recuperación, gestión del desempeño y la capacidad, así como la continuidad del servicio. (Jaspe Díaz, 2011)

Otro estudio con gran similitud; a los dos ya citados es el que lleva por nombre **"Desing and Implementation of Firewall Policy Advisor Tools"**. Los firewalls son elementos en la seguridad de la red que administran reglas del firewall, estos se han vuelto muy complejos y propensos a errores. De ahí que el estudio hace referencia a las reglas de filtrado del firewall que deben ser estrictas y organizadas cuidadosamente para lograr implementar correctamente las políticas de seguridad. Se dan a conocer un conjunto de técnicas y algoritmos que proporcionan una detección automática de anomalías para descubrir conflictos de reglas y problemas potenciales en los firewalls. Además de la edición o creación de políticas sin anomalías para la inserción, modificación y eliminación de reglas. De igual manera la traducción concisa de reglas de filtrado a una descripción textual de alto nivel para la visualización y verificación del usuario. De modo que se implementó una herramienta llamada "Asesor de políticas de Firewall". Que simplifica la administración de cualquier política de cortafuegos genéricos estrictamente como reglas de filtrado, al mismo tiempo minimiza la vulnerabilidad de la red debido a una configuración incorrecta de las reglas que contengan los cortafuegos. Se modelan las políticas de firewall, esto como requisito básico para cualquier solución de administración, donde se modelan las relaciones y la representación de estas.

Al tratarse de un modelo completo que incluye lo antes mencionado, este es más eficiente, fácil de implementar y de usar. Se dice que el modelado de relaciones de las reglas es necesario para analizar la política de firewall y el diseño de técnicas dirigidas a la administración; del mismo modo que la detección de conflictos y su edición. Se representaron mediante un único árbol con raíz al que denominaron árbol de políticas. Este proporciona una representación simple y comprensible de las reglas de filtrado y, al mismo tiempo, permite descubrir fácilmente las relaciones y anomalías. Cada nodo de un árbol de políticas representa un campo de regla y cada rama de este nodo representa un valor posible del campo asociado. La seguridad del firewall requiere una adecuada gestión para proporcionar un servicio de seguridad. En pocas palabras un firewall no necesariamente hace que la red sea segura, su complejidad de administrar las reglas y el potencial de la vulnerabilidad de la red se debe al conflicto de reglas.

El "Firewall Policy Advisor" proporciona una serie de herramientas fáciles de usar para proteger la política de firewall ante las anomalías. El administrador puede hacer uso del

asesor de políticas sin un análisis previo de reglas de filtrado. Se define todas las posibles relaciones de reglas se usan para clasificar las anomalías. Basado en este modelo y formalización, el asesor de políticas implementa diversas herramientas en la administración. (Al-Shaer & Hamed, 2014)

Diseño de un sistema de seguridad perimetral en las instalaciones del consorcio expansión PTAR Salitre, Sede Bogotá D.C. Es otro de los proyectos con perfil similar al que se elabora. Este tiene el objetivo de realizar un aseguramiento de las redes de datos, a su vez la periferia de la edificación, planteado un sistema de seguridad por anillos, y que este sería implementado de manera paulatina, con base a la normatividad aplicable en cada una de ellas, abordando la configuración de redes, la implantación de mecanismos de seguridad como firewalls, IDS, distribución de redes mediante VLANS de comunicación, entornos de acceso físico por biometría y vigilancia de la infraestructura y un compendio ambiental por medio de circuitos cerrados de televisión CCTV.

Los resultados esperados con este diseño es el aseguramiento de la información para brindar el aseguramiento de su información, garantizando el desarrollo de las actividades y al efectuarse por anillos de seguridad; la gerencia estará en la disposición de realizar la implementación abarcada por fases, donde nace la necesidad de realizar planes de trabajo para ampliar las políticas de seguridad, un control en el acceso lógico y físico, con el fin de generar concientización del personal en el correcto uso del manejo de la información y mantener libre de riesgos de filtración de información en los puestos de trabajo y una constante búsqueda de riesgos para su eliminación. Con la implementación del sistema se generará el aseguramiento de la capa de red, tomando en cuenta el modelo OSI, buscando ampliar el aseguramiento de la información y brindar el primer bloque de seguridad. (Bohorquez & Paez Cuadros, 2017)**.**

El último proyecto de referencia lleva por nombre **“Propuesta para la implementación de un Firewall en el departamento de Administración de Servidores, DGSCA”.** A continuación, se aborda la importancia de la implementación de un mecanismo de seguridad, con apoyo de herramientas que trabajen en conjunto para proteger la red de cualquier organización. Se dice que un firewall es un componente o conjunto de componentes que restringen el acceso entre una red protegida e internet, o entre otros

conjuntos de redes. A lo largo del proyecto se realizan varias preguntas que ayudan a tomar decisiones para tomar el camino correcto, una de ellas es: ¿Comprar o diseñar el Firewall? Se realiza una comparación de un firewall y sus componentes para un buen funcionamiento. Esto ayuda a la decisión de qué elementos se requieren y si es necesario comprar en su totalidad un Firewall.

Se habla de los requerimientos que se necesitan para llevar a cabo la instalación y configuración del firewall seleccionado, estos son: una máquina a utilizar (que abarca software y hardware), elección del software, el sistema operativo, rapidez, elección del hardware, ubicación del firewall, etc. Que generarán el servicio de proporcionar seguridad y administración de redes en el DGSCA de la UNAM. Las políticas de seguridad son importantes en la realización de reglas de filtrado en este servicio y que guardan una estrecha relación en especial que tienen que ver con el control de acceso a los sistemas. Si se desea un nivel de seguridad alto se debe de dar valor a la información de la organización, implementando un firewall en conjunto con herramientas de seguridad correctamente configuradas, siendo una alternativa para obtener protección y seguridad, en definitivo, antes de elegir un firewall es necesariamente realizar un análisis que permita valorar las necesidades, beneficios y requerimientos que vayan acorde con lo requerido, que sea una inversión y no un gasto. (Hernández Valverde, 2004)

CAPÍTULO II

METODOLOGÍA Y DESARROLLO

2.1. Fundamentos Teóricos

2.1. Sistemas de información (general)

Con el propósito de adentrarse en el fundamento teórico, a continuación, se darán a conocer algunos de los elementos que forman parte en el trayecto del proyecto. Para comenzar se describe de manera general la definición de los sistemas de información como primer punto clave, incluso de ahí parten los demás temas que se darán a conocer más adelante. Se dice que un sistema de información (por sus siglas en inglés: information system) es un conjunto de componentes que se relacionan entre sí donde recaban, procesan, almacenan y distribuyen datos e información y de tal manera proporcionan un mecanismo de retroalimentación para lograr un objetivo.

Dicho mecanismo ayuda a las organizaciones a lograr con éxito sus objetivos, busca generar el incremento de ganancias o mejorar el servicio al cliente. Se recomienda a las empresas el uso de los sistemas de información con el fin de acrecentar sus ganancias y la reducción de costos. Actualmente han incrementado las instituciones gubernamentales que han optado por la adquisición de sistemas de información, quienes buscan otorgar un mejor servicio a la ciudadanía, mayor eficiencia en el desempeño de las actividades diarias, la privacidad de su información, entre otras. Los elementos de (SI) son los recursos, equipo humano, la información y las actividades que son llevadas a cabo en las organizaciones.

Los Sistemas de Información, son un tema extenso de conocer y hablar, pero de manera general se puede decir que se utilizan en casi todas las profesiones, empresas, instituciones de gobierno, educativas, de salud, etc. que otorgan beneficios, entre los cuales destacan la velocidad, la precisión y la reducción de costos. (M. Stair & W. Reynolds, 2010)

2.1.1. Seguridad

Con respecto al tema de seguridad en el área informática se ha convertido en un tema de interés, ya que es indispensable conocer la importancia que conlleva en la actualidad. La definición de seguridad informática se dirige a el impedimento en la ejecución de

operaciones no autorizadas sobre un sistema o red informática cuyos efectos puedan conllevar daños sobre la información, equipo o software. En pocas palabras se define como la protección de información y sistemas de información de acceso no autorizado. Esto se vincula con tres elementos básicos: la primera es la información que, como activo intangible, representa quizá uno de los elementos más sensibles y vulnerables; el software, cuya pérdida o modificación puede representar daños económicos u operativos no solo hacia el usuario sino a toda una organización; por último, el hardware, que al fallar provoca retrasos en la operación diaria y la consecuente pérdida de tiempo y costos elevados.

Entre otras definiciones se dice que la seguridad informática es una disciplina que se ocupa en diseñar normas, procedimientos, métodos y técnicas destinados a formar un sistema de información seguro y confiable. (Aguilera López, 2010) Existe un sinfín de medidas preventivas que permiten proteger cada uno de los elementos antes mencionados, como controles de acceso de hardware y software, respaldos de información, actualizaciones, entre otros, más adelante se mencionan algunos temas referentes.

Riesgos en seguridad de las TIC

Actualmente existen múltiples riesgos dirigidos a equipos, sistemas de información y comunicaciones, quienes no cuentan con controles de protección que aseguren su información. Dichas amenazas son de manera global, tema que preocupa a organizaciones, instituciones públicas y privadas. Diariamente se desarrollan nuevos métodos que afectan a la seguridad de la información de las organizaciones, a lo antes expuesto se suman vulnerabilidades internas que son un factor de riesgo no menor, donde existe repercusiones en la confiabilidad por parte de usuarios, clientes y socios de negocios.

Se deben de tomar en cuenta los riesgos asociados con el diseño, desarrollo e implementación que surgen en los sistemas, los cuales pueden ser problemas potenciales, sino se tienen las medidas adecuadas para salvaguardar los datos y la información, estos riesgos se pueden presentar por vulnerabilidades y amenazas en cualquier momento y se clasifican de la siguiente manera: Riesgos de integridad, Riesgos de relación, Riesgos de acceso, Riesgos de utilidad y Riesgos de infraestructura. (Burgos Salazar & G. Campos, 2009)

Vulnerabilidad, amenazas y ataques

Estos conceptos se relacionan entre sí, haciendo parte de la concepción de la seguridad en diversos ámbitos, dado que son aplicados en referencia a la seguridad informática y de la información. Se dice que las vulnerabilidades son una debilidad en la tecnología o en los procesos relacionados con la información, se consideran características propias de los sistemas de información o de la infraestructura que la contiene. Las amenazas son los posibles ataques que manipula una persona que aprovecha las vulnerabilidades que se van presentando y que afectan directamente a la información o los sistemas que la procesan.

Los ataques se producen a raíz de alguna vulnerabilidad o debilidad en el software o hardware que son detectados por delincuentes, para obtener beneficios, que, por lo general, es de índole económico. De esta manera causan un efecto negativo en la seguridad de los sistemas comprometidos, desviándose luego a los activos de la organización. Dependiendo del ataque o en su caso algún virus informático que afecte, se pueden provocar diversos daños. (Tarazona T.)

Clasificación de los ataques de red

Existe un sinfín de tipos de ataques que recibe una red o en ocasiones el software en internet, enseguida se mencionan algunos de los ataques que amenazan constantemente a una infraestructura.

Ataque de reconocimiento, es el descubrimiento y el mapeo de sistemas, servicios o vulnerabilidades. El ataque de acceso, aquel donde existe la manipulación no autorizada de datos, acceso al sistema o privilegios del usuario. Ataques a contraseñas, consiste en ingresar al sistema de la víctima, a través de la red, con credenciales y haciendo uso de conexión remota. El siguiente es el ataque de suplantación de identidad (Spoofing), que consiste en aplicar técnicas como su nombre lo dice de suplantación con usos maliciosos o de investigación. Por último, la denegación de servicio, donde ocurre la desactivación o corrupción de redes, sistemas o servicios. Otros más son los virus o códigos informáticos, el uso no autorizado de Sistemas informáticos, el robo de información, fraudes, alteración de la información, su divulgación, desastres naturales, el sabotaje, vandalismo y espionaje. Más adelante se

explicarán algunos de los ya mencionados, más a fondo para conocer la manera en cómo funcionan.

Ataques internos, externos, pasivos y activos

Para comenzar a describir cómo se conforman los distintos ataques antes ya mencionados, se comenzará por el ataque de reconocimiento, es aquel donde los actores de amenazas externas pueden hacer uso de herramientas de Internet, por ejemplo, utilidades *nslookup* y *who1s*, para determinar rápidamente el espacio de direcciones IP asignando a una determinada entidad. Una vez realizado esto, el actor de amenazas puede hacer ping a las direcciones IP disponibles públicamente para identificar las que están activas, sistemáticamente a todas las direcciones de red en un rango o subred dado. El actor busca información inicial sobre un objetivo, que puede usar distintas herramientas, como la búsqueda de Google, sitios web de organizaciones, whois y más.

Los ataques de acceso explotan las vulnerabilidades conocidas en los servicios de autenticación, servidores FTP y servicios web para así obtener acceso a cuentas web, base de datos confidenciales e información confidencial. Esto permite a las personas obtener acceso no autorizado a información privada, el ataque de acceso se clasifica en cuatro tipos: ataques de contraseña, explotación de confianza, redirección de puertos y hombre en el medio (*man-in-the-meddle*). El ataque a contraseñas, con el uso de distintas herramientas o maneras de ingresar a un sistema, se genera un diccionario (hash) de todas las posibles combinaciones y se compara con el patrón (hash) que permite el acceso.

Se divide en dos formas de operación: la primera es el ataque de diccionario y el otro es el ataque por fuerza bruta, que se basa en la formación de palabras mediante combinación de caracteres hasta encontrar una que coincida con la contraseña a desbloquear. (Cirilo Cruz, Zúñiga López, Avilés Cruz, & Villegas Cortez, 2018)

Denegación de servicio

El ataque de denegación de servicio (DoS), colapsa absolutamente un servidor y genera procesos muy lentos en la navegación a través de él. Ya que no solo puede atacar a servidores web, sino también a servidores de correo electrónico, servidores DNS, etc. Consta de tres categorías: la Inundación de conexiones, donde normalmente el protocolo que usa es TCP, al ser conectivo, fiable y orientado a conexión. Se dice que el atacante establece cientos de conexiones en el servidor hasta colapsar y haciendo que no se aceptan conexiones de usuarios legítimos. El siguiente es la Inundación de ancho de banda, el usuario malintencionado envía demasiados paquetes al servidor, hasta que impide que los paquetes legítimos puedan llegar a él, es donde el ancho de banda no llega a ser suficiente para más paquetes.

Por último, el ataque de vulnerabilidad, si en el servidor hay alguna vulnerabilidad, el atacante se enfoca en explotarla con él envió de mensajes construidos específicamente para provocar el fallo de las máquinas. (Zapata Molina, 2012)

Suplantación de servicio

El siguiente es el ataque de suplantación de identidad, Spoofing aplica técnicas de suplantación con usos maliciosos o de investigación, su objetivo es por medio de este ataque alcanzar la confianza de su víctima haciéndose pasar por otra máquina.

2.1.2. Política de seguridad

Siendo un conjunto de directrices, normas, procedimientos instrucciones que guía las instrucciones de trabajo y definen los criterios de seguridad para que sean adoptados a nivel local o institucional, tienen el objetivo de establecer, estandarizar y normalizar la seguridad tanto en el ámbito humano como tecnológico. Tratan los aspectos y elementos esenciales, donde se debe aplicar seguridad y tener bajo control. Cada política contiene una lista de check list de cada una de las acciones más importantes dentro de una organización. (Dussan Clavijo, 2006). Los autores de la siguiente

definición de política de seguridad abordan el tema de seguridad informática como un problema de personas, mientras que algunos comentan que es un problema de tecnología, y podría decirse que las dos opiniones tienen cierta realidad.

Las políticas representan aquello que la gerencia puede utilizar para demostrar la importancia de la Seguridad Informática, y qué obligaciones tienen los trabajadores para prestar atención ante esta situación. En general las políticas son instrucciones gerenciales que trazan una dirección predeterminada o describen la manera de manejar un problema o situación. De igual manera se pueden considerar como reglas de negocio, aunque los documentos de políticas de seguridad informática varíen de una organización a otra, un típico documento de este tipo incluye una exposición de motivos, la descripción de las personas a quienes van dirigidas las políticas, el historial de modificaciones efectuadas, estas definiciones de términos especiales y las instrucciones gerenciales específicas sobre el tratamiento de las políticas. (Corrales Hermoso, Beltrán Pardo, & Guzmán Sacristán, Diseño e implantación de arquitecturas informáticas seguras. Una aproximación Práctica, 2006)

2.1.3. Medidas de seguridad avanzada

Existe la posibilidad de adoptar medidas que apoyen a forjar una garantía de seguridad. Para implementarlas es necesario conocer su funcionamiento y cómo logran otorgar protección dependiendo de las necesidades de una organización.

2.1.3.1. Cortafuegos o firewall

Se define como un filtro que controla cada una de las comunicaciones que atraviesan una red y en función de su naturaleza permite o deniega su paso. Para permitir o denegar una comunicación, el firewall examina el tipo de servicio al que corresponde, estos pueden ser HTTP, SMTP o FTP, analiza así mismo el tráfico entrante o saliente. En el momento de instalar un firewall, se configura con una serie de pasos y reglas que deben cumplir todo el tráfico que pasa a través de él. Un ejemplo de ello, es cuando se instala un firewall en una empresa y se establece una

regla que bloquee el protocolo FTP de salida, los usuarios de esa red no podrán establecer sesiones FTP con el exterior.

Un perfil de firewall se dice que es una forma de agrupar configuraciones, como reglas de firewall y seguridad de conexión, aplicadas al equipo dependiendo del lugar en el que esté conectado. Se dice que hay tres posibles perfiles; Dominio, Privado y Público. (Raya Cabrera, 2014). Jean Paul define a Firewall como un sistema de defensa que forma parte de una red de trabajo y está diseñado para denegar o permitir el acceso a ella en base a reglas configurables y otros criterios predefinidos. Las funcionalidades que lo conforman destacan: el bloque de paquetes que se originan desde un determinado rango de IP, puertos dominios, direcciones de correo, etc. también los paquetes generados por determinados protocolos o aplicaciones no autorizados, una más son los paquetes que son reconocidos por el firewall como ataques informáticos.

En algunos casos, genera informes que son útiles como una herramienta de análisis del comportamiento de red interna y externa, la generación de registros que puedan ser utilizados en un análisis forense. La integración de sistemas de defensa en contra de virus, spam, y malware en general, la segmentación segura entre distintas redes internas además de Internet. La clasificación de firewalls son parte de diferentes características o modos de empleo como el Modelo de arquitectura, Instaladores de software vs appliance, firewalls de host vs. Firewalls de red que dependen de diversos filtros. (García Moran, Fernández Hansen, Martínez Sánchez, Ochoa Martín, & Ramos Varón, 2011)

2.1.4. Palo Alto Networks

Palo Alto Networks, conocido a nivel mundial y reconocido en el cuadrante de Gartner como líder mundial en ciberseguridad, ofrece continuamente innovación para permitir una transformación digital segura, esta plataforma está diseñada para prevenir las brechas y para facilitar al administrador información útil sobre las amenazas detectadas en todas las funciones de seguridad de un sistema. Tiene la capacidad de analizar malware sobre cualquier puerto, aplicación o protocolo mediante su tecnología avanzada. Su principal objetivo es habilitar de manera

segura el uso de aplicaciones para todos los usuarios en la red y mejorar el desempeño y velocidad de análisis de tráfico generado por los usuarios, brindando protección ante amenazas desconocidas.

Algunas de las características de esta plataforma de seguridad se mencionan a continuación: Posee un potente motor para la detección de aplicaciones de manera nativa, analiza Malware sobre cualquier puerto, aplicación o protocolo. Del mismo modo analiza todo el tráfico por cada uno de sus módulos de seguridad en un solo paso, de manera que mejora el desempeño y velocidad de análisis. Brinda protección para aplicaciones SaaS en la nube como Office 365, Salesforce, etc., la certeza de que todos los equipos están seguros, sin importar que se encuentren en un entorno vulnerable. Estas características están diseñadas para trabajar en conjunto y funcionar consistentemente para todo tipo de usuarios, aplicaciones y ubicaciones. (Networks, 2020)

2.1.5. Fortinet

La siguiente plataforma de ciberseguridad es una de las más conocidas en el país, ya que genera mayor rendimiento en las industrias, ofrece una protección amplia, integrada y automatizada en cualquier lugar donde se necesite. Fortinet Security Fabric es una plataforma integrada, que fue impulsada por FortiOs para generar una seguridad y rendimiento consistentes en todos los puntos de la red, actualmente este sistema operativo de seguridad aporta más de 300 funciones y actualizaciones.

Las empresas, gobiernos y proveedores de servicios adoptan las soluciones que ofrece este sistema para impulsar la innovación digital y obtener resultados positivos. Sus principios se basan en forma amplia mediante la reducción del riesgo, la administración de toda la superficie de ataque digital, es de forma Integrada que genera el cierre de brechas de seguridad y reduce la complejidad, Automatizada de manera que reduce el tiempo de prevención y operaciones eficientes. Sus funciones de consolidación y aceleración se han mejorado en el nuevo FortiGate 7121F, este software no es libre, por tal motivo se ofrecen opciones de pago a medida al rendimiento de protección que requiera la organización, entre más alta sea la protección, más altas serán las opciones de pago. (Fortinet, 2021)

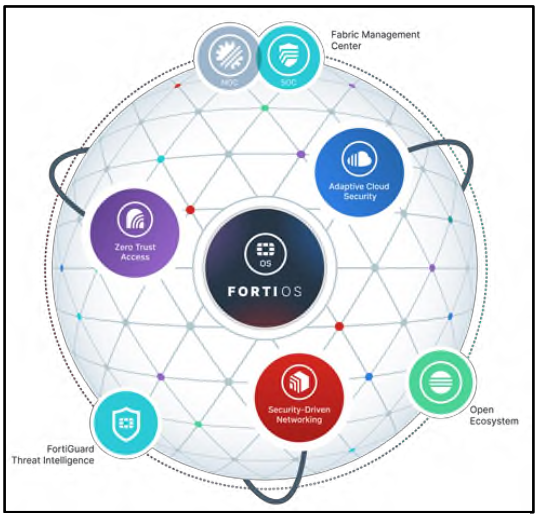


Ilustración 1 Fortinet

2.1.6. Cisco

La cartera de Cisco es extensa, uno de sus productos es la seguridad es Cisco Secure Firewall que ofrece una mayor protección para la red quien no está a salvo de amenazas. La plataforma de Cisco, está generando una base para una seguridad ágil e integrada, lo que la lleva a ser uno de los mejores sistemas de seguridad hoy en día. Permitiendo una gestión más ágil y con un enfoque integrado para armonizar políticas y cumplimiento en redes cada vez más heterogéneas. Secure Firewall brinda un conjunto de integraciones entre núcleos de las funciones de red y seguridad, ofreciendo una arquitectura más segura.

Algunas de sus principales características son las siguientes: Una integración de carga de trabajo seguro que permite una visibilidad completa y la aplicación de políticas para aplicaciones modernas distribuidas y dinámicas en la red. Inteligencia de amenazas avanzada al defender la infraestructura de la organización de amenazas maliciosas y desconocidas. Análisis y registro de seguridad de Cisco donde se genera un análisis de comportamiento de amenazas en tiempo real para su detección, permitiendo tiempos de respuesta mucho más rápidos. Contiene un sistema de prevención de intrusiones de próxima generación y una respuesta de amenazas de SecureX. Ayudando a las organizaciones a cumplir con cada uno de los requisitos reglamentarios. (Firewall, 2020)

2.1.7. PfSense

El software pfSense es una distribución personalizada de código abierto y gratuito de FreeBSD, que está diseñada específicamente para ser usado como firewall y enrutador, el cual administra por completo a través de la interfaz web. Siendo una plataforma de enrutamiento y firewall potente y flexible, agrega una extensa lista de características relacionadas y un sistema de paquetes que permite una mayor capacidad de expansión sin agregar posibles vulnerabilidades de seguridad a la distribución base. PfSense es de código abierto y se distribuye bajo la licencia Apache 2.0., es un firewall gratuito. (pfSense, 2020)

2.1.8. SmoothWall

SmoothWall es un firewall gratuito que incluye su propio sistema operativo GNU/Linux de seguridad reforzada y una interfaz reforzada y una interfaz web fácil de usar. Es lo suficientemente fácil de instalar que hasta lo pueden hacer los usuarios sin tener un breve conocimiento de Linux. Se dice que su software admite una amplia variedad de tarjetas de red, módems y otro tipo de hardware. Trabaja con distintos métodos de conexión e ISP diferentes de todas partes del mundo. Se administra y configura el software mediante un navegador web. Esta plataforma produce soluciones de seguridad con soporte comercial diseñadas para escuelas, redes empresariales, pequeñas y medianas empresas.

El producto incluye la gama de guardián de filtros de contenido web, firewalls avanzados y otras aplicaciones de seguridad de Internet, correo electrónico y VPN. Una solución gratuita de cortafuegos de código abierto. (Express, 2020)

2.1.9. IPFire

De igual forma es un cortafuego de código abierto, IPFire es una solución de firewall potente y profesional, el objetivo principal es la seguridad. Se dice que es fácil de configurar y su sistema de detección de intrusos evitan que los atacantes logren ingresar a la red. En su configuración, la red se divide en varias zonas con diferentes políticas de seguridad como LAN y DMZ para la administración de

riesgos dentro de la red y obtener una configuración personalizada para cada una de las necesidades de cada segmento de red. Un tema importante es su constante actualización que mantiene a IPFire fuerte contra las vulnerabilidades de seguridad y los nuevos vectores de ataque.

Emplea un cortafuego Stateful Packet Inspection (SPI), que se basa en Netfilter, un marco de filtrado de paquetes de Linux. Quien filtra paquetes rápidamente y logra alcanzar rendimientos de hasta varias decenas de Gigabit por segundo. Contiene una interfaz de usuario web intuitiva que permite crear grupos de hosts y redes que se utilizan para mantener un gran conjunto de reglas breves y ordenadas, un punto importante es su entorno complejo con un estricto control de acceso, los informes gráficos y de registro brindan una buena comprensión. Este sistema de detección de intrusiones (IDS) analiza el tráfico de la red e intenta detectar vulnerabilidades, fugas de datos y otras actividades sospechosas. Cuando sucede la detección, se generan alertas y el atacante logra ser bloqueado inmediatamente. (Source, 2021)

2.1.10. Proxy

Un servidor proxy o representante es una aplicación o sistema que gestiona las conexiones de red, se dice que sirve de intermediario entre las peticiones de servicios que solicitan los clientes, como http, FTP, telnet, ssh, entre otros., de manera que crea una memoria caché de estas peticiones y respuestas por parte de servidores externos, su finalidad es poder servir rápidamente a los usuarios en conexiones siguientes que hayan sido solicitados y respondidos previamente, sin la necesidad de acceder remotamente de a servidores externos. En su mayoría añaden funciones de control y autenticación de usuarios, así como reglas de filtrado de cada uno de los contenidos solicitados y las funciones de registro de logs.

Algunas de las ventajas se encuentra la mejora de velocidad de respuesta a peticiones, respondiendo de manera inmediata guardando la respuesta de una petición para darla directamente cuando otro usuario la solicite. Una de las maneras para tener contenido actualizado es el de conectarse con el servidor remoto para así comprobar que la versión que se tiene en caché sea la misma que la existente en el servidor remoto. Existen distintos tipos, características y funciones principales,

que a continuación se mencionan; Proxy caché Web, NAT, Transparente, Anónimo, Inverso y Abierto.

Dependiendo del tipo de tráfico que circula por una red se requiere de un proxy que cumpla con las necesidades del tráfico, en caso de requerir el aceleramiento de descarga de contenidos evitando una sobrecarga en la salida de Internet o en la autenticación de usuarios. (Costas Santos, Seguridad y Alta Disponibilidad, 2014)

2.1.11. Redes

Una definición de redes puede hacer referencia a un conjunto de elementos interconectados y organizados para lograr un fin u objetivo común. se pueden designar diferentes significados; una de ellas es la red telefónica que intercomunica a una población; otra es una red informática o de computadoras, donde ocurre el intercambio de información (internet, se puede definir como una red), etc. Existe un sinfín de definiciones y áreas donde se aplica una red, se dice que es un sistema donde los elementos que la componen son autónomos y están conectados entre sí por medios físicos y lógicos, que son capaces de comunicarse para enviar y recibir recursos, estos pueden ser recursos periféricos, carpetas y documentos que la componen.

Algo más sencillo de entender es la comunicación que existe dentro de las computadoras donde permite la transmisión de datos de una máquina a otra, logrando con ello un intercambio de todo tipo de información y recursos. Que, en conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos que comparten archivos, recursos (hardware), servicios (acceso a internet, e-mail, chat), etc. generan un incremento en la eficiencia y productividad de las organizaciones. (Faure González & García Zayas, 2012)

2.1.11.1. Infraestructura de red

Un término para conocer la definición de infraestructura, es que sirve como sostiene y permite funcionar algo. En general las infraestructuras constituyen soportes físicos donde a través de ellas se presentan las actividades económicas y sociales de un país. Se puede definir como la infraestructura que posibilita que varios dispositivos

intercambien datos entre sí, conectados por un medio físico que permita la transmisión de los datos. Cada uno de los dispositivos que conforman la red también se conocen como nodos, en cuanto a los medios físicos a través de los cuales viajan datos, pueden ser medios guiados (cable de cobre o la fibra óptica), o se pueden utilizar ondas electromagnéticas transmitidas a través del aire.

En conclusión, una infraestructura de red da paso al acceso de archivos ubicados en otras computadoras de una empresa u organización, donde se pueden enviar datos a otros dispositivos de comunicación. (Santos González, 2014)

Componentes físicos y lógicos

Como ya se sabe, la infraestructura de red es la plataforma que da soporte a la red, que proporciona un canal estable y confiable por el cual se producen comunicaciones, que es dividida en tres categorías de componentes de red: la primera son los dispositivos que se conforman de los medios como elementos físicos o el hardware, que a su vez se compone por componentes visibles, como una computadora, una PC, un switch, un router, un punto de acceso inalámbrico o el mismo cableado que se utiliza para conectar todos estos dispositivos. La segunda son los medios inalámbricos, los mensajes se transmiten a través del aire mediante radiofrecuencias visibles u ondas infrarrojas.

La tercera y última se refiere a los servicios y procesos, que son programas de comunicación, denominados “software”, que son ejecutados en los dispositivos conectados en red. Normalmente proporciona información en respuesta a una solicitud, incluyendo varias de las aplicaciones de red comunes que utilizan los usuarios, por ejemplo, servicios de hosting de correo electrónico, web hosting, etc. Estos procesos proporcionan la funcionalidad que direcciona y traslada mensajes a través de la red. (Cisco, 2019)

Clasificaciones de redes

En función de la distancia física entre los nodos de una red, las comunicaciones y servicios que esta proporcione, las redes se pueden clasificar como área local,

metropolitana y amplia. Se sabe que las redes pueden transmitir y recibir información con el fin de aumentar la eficiencia y efectividad organizacional a la vez que permiten que grupos de trabajo ubicados en diferentes puntos geográficos comparten documentos y opiniones, lo cual fomenta el trabajo en equipo, las ideas innovadoras y las estrategias de negocio dependiendo al giro de la organización.

2.1.12. LAN

Las redes LAN (Local Area Network o red de área local) es aplicada a una red de datos cuando los dispositivos de la red se encuentran ubicadas en un área geográfica limitada. La distancia que surge entre estos dispositivos hacia una red LAN puede variar entre unos pocos metros hasta varios cientos de metros, en ocasiones kilómetros. Los equipos deben pertenecer a una misma unidad organizativa, es decir una empresa, institución educativa, organismo público, etc. Los estándares para una red LAN son Ethernet y Wi-Fi. Para comprender mejor, se dice que es una simple red punto a punto donde una organización pequeña puede usar para compartir archivos y dispositivos de hardware, como impresoras.

En ocasiones este tipo de red no cuentan con un servidor, sino que, en su lugar, cada computadora está conectada a la siguiente, su desempeño consiste comúnmente menor debido que, en realidad, una computadora comparte los recursos de otra. (M. Stair & W. Reynolds, 2010)

2.1.13. MAN

La siguiente red es conocida como MAN (Metropolitan Area Network o red de área metropolitana) esta es aplicada en redes que unen a redes LAN o a su vez dispositivos dispersos en varias ubicaciones dentro de un núcleo de población, o de varios cercanos entre sí. Se ponen en funcionamiento por los administradores de telecomunicaciones que operan en la zona de cobertura de la red MAN. Por ejemplo, una MAN puede agrupar muchas redes instaladas dentro de una ciudad en una sola red de gran tamaño o, inclusive, conectar varias LAN en una sola LAN extensa. En pocas palabras una red de telecomunicaciones que conecta a usuarios con sus dispositivos en un área geográfica que abarca un campus o toda una extensa región. (Santos González, Diseño de redes telemáticas, 2014)

2.1.14. WAN

Para continuar, se hablará de la red de área amplia (WAN, por sus siglas: Wide Area Network) que conecta regiones geográficas de gran tamaño. Este tipo de red puede ser propiedad privada o rentada, e incluye redes públicas. Un ejemplo sencillo para comprender el término de esta red es cuando se genera una llamada telefónica de larga distancia o se accede a internet, en ese momento se hace uso de una WAN. Esta consiste de equipos de cómputo que son propiedad del usuario junto con el equipo de comunicaciones de datos y enlaces de telecomunicaciones que son proporcionados por compañías transmisoras y proveedores de servicios. Se dice que las redes WAN se pueden dividir en dos partes, la red de acceso y la red de transporte, la primera se refiere a la infraestructura necesaria para que los clientes de una operadora accedan a la red WAN, la segunda es la infraestructura de la red WAN, aunque en ocasiones se considera red WAN tanto a la red de acceso como a la red de transporte. (M. Stair & W. Reynolds, 2010)

2.1.15. Ethernet

Este tipo de red se diseñó como una tecnología *half-duplex,* es decir, que la transmisión de datos entre una estación de origen y una de destino solo se puede producir en un único sentido a la vez. Cualquier estación ethernet antes de transmitir información, esta comprueba que el medio esté libre, para que pueda transmitir y ocuparlo. Para que una red Ethernet pueda trabajar en modo *full-duplex* se tienen que cumplir ciertas condiciones: tomar en cuenta el medio físico quien tiene que permitir la transmisión full-duplex, solo puede haber dos dispositivos conectados entre ellos y que las tarjetas de red de los dos equipos deben soportar este tipo de transmisión. Una ventaja de utilizar Ethernet es el aumento del rendimiento de la red, permitiendo distancias mayores y de tal manera que simplifica el funcionamiento, porque se utiliza un protocolo de acceso al medio. (Íñigo Griera & Barceló Ordinas, 2009)

2.1.16. Red inalámbrica

Las redes WLAN (Wireless Local Area Network con sus siglas: Red Inalámbrica de Área Local) se definen como extensiones de las redes cableadas mediante la tecnología de radiofrecuencia que permiten la movilidad de cada uno de los usuarios que conforman una red, este estándar de comunicaciones en que se basan tecnologías WiFi, que son capaces de alcanzar una distancia mucho mayor en base a repetidoras, interconectando diversos tipos de instrumentos mediante ondas de radio. Las versiones del estándar IEEE 802.11 que soportan gran velocidad son conocidas como el 801.11n y el 802.11ac. Se sabe que son redes de rápida instalación, movilidad y accesibilidad, es por ello, que este tipo de redes son fundamentales para desarrollar la tecnología IP por un servicio masivo y velocidad en la transmisión de datos.

El modo de configuración de una red inalámbrica de banda ancha debe pasar por la administración de switches, routers y puntos de acceso mediante un software controlador que sea de ayuda en las tareas de configuración, así mismo el monitoreo de la misma que debe ser soportada por ese mismo software para realizar el monitoreo de estadísticas en la red de acceso WLAN, el soporte del protocolo SNMP y configuración de alertas. (Mariño Arroyo, Márquez Camarena, & Núñez Lira, 2019)

2.1.17. Metodología de Investigación

La metodología de investigación se divide en varias etapas y procesos que la conforman, el diseño metodológico, implica decidir los procedimientos, estrategias y operacionalidad de éstos para alcanzar los objetivos de investigación para cada tipo de proyecto. Para entender mejor, es llevar a la práctica los pasos generales del método científico, al planificar las actividades sucesivas y organizadas donde se alojan las pruebas que se han de realizar y las técnicas para recabar y analizar los datos. Existen dos tipos de enfoques en la investigación: el enfoque cuantitativo y cualitativo. Estos enfoques emplean procesos metódicos y empíricos en su esfuerzo para generar conocimiento, estos métodos hacen uso de cinco estrategias que son similares y relacionadas:

Mediante la observación y evaluación de fenómenos, se establecen suposiciones o ideas, demuestran el grado en que dichas suposiciones o ideas tienen fundamento, son revisadas sobre la base de las pruebas o del análisis, de manera que proponen nuevas observaciones y evaluaciones para esclarecer, modificar y fundamentar estas suposiciones e ideas o inclusive generar otras. El primer enfoque es el cuantitativo, que generalmente utiliza la recolección de datos para probar hipótesis con base en la medición numérica y el análisis estadístico, con el fin de establecer pautas de comportamiento y con ello probar las distintas teorías pensadas. El segundo enfoque, es el cualitativo que, a diferencia del primero, este utiliza la recolección y análisis de los datos para afinar las preguntas de investigación o revelar nuevas interrogantes en el proceso de interpretación. Tanto en el proceso cuantitativo como cualitativo es posible regresar a una etapa previa, a su vez el planeamiento siempre puede ser susceptible a modificarse, ya que se encuentra en evolución. (Hernández Sampieri, 2014)

2.1.18. Metodología de Desarrollo

La metodología hace referencia al conjunto de procedimientos basados en principios lógicos, utilizados para alcanzar una gama de objetivos que rigen a una investigación científica o en una exposición doctrinal. Se puede definir una metodología como un conjunto de técnicas, recomendaciones y verificaciones, que permitan sistematizar los procesos en los que se deriva la gestión de un proyecto. El uso de esta herramienta puede aportar ciertas ventajas como: facilitar la tarea de planificación, de control y seguimiento de un proyecto, mejorar la relación coste/beneficio, optimiza el uso de recursos disponibles, facilita la evaluación de resultados y el cumplimiento de los objetivos, la comunicación efectiva entre los interesados del proyecto, optimiza las fases de desarrollo define el ciclo de vida que más ajuste a las condiciones y características del desarrollo.

Las metodologías pueden clasificarse en dos grupos, las metodologías tradicionales, que se basan en una fuerte planificación durante todo el desarrollo y un ciclo de vida más tradicional, y en cambio las metodologías ágiles, en donde el desarrollo de software es incremental, cooperativo, sencillo y adaptado. (Girón Sevillano, 2021)

2.1.18.1. Metodología OOSTMM - (Open Source Segurity Testing Methodology Manual)

OSSTMM se define como una guía para mejorar la seguridad en los equipos informáticos, es así que esta metodología se divide en canales, módulos, ambientes y fases según la prueba de seguridad que se desea realizar. Se estandariza para las buenas prácticas de seguridad para la implantación de un sistema de seguridad de información. Como principal propósito es el de proveer de una metodología científica para examinar la organización sobre la seguridad de adentro hacia afuera, como segundo propósito es proveer guías para el auditor de sistemas, destinadas a la certificación de la organización.

Esta metodología realiza algunas pruebas de seguridad que pueden abarcar todas las formas y tipos, que van desde la intrusión, hasta la auditoría guiada. OSSTMM contempla seis tipos de test: Blindaje o Hacking ético, doble blindaje, auditoria de caja negra o pruebas de penetración, de caja gris, de doble caja gris, test Tándem o secuencial e inverso. La competencia abarca la seguridad operativa, y de manera que se comprometa en las diferentes áreas o canales: seguridad física, de las comunicaciones y del espectro electromagnético. (Cruz-Gavilanes & Martínez-Santander, 2017)

2.1.18.2. UTM (Unified Threat management/Gestión Unificada de Amenazas)

Gestión unificada de amenazas (UTM) o la gestión de seguridad unificada (USM) es una tendencia en el mercado de seguridad de firewall. Es una solución en las industrias de seguridad de redes, se dice que es el avance de cortafuegos tradicional capaz no solo de proteger contra intrusiones, pero del mismo modo filtra contenido, spam, detección de intrusiones, equilibrio de carga, fuga de datos, tareas de prevención y antivirus manejadas por múltiples sistemas. UTM es un cortafuego que inserta la identidad del usuario en la coincidencia de reglas de firewall, permitiendo a las empresas configurar políticas e identificar a los usuarios directamente por el nombre de usuario en lugar de direcciones IP.

El objetivo de UTM es simplificar la solución de seguridad general a pesar del alcance y la complejidad de los problemas de seguridad. Uno de los más aparentes aspectos de esta simplificación es la consolidación física de un punto de productos dentro de una sola tecnología; de ahí parte el término gestión unificada de amenazas. Las ventajas en la administración de amenazas tecnológicas en la gestión de seguridad son: la reducción de

la complejidad, fácil de implementar, existen sinergias con las soluciones de software de alta gama, baja interacción del operador y la fácil resolución de problemas. Un objetivo del desarrollo de la tecnología de seguridad es proteger datos o activos de información, minimizando la pérdida de datos dentro de las redes corporativas.

Existen dos tipos de UTM que son hardware appliances y software, la primera son dispositivos rackeables y no rackeables que vienen con su respectivo Sistema Operativo y una infraestructura para su respectiva conexión y configuración dentro de la red. Entre sus características principales están: firewall throughput, VPN throughput y cantidad máxima de usuarios. La segunda son sistemas operativos listos para ser instalados, con licencia y Open Source, este software depende de un hardware para funcionar, hardware puede ir desde un potente servidor hasta una sencilla PC, siempre y cuando cumpla con las características mínimas que requiere el Software UTM. (Agham, 2016)

2.2 Metodología de la Investigación

La investigación será profundizada en un estudio cuantitativo con un alcance descriptivo para llevar a cabo el proceso del proyecto. El alcance descriptivo es el más apto para el desarrollo de la investigación porque se conoce el problema, pero se busca describir fielmente cómo ocurre su magnitud y su alcance en torno al estado actual de la infraestructura de red en el H. Ayuntamiento de Teteles, conocer la manera en cómo se está elaborando actualmente, la organización de la red de datos, como laboran los usuarios y si existen afectaciones en el uso de este servicio.

Otro tipo de investigación, fue el de campo, para ello se dio a la necesidad de dirigirse personalmente al Ayuntamiento de Teteles, de tal modo se obtuvo un panorama más amplio en cómo está constituida la infraestructura de red, que a su vez esta investigación se fusionó con la técnica de observación para la recolección de información, se tomaron fotos de

algunas de las áreas, con la aplicación de estos mecanismos se logró recolectar datos más confiables, certeros y con una idea clara del estado actual del lugar, la situación de los recursos informáticos, el tipo de conexión de red y el funcionamiento de cada una de las áreas que conforman la organización.

El propósito es medir una serie de conceptos en específico como: el tipo de conexión de red que utilizan, si es WAN o LAN, los dispositivos que ocupan este servicio, cuantos usuarios manejan estas herramientas y que tanto conocen de la seguridad que se debe aplicar diariamente en sus actividades laborales, si existen técnicas de seguridad, los recursos con los que cuentan, entre otros datos importantes para el desarrollo del proyecto.

Mediante la descripción, representación y el resumen de información se generan gráficas que apoyen a entender y resumir la información del estudio realizado. Para ello, a lo largo del proceso de investigación se aplicaron una serie de cuestionarios al personal del H. Ayuntamiento de manera que agilicen la obtención de datos y se logren analizar mediante la estadística descriptiva representando dicha información.

Población objetivo

La investigación está dirigida a la seguridad de red de datos que se genera en las instituciones de gobierno del estado de Puebla, con el uso de la técnica de muestreo intencional se pretende llevar a cabo la aplicación de encuestas a los integrantes o usuarios de una organización de gobierno con el objetivo de conocer el manejo, la seguridad de red de datos, tipo de infraestructura y los recursos informáticos con los que se cuenta actualmente, para ello se delimitó la población objetivo tomando en cuenta los ayuntamientos que conforman el distrito electoral federal #3 que pertenecen al Estado de Puebla, los cuales son: Teziutlán, Ayotoxco de Guerrero, Cuetzalan del Progreso, Chignautla, Hueytamalco, San José Acateno, San Juan Xiutetelco, Tenampulco, Tlatlauquitepec, Atempan, Hueyapan, Yaonáhuac, Zaragoza, Zacapoaxtla y Teteles de Avila Castillo, este último es la muestra a estudiar. (Electoral, 2021) Con respecto a los resultados que se obtengan en los cuestionarios se busca conocer la prevalencia del estado actual de infraestructura de red en el Ayuntamiento de Teteles, al mismo tiempo tener un

panorama más amplio de la situación actual y percatarse de las necesidades que requiere esta población.

Por otra parte, el municipio de Teteles de Avila Castillo se encuentra localizado en la sierra Norte del estado de Puebla, contando con una superficie de 9.83 kilómetros cuadrados, actualmente cuenta con una población total de 6,653 personas aprox., perteneciente al distrito federal electoral núm. III con cabecera en Teziutlán. (INEGI, 2021)

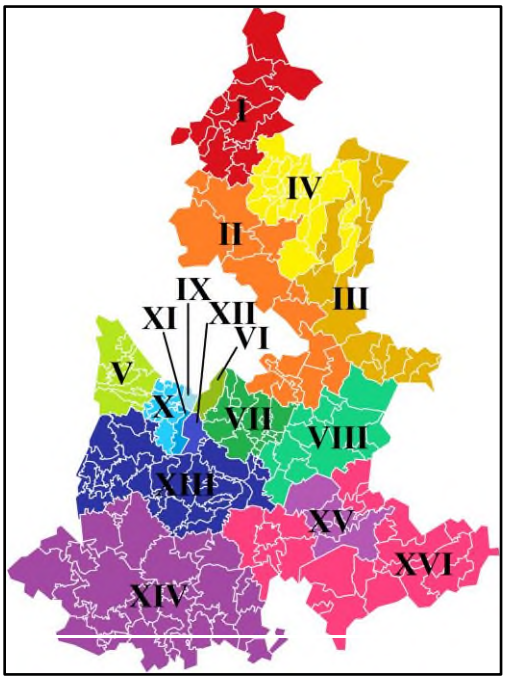


Ilustración 2 Región 03 de Puebla

Ilustración 3 División de regiones de Puebla

El proceso de recolección de información implica generar un plan detallado de procedimientos que nos apoyen a reunir los datos necesarios con el propósito de obtener, conocer y analizar los datos que aporten información valiosa al proyecto. con el objetivo de analizar la relación que existe entre el estado actual de la infraestructura, la disponibilidad de la red, el manejo de los recursos informáticos y el grado de seguridad en la información. Con la finalidad de recolectar los datos que vengan del instrumento de recolección de información a utilizar, que a continuación será descrito.

Como fue mencionado anteriormente el tipo de investigación a emplear en el proyecto es de carácter cuantitativo, ya que se evaluará la realidad de la calidad de los servicios que se

otorgan a la población, en su caso el H. Ayuntamiento de Teteles a través de la aplicación y análisis del instrumento de recolección de información: para este proyecto se optó por utilizar el instrumento de recolección de datos más utilizado como son los cuestionarios que consiste en un conjunto de preguntas que serán respecto al estado actual de la infraestructura de red, recursos informáticos y seguridad dirigido hacia los usuarios (empleados) que conforman el Ayuntamiento.

Instrumentos de recolección de datos

Como ya fue mencionado el instrumento de recolección de datos será el cuestionario, ya que los actores sociales son quienes proporcionan los datos relativos, con la aplicación de cuestionarios mixtos se abordarán tanto preguntas cerradas como abiertas y que por motivo de la contingencia actual que vive el país, se hace de forma autoadministrada y se envían los cuestionarios a usuarios del H. Ayuntamiento, mediante formularios en Google Drive.

Normalmente se deben tomar en cuenta los siguientes puntos:

Se dice que es sumamente importante ser breve y lo suficientemente amplio para obtener datos factibles, que, a su vez, sea expuesta la importancia del tema de manera clara, precisa y ordenada, comenzando de forma general a lo específico. (Osorio Rojas, 1998, 1).

2.3 Metodología de desarrollo

El H. Ayuntamiento de Teteles de Ávila castillo ubicado en calle Epifanio Valera #1, colonia centro, CP. 73930, Teteles de Ávila Castillo, Puebla. (Teteles, 2021) Conformada por varias áreas que van desde la secretaria de ayuntamiento hasta la dirección de obras, su estructura organizacional se muestra a continuación:

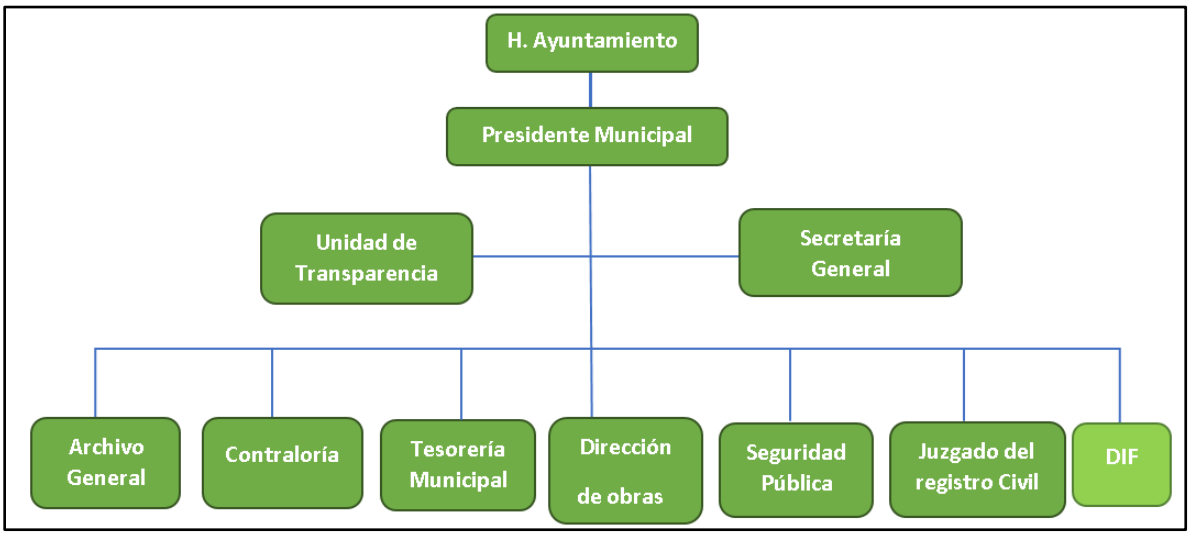


Ilustración 4 Organigrama Ayuntamiento de Teteles de Ávila Castillo

Levantamiento de Información

Actualmente, para conocer la infraestructura de la red del Ayuntamiento se tomó la decisión de asistir personalmente a las instalaciones y realizar una inspección de las instalaciones de manera general y ver como se encuentran los recursos informáticos que son parte de la organización. Para tener un panorama más amplio de estado físico de la infraestructura, a continuación, se muestran algunas imágenes de los equipo y recursos de algunas de las oficinas del ayuntamiento:

Ilustración 5 Módem

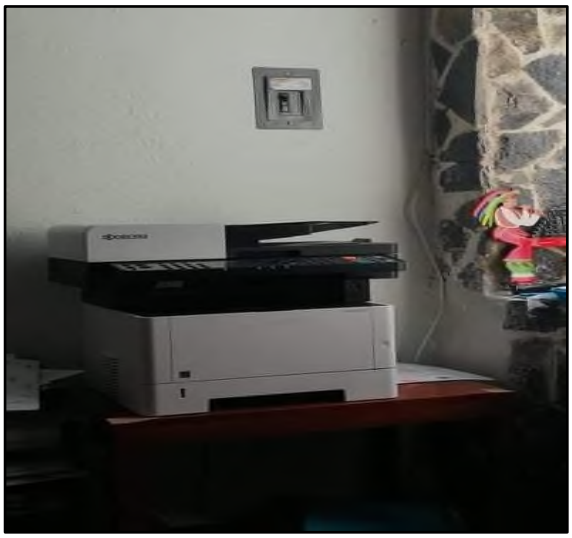


Ilustración 6 Copiadora en red

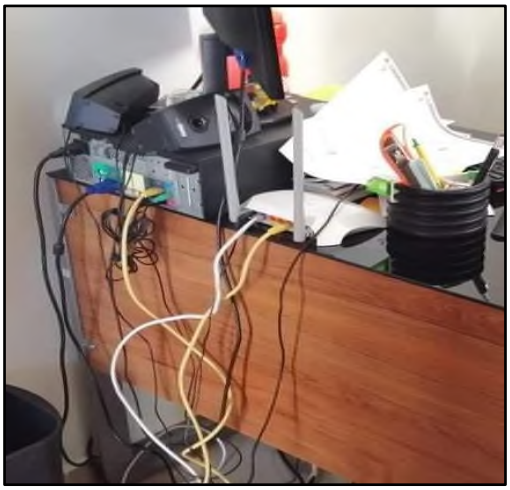


Ilustración 7 Cableado

Ilustración 8 Equipos informáticos

Ilustración 10 Módem 2

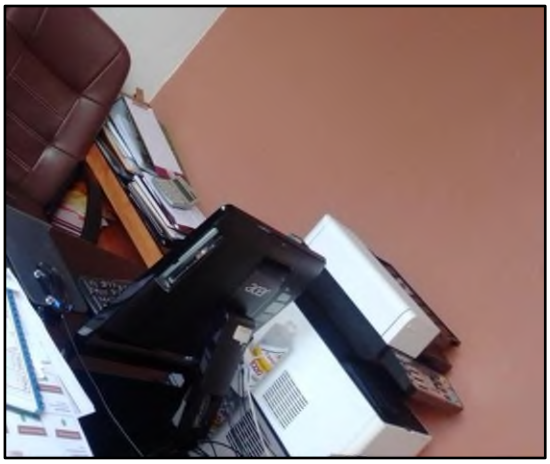


Ilustración 9 Equipo de cómputo

Por tal motivo, se resume en una tabla para lograr tener un panorama mucho más amplio del estado actual de los recursos informáticos.

Recursos informáticos activos en el Ayuntamiento de Teteles						
			Tipo de Red			
Área	Equipo	Marca	LAN	WAN	Cantidad	Usuarios
Presidencia	Laptop			x	1	1
Secretaría	Módem	Telmex			1	
	Computadora de escritorio			x	1	1
	Impresora			x	1	
Juzgado	Módem	TP Link		x	1	
	Computadora de escritorio			x	2	10
Registro civil	Computadora de escritorio		X		1	1
Contraloría	Laptop			x	1	1
	Impresora		x		1	
Tesorería	All one			x	1	1
	Laptop			x	2	2
	Copiadora		x		1	
	Impresora		x		2	
Regiduría	All one			x	1	1
	Impresora			x	1	
Regiduría de cultura	Computadora de escritorio			x	1	1
Obras públicas	Computadora de escritorio			x	2	2
	All one			x	1	1
	Módem	TP Link			1	
	Impresora		x		1	
DIF	All one			x	1	1
	Computadora de escritorio			x	1	1
	Laptop			x	1	1
	Copiadora		x		1	
	Módem	Telmex			1	
Total					29	25

Tabla1 Recursos informáticos

Analizando los recursos informáticos y los modos de conexión a internet se logra identificar que la mayoría de las áreas del ayuntamiento se conectan mediante la red de Wifi, considerando que el número de usuarios se puede duplicar ya que normalmente hacen uso de dos o tres dispositivos que pueden ser celulares, tablets, etc., conectados al mismo tiempo a la red de internet del ayuntamiento, dando como resultado problemas de velocidad de internet y la seguridad de los equipos, debido a que es propensa a las interferencias o la pérdida de señal en toda la infraestructura. Durante la visita al ayuntamiento, algunos de los usuarios comentaban acerca de las fallas de internet y que en ocasiones no se lograba realizar de manera eficiente los servicios que se otorgan a la ciudadanía.

Además, el libre acceso que existe a la red de internet ya que cualquiera de los usuarios se puede conectar, afectando la velocidad de internet, a su vez que no hay restricciones, alguna política o un uso adecuado de los recursos informáticos, la falta de un sistema de control de acceso a la red wifi que limite la conexión a los usuarios y dispositivos conectados.

Por estos motivos se propone el presente proyecto donde se logren cubrir las necesidades sobre los problemas antes mencionados, diseñando una infraestructura adecuada que brinde los servicios necesarios que generen mayor seguridad, un sistema de control de acceso a la red, una reducción de dispositivos que brindan internet como lo son los módems, la generación de políticas que fortalezcan el uso de la red, a su vez los usuarios tengan la certeza de que realizaran sus actividades de manera segura.

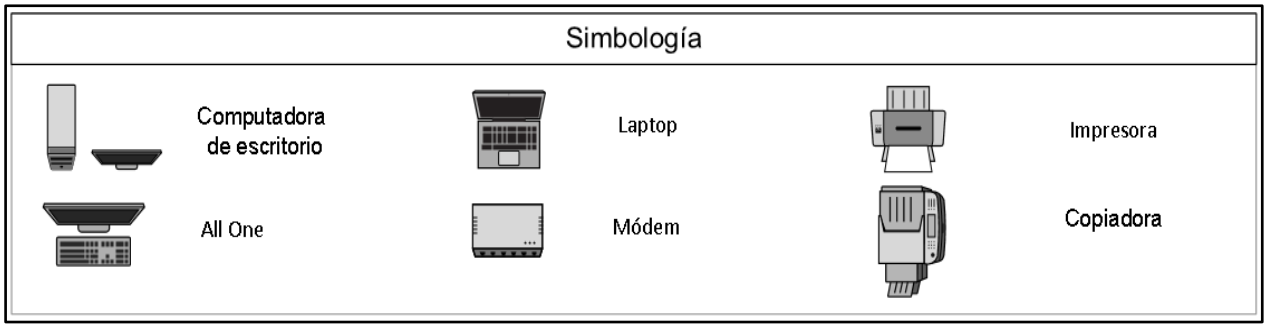


Ilustración 11 Simbología croquis de infraestructura

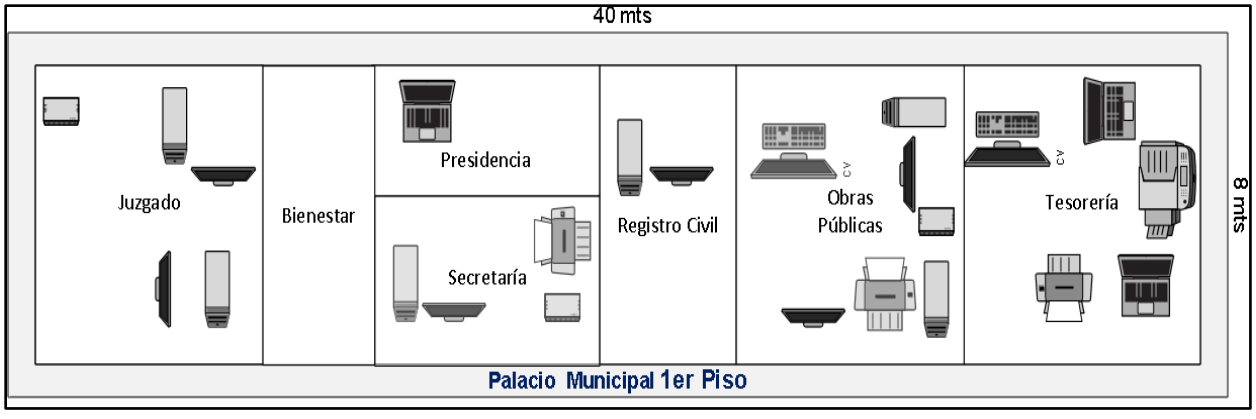


Ilustración 12 Recursos informáticos piso 1 ayuntamiento

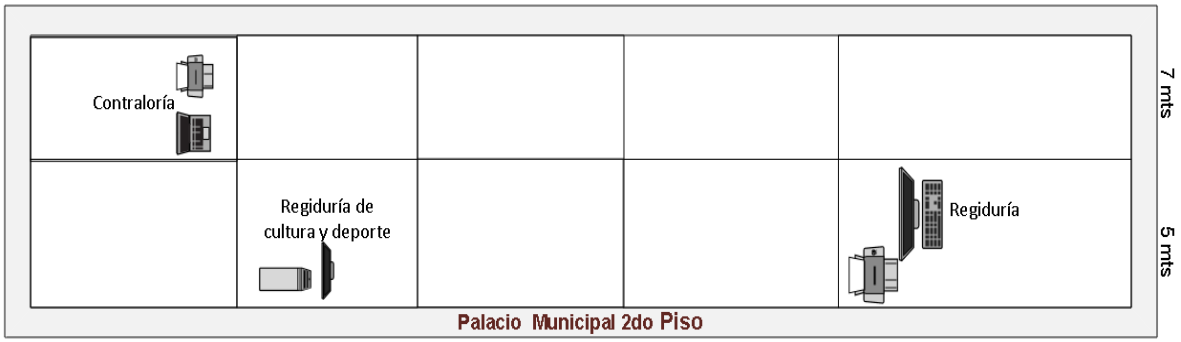


Ilustración 13 Recursos informáticos piso 2 ayuntamiento

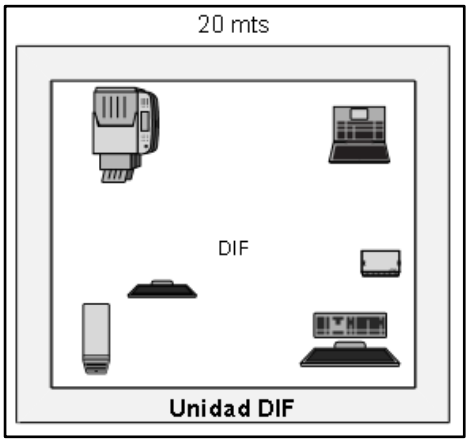


Ilustración 14 Recursos informáticos Unidad del DIF Teteles

El motivo de seleccionar UTM como metodología de desarrollo es que reúne en un solo hardware diferentes servicios de seguridad de forma que se implementa en el punto perimetral del área de red. La Gestión unificada de amenazas (UTM), apoyará a encaminar y dirigir el proyecto en cuestión al diseño de la seguridad perimetral, otorgando una solución de seguridad mediante varias funciones de protección en la red. Algunas de las funciones que se pueden aplicar a favor de la seguridad son antivirus, prevención y detección de intrusiones, filtrado de contenido, la prevención de fugas y el firewall de red que es uno de los temas más puntualizados a tratar en este proyecto. Otros servicios son el enrutamiento remoto, la traducción de direcciones de red y la compatibilidad para redes privadas virtuales (VPN).

Según la forma en cómo se desempeñe la red, se seleccionan los elementos que otorgue gran ayuda ya que en una sola herramienta se concentran diferentes funciones de control de amenazas, facilitando así el trabajo de los usuarios de la red en general.

Herramienta UTM a utilizar en el diseño de la seguridad perimetral

El diseño de seguridad perimetral en la infraestructura de red a favor del Ayuntamiento de Teteles cumple con los requerimientos más importantes para garantizar una correcta funcionalidad de las conexiones a internet mediante red y wifi. mediante el estudio de distintas herramientas de firewall se optó por el sistema Smoothwall, se ajusta con los parámetros de rendimiento del sistema ya que es una plataforma libre de licenciamiento apoyando a la reducción de costos por parte del ayuntamiento, a su vez que cumple con todas las funcionalidades necesarias para brindar las soluciones que vayan más acorde con la situación actual del ayuntamiento.

El H. Ayuntamiento de Teteles de Ávila Castillo como ya se mencionó no posee el presupuesto para el licenciamiento de UTM, y la infraestructura es pequeña, el software a utilizar es smoothwall, que es un firewall open-source basado en FreeBSD, es parte de UTM OpenSource y que brinda varias utilidades que pueden ser implantadas y están acorde a las necesidades del organismo de gobierno. A pesar de ser un software libre, otorga algunas características esenciales para el proceso del diseño y configuración, por ejemplo: es un cortafuego, tiene una tabla de estado, NAT, HA, Multi-WAN, VPN, otorga informes, Monitoreo en tiempo real, clientes DNS, DHCP, etc.

Ubicación del Firewall

Después de tener un panorama más amplio de la infraestructura actual del ayuntamiento de Teteles, se realizó un análisis del área específica para ubicar e instalar el servidor para el sistema de firewall smoothwall. Considerando que debe estar en una ubicación segura físicamente, tomando en cuenta ciertos requisitos como asegurar el estricto acceso a personas ajenas a la administración del sistema, debe estar en una habitación cerrada, con ventilación adecuada, así como el espacio del área, la manera de colocación, el tamaño que abarcara, el número de materiales a montar, entre otros.

Por lo tanto, el sistema de firewall se instalará en el site del área de Regiduría, en cual se encuentra en el segundo piso del palacio municipal, de manera que se instalará de manera segura, para que se ofrezca un mejor servicio y transporte de red de datos.

CAPÍTULO III

IMPLEMENTACIÓN Y PRUEBAS

3.1 Análisis de datos

Cuestionario a usuarios finales

Como ya fue mencionado anteriormente se realizaron unos cuestionarios al personal del ayuntamiento con el fin de conocer el conocimiento y la importancia que los usuarios le dan a las TIC (Tecnologías de la información) en cuanto a seguridad informática y red de datos. Para conocer a fondo lo que conforma esta encuesta, puede visitar el siguiente link: (https:///forms/d/1S9kLISXghLNOSXI_owo_Izw4Ca9XXus56Zptop1CaRk/edit).

Cuestionario de Diseño de Infraestructura de red (Usuario)

Ilustración 15 Cuestionario de Diseño de Infraestructura de red (Usuario)

A continuación, se muestran los resultados:

Gráfica 1: Formación

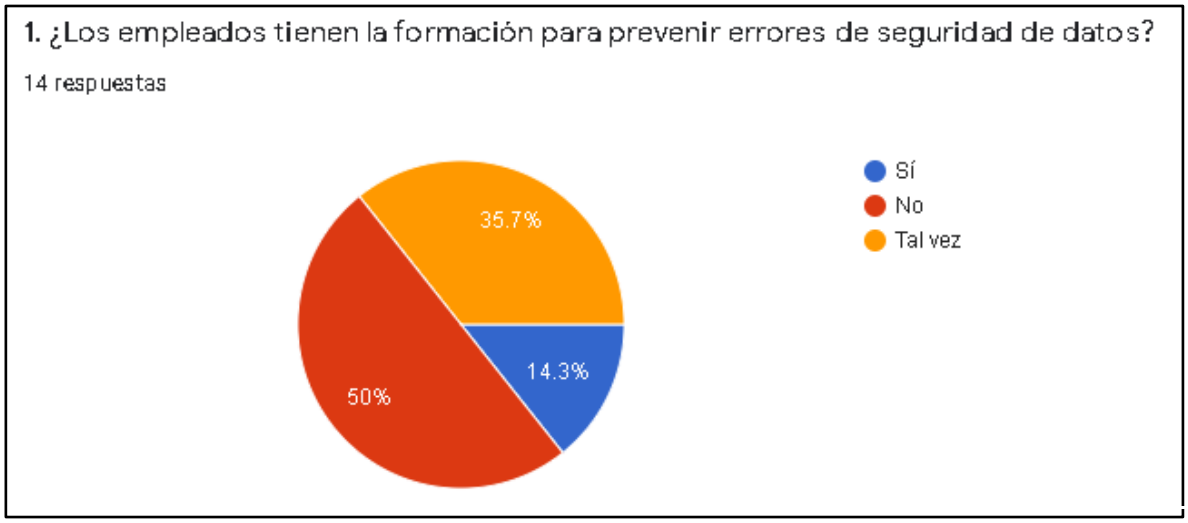


Ilustración 16 Gráfica 1: Formación

Se puede percatar de la falta de formación para prevenir errores en cuestión a la seguridad de datos por parte de los usuarios, es necesario que el personal tenga alguna noción de los inconvenientes que pueden presentarse en las actividades relacionadas con la información de los datos a lo largo de la jornada laboral.

Gráfica 2: Identificación

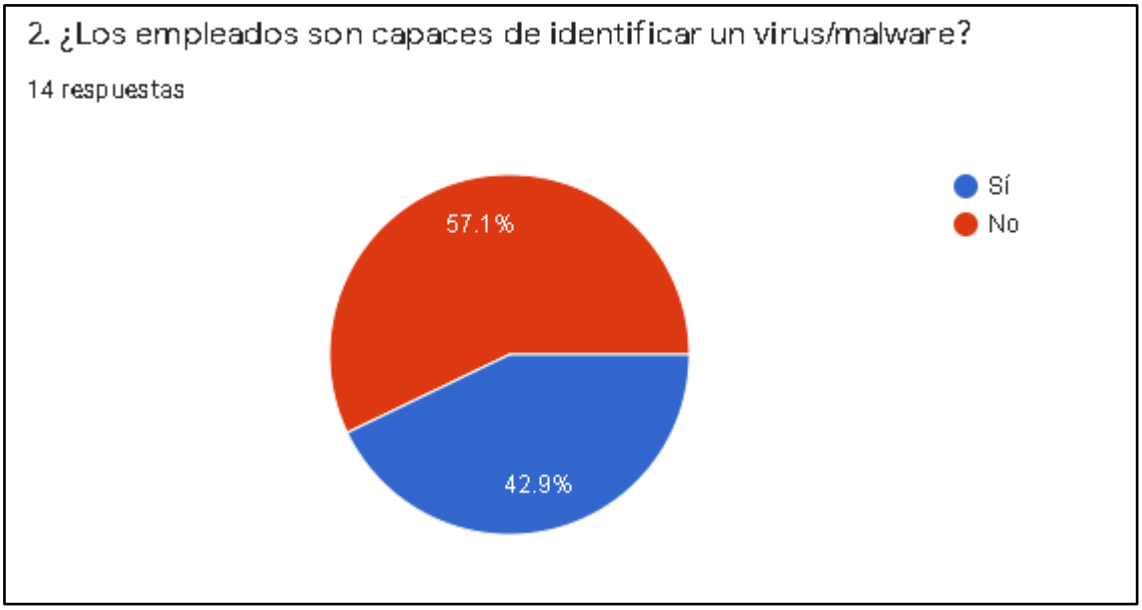


Ilustración 17 Gráfica 2: Identificación

El 57.1% de los usuarios, poco más de la mitad es capaz de identificar algún virus que ataque a sus computadoras o dispositivos de comunicación, pero aun así casi la mitad desconoce las afectaciones que surgen con estos ataques, esto debe reforzarse, para mitigar los diversos ataques, un ejemplo el phishing que sufren algunas instituciones de gobierno.

Gráfica 3: Riesgos

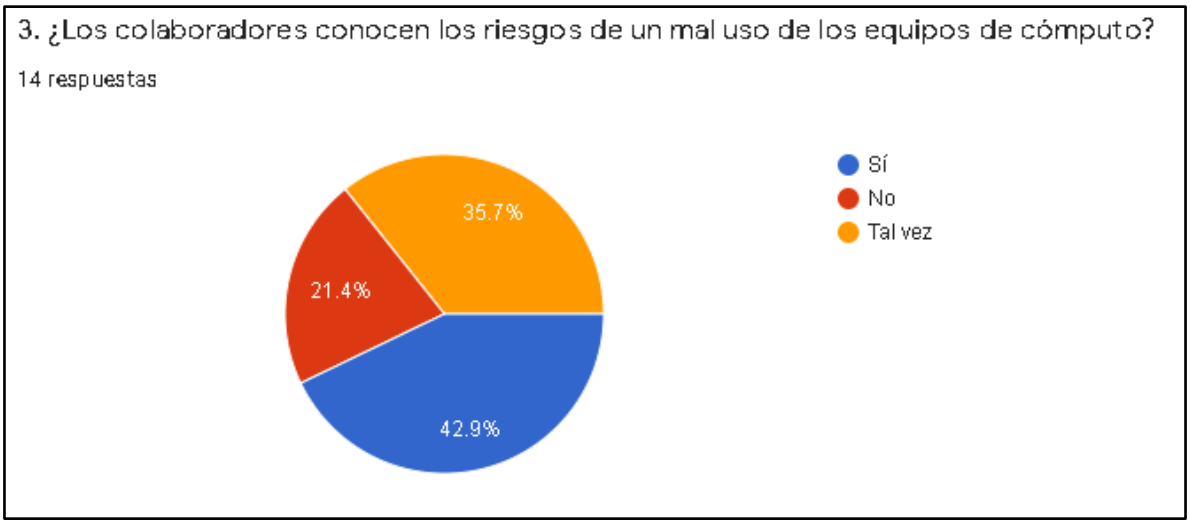


Ilustración 18 Gráfica 3: Riesgos

Las respuestas se dividen en tres partes, el porcentaje más alto es de un 42.9% donde los usuarios conocen los riesgos que conlleva dar un mal uso a sus equipos de trabajo, sin embargo, un 35.7% tal vez si tenga alguna noción de lo que puede surgir al no tener un debido cuidado de los recursos informáticos y el 21.4% desconoce totalmente de estos riesgos, se sabe que los recursos deben tener un cuidado y mantenimiento constante para que tengan una larga vida y funcionen de una manera adecuada.

Gráfica 4: Streaming

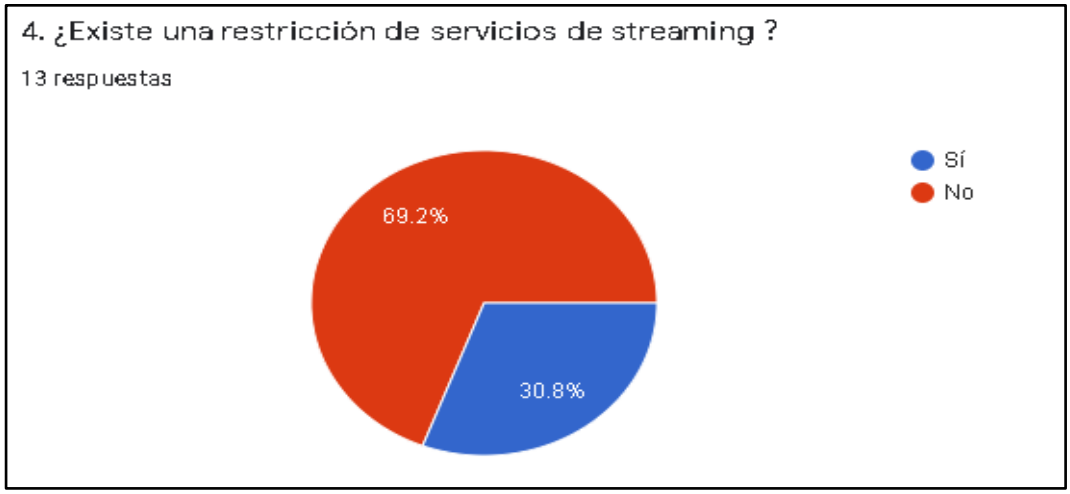


Ilustración 19 Gráfica 4: Streaming

El streaming ha sido parte de la distracción actual de los usuarios a nivel mundial, es como se logra percatar por parte del personal del ayuntamiento donde el 69.2% no tiene una restricción de estos servicios en sus computadoras, laptops, all one, celulares, etc. solamente el 30.8% menciona que, si tiene restricción, pero no se sabe a ciencia cierta qué tipo de servicios no tengan acceso.

Gráfica 5: Prevención

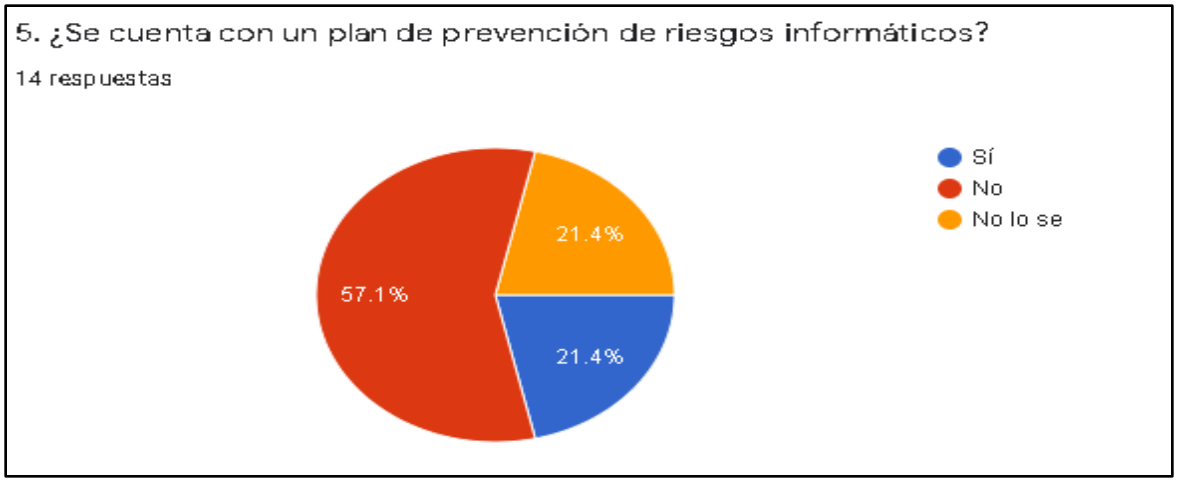


Ilustración 20 Gráfica 5: Prevención

El 57.1% afirma que no existe un plan de prevención enfocado a los riesgos que surgen a nivel informático, esto da paso a optar por establecer un plan que mitigue los distintos tipos de riesgos que pueden afectar a los recursos informáticos y la infraestructura de red de datos.

Gráfica 6: Calidad de los servicios

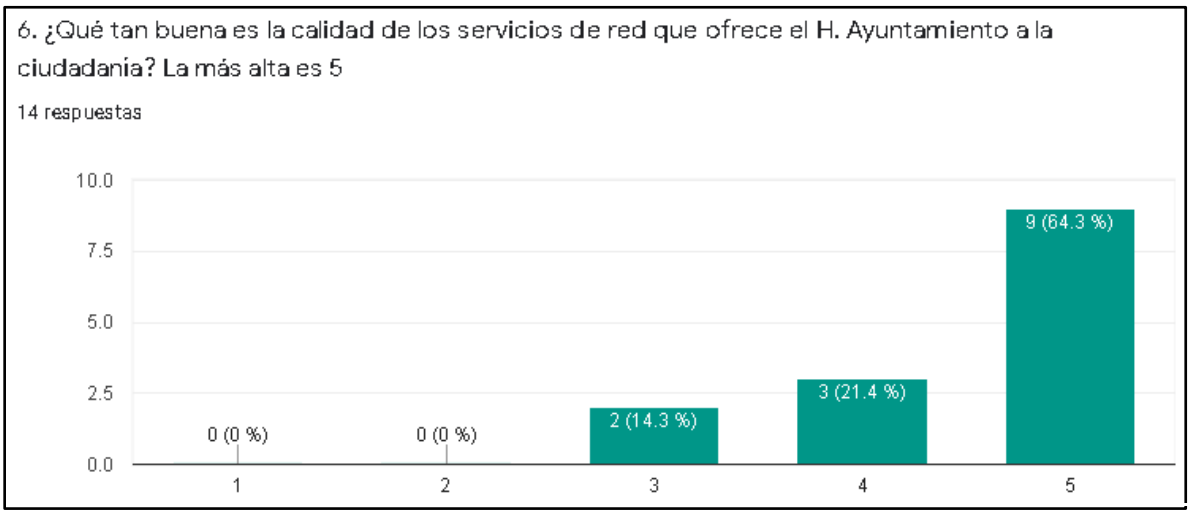


Ilustración 21 Gráfica 6: Calidad de los servicios

La mayoría de los usuarios califican con buena calidad a los servicios que provee la red a las aplicaciones, sistemas, programas, flujo de datos y que consideran que garantizan un alto nivel de rendimiento.

Gráfica 7: Cursos de orientación

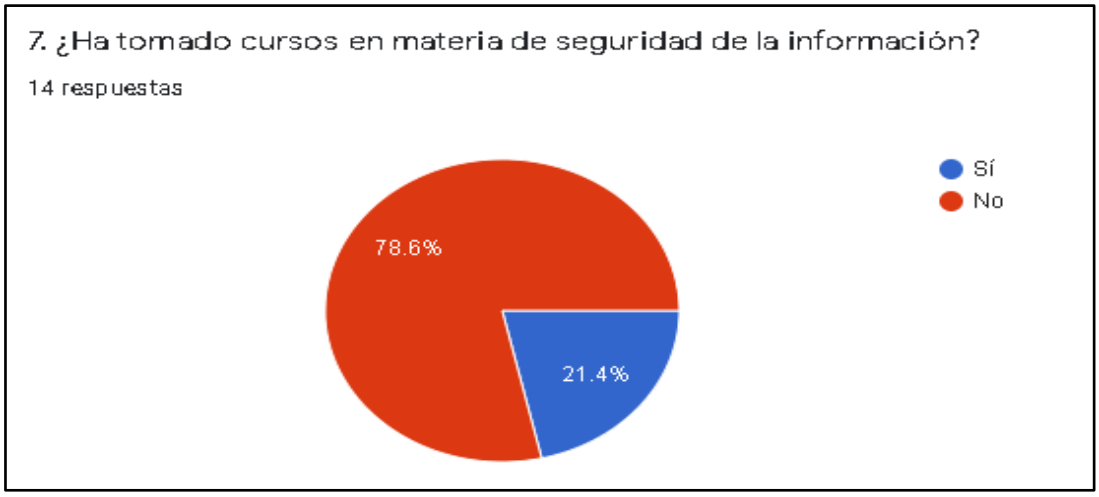


Ilustración 22 Gráfica 7: Cursos de orientación

Para tener un panorama claro de lo que significa la seguridad de la información, se requiere que los usuarios conozcan a fondo lo que esto conlleva, para ello es necesario optar por cursos que guíen a los empleados y de tal manera estén preparados cuando surja algún inconveniente en la seguridad de los recursos informáticos. El 78.6% de los usuarios del ayuntamiento no han tomado algún curso que hable acerca de este tema y en la actualidad es necesario estar informados en este ámbito.

Gráfica 8: Amenazas

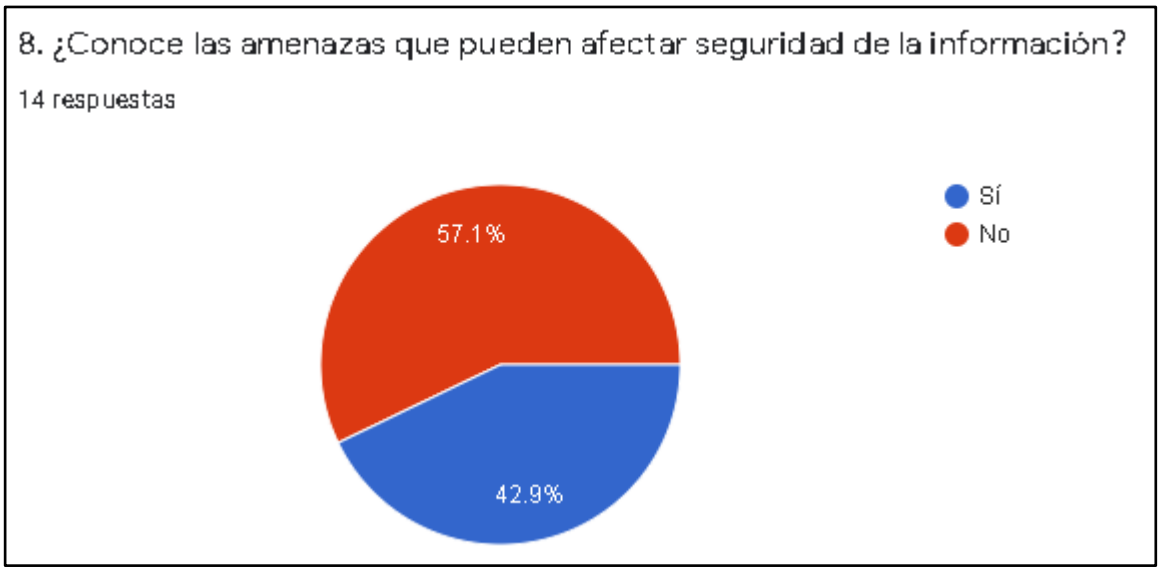


Ilustración 23 Gráfica 8: Amenazas

Otro tema interesante es conocer los tipos de amenazas que pueden afectar a los recursos y datos de información, es posible percatarse que la mayoría desconoce acerca del tema, un 57.1% afirma no tener conocimiento de las afectaciones y motivos por lo que surgen estas amenazas.

Gráfica 9: Rendimiento

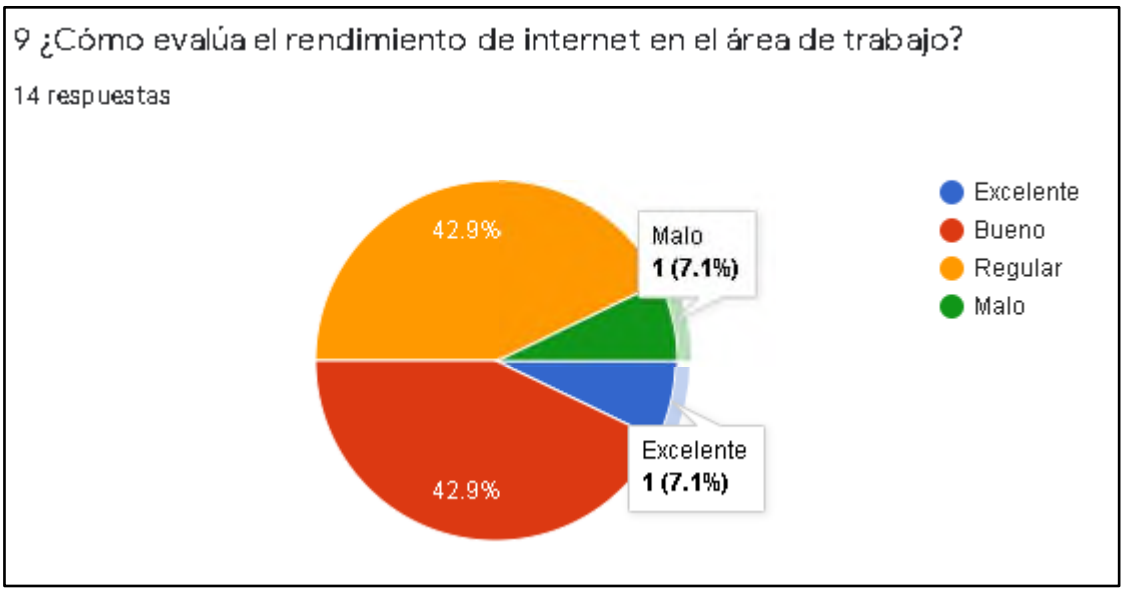


Ilustración 24 Gráfica 9 Rendimiento

Con el estudio antes realizado se conoce que la mayoría de los usuarios hacen uso de la red de wifi para sus actividades diarias, es así cómo se plasmaron las respuestas de los empleados en donde el 42.9% califica como regular el nivel de rendimiento y donde sólo un 7.1% lo califica como excelente, sin dejar de lado que de igual manera un 7.15% califica como malo el rendimiento de este servicio de internet.

Gráfica 10: Control

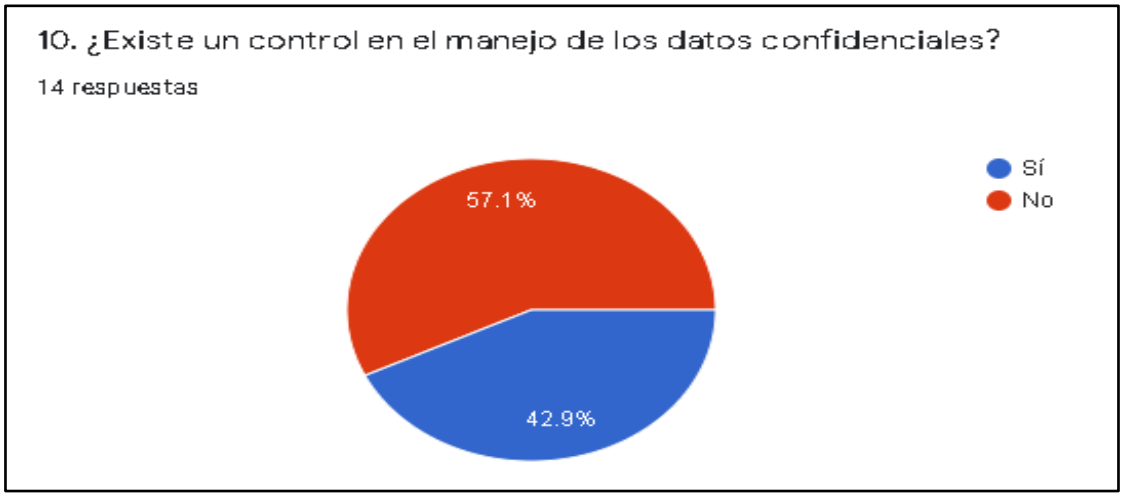


Ilustración 25 Gráfica 10: Control

Por otro lado, el 57.1% afirma que no se le da un control al manejo de información, es necesario controlar el flujo de datos y poner énfasis en la seguridad que debe tener cierta información confidencial.

Gráfica 11: Sistema de seguridad de datos

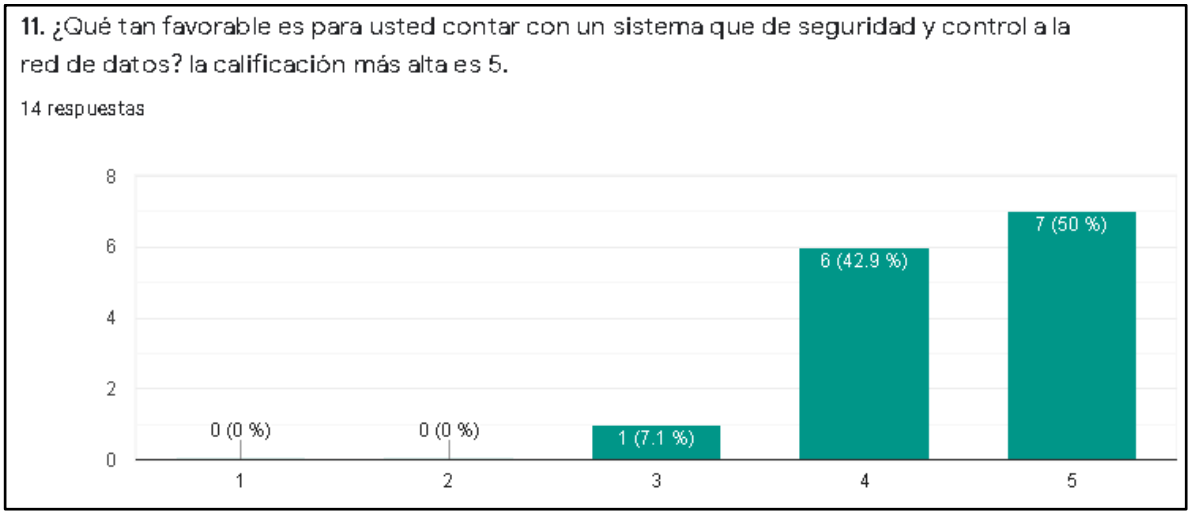


Ilustración 26 Gráfica 11: Sistema de seguridad de datos

La mayoría de los usuarios califica como necesario y favorable el optar por un sistema que brinde seguridad y un debido control en la red de datos con un 50%. Donde se logren identificar los riesgos, la mejora de los procedimientos, así como las políticas preexistentes o incluso implementar nuevas.

Gráfica 12: Instalaciones de red y comunicación

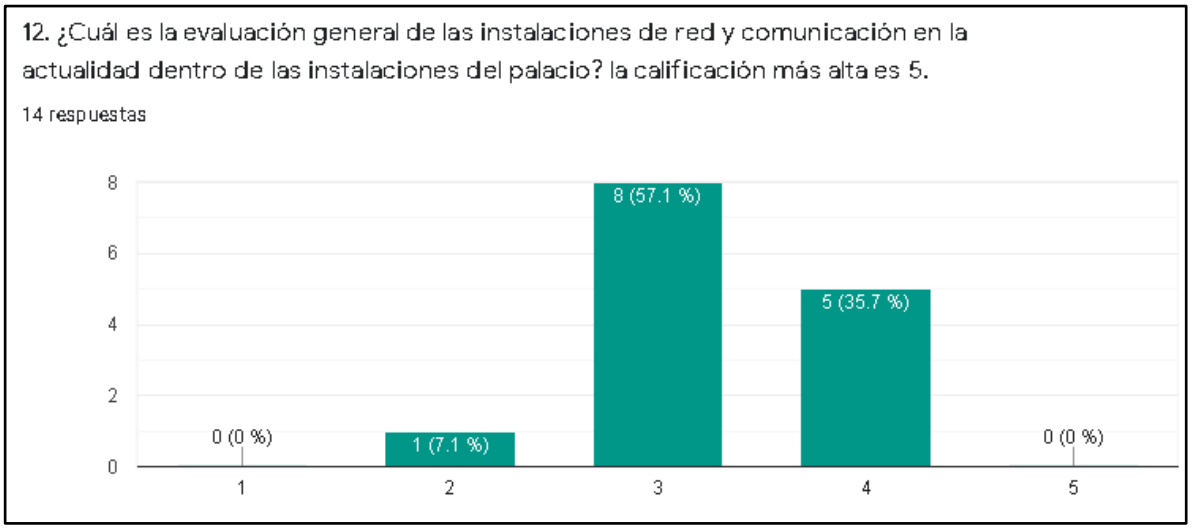


Ilustración 27 Gráfica 12: Instalaciones de red y comunicación

Las instalaciones de red funden como una parte importante para la comunicación dentro del ayuntamiento, el 57.1% califica a las instalaciones con un nivel medio, esto confirma la necesidad de mejorar la infraestructura para un mejor rendimiento de los recursos informáticos.

Gráfica 13: Funcionamiento

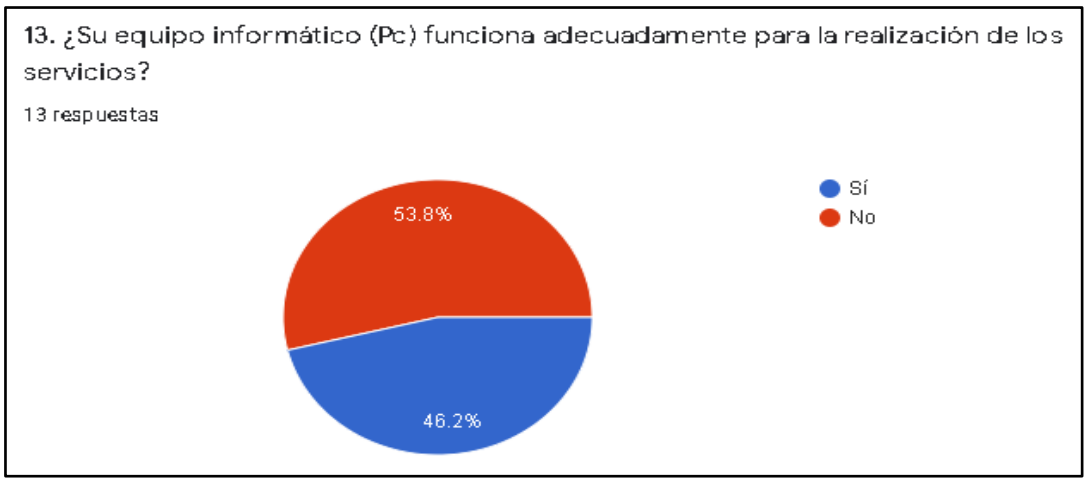


Ilustración 28 Gráfica 13: Funcionamiento

Del mismo modo, los equipos informáticos deben estar en buenas condiciones para las diversas actividades y procesos que llevan a cabo los usuarios, caso contrario con las respuestas de los usuarios donde el 53.8% dice que sus equipos no cuentan con un correcto funcionamiento, donde se puede percatar las malas condiciones en las que se encuentran la mayoría de los recursos informáticos.

Gráfica 14: Actualización

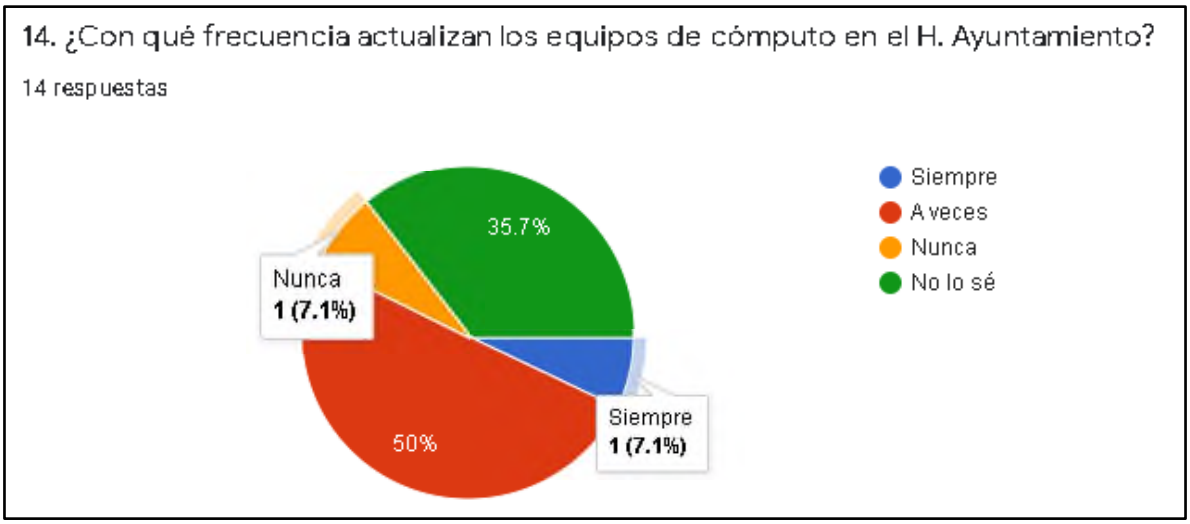


Ilustración 29 Gráfica 14: Actualización

Se sabe que en la actualidad es necesario tener actualizados los sistemas, equipos, programas, etc. para disminuir las afectaciones que pueden surgir cuando se enfrentan a fallas, virus, ataques, entre otros. Solo el 7.1% respondió que siempre tienen actualizados sus equipos de cómputo, caso contrario donde el 50% no aplica constantemente las debidas actualizaciones y el poner énfasis en que el 7.1% nunca ha optado por generar actualizaciones a sus equipos de cómputo.

Gráfica 15: Medidas de seguridad

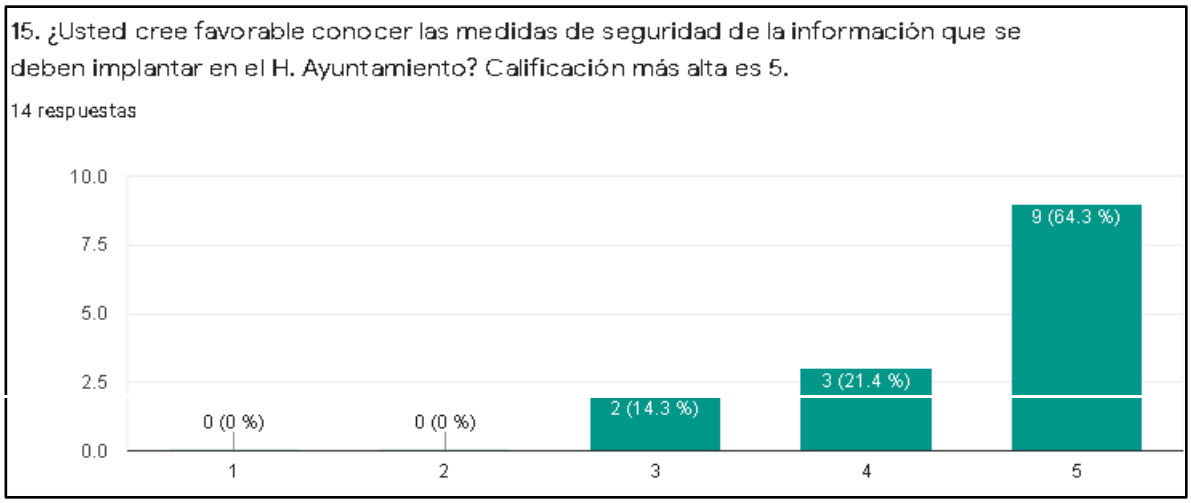


Ilustración 30 Gráfica 15: Medidas de seguridad

Se puede notar el interés que los empleados tienen acerca de conocer más acerca de las medidas de seguridad de la información que pueden aplicarse a cada una de las áreas del ayuntamiento de Teteles, donde el 64.3% está interesado en las ventajas que pueden surgir al implementar mejores herramientas de seguridad en la infraestructura de red y datos.

3.2 selección de pruebas estadísticas

En la presente investigación se tomó como pruebas estadísticas a la estadística descriptiva ya que apoya a condensar o resumir el total de los datos o características de una serie de valores, a su vez que este método es relativamente sencillo y eficiente de resumir y caracterizar los datos resultantes, de manera adecuada de presentar la información obtenida. (Hernández Sampieri, 2014)

Así que, para la recopilación y organización de la información de los cuestionarios aplicados, se tuvo que valer de las técnicas numéricas y gráficas, mediante las cuales se presenta la información, sin hacer predicciones ni inferencias acerca de la población objetivo. Las gráficas antes mostradas, apoyan de forma resumida a entender, conocer y profundizar acerca de la seguridad del H. Ayuntamiento de Teteles de Ávila Castillo, con

los datos recabados, se obtiene un panorama más amplio de la situación actual, de las necesidades, la manera en como aplican la seguridad y el control en los datos en cada área del ayuntamiento.

Por esta razón y más es porque fue seleccionada la estadística descriptiva como método de recolección y análisis del conjunto de los datos, con el objetivo de describir las características y comportamientos de este conjunto mediante las gráficas.

3.3. Realización de análisis (Interpretación)

Con base a los resultados obtenidos de los correspondientes cuestionarios aplicados a los empleados del ayuntamiento de Teteles de Ávila Castillo, se logró percatar las diversas situaciones que se presentan actualmente, un tema a puntualizar es que el 50% de los usuarios no cuentan con una formación que aporte a conocer las maneras de prevención de errores en la seguridad de los datos, a su vez, un 57.1% no tienen la noción de lograr identificar cómo se genera un virus, las causas y los riesgos que puede tener al adquirir un malware en los recursos informáticos de los que hace uso.

Se puede observar que más de la mitad de los usuarios carecen de conocimientos referentes al tema de seguridad en los datos que se manipulan diariamente, del mismo modo, mencionar que es importante dar un uso adecuado a estas herramientas de trabajo, estar en las mejores condiciones físicas para el proceso correcto de información. Tema que un 21.45 de los empleados desconoce, es fundamental que los usuarios conozcan los riesgos que se presentan debido a un mal uso de los equipos de cómputo y que a su vez es necesario contar con un plan de prevención de riesgos informáticos; un 57.1% de las respuestas dieron a conocer que no existe un plan que atienda este tipo de situaciones.

El uso de servicios de streaming, que se conforma de redes sociales, audio y video, no debe ser usado en horas de trabajo, pero el 69.2% de los empleados utilizan estos servicios, lo cual puede ser motivo del bajo rendimiento que existe en la velocidad de internet y que afecta a otros usuarios en la realización de sus tareas administrativas.

Otro tema a comentar es el de la calidad de los servicios de red que ofrece el ayuntamiento hacia la ciudadanía, a pesar de que un 64.3% califica como bueno el servicio, el 37.75% le da un nivel intermedio a la calidad de los servicios que se otorgan en el ayuntamiento.

Con el resultado de algunas de las preguntas del cuestionario, permite dar la siguiente recomendación que puede ser de apoyo para los empleados de esta institución, el 78.6% de los resultados afirman que no han tomado algún curso en materia de la seguridad de la información, es por ello que se recomienda a los encargados de la gestión de programas culturales o sociales el tomar en cuenta la gestión y aplicación de cursos que estén dirigidos en el tema de la seguridad de información, prevención de riesgos, cuidado de los recursos informáticos, entre otros temas que pueden ser de interés y ayuda para los empleados de dicho ayuntamiento.

El rendimiento de internet es otro tema que evaluaron los usuarios, donde sólo un 7.1% califica como excelente a la calidad del rendimiento de este servicio, a comparación del 42.9% que evalúan como bueno y regular, esto puede ser resultado del uso de internet en otros recursos como el streaming que es el principal causante de las no tan buenas condiciones del servicio de internet, sin dejar de lado que un 7.1% califica como mal al rendimiento.

Otro tema importante es el control del manejo de la información, a través de las respuestas se pudo notar que en la mayoría de los casos no existe un control en el manejo de los datos públicos y confidenciales, esto se refleja en que un 57.1% un poco más de la mitad admite que no existe tal control en el ayuntamiento. Es necesario tomar las acciones necesarias para aplicar estas políticas o normas que aportarán un mejor uso a la información que se genera día con día en la institución de gobierno.

Se les cuestionó a los usuarios acerca de qué tan favorable sería para ellos y el ayuntamiento el contar con un sistema que ofrezca seguridad y control a la red de datos, el 92.9% califican altamente esta propuesta y que es necesaria para mejorar las instalación de red y comunicación. A su vez, es necesario implantar medidas de seguridad de la información que aporten resultados positivos en el H.Ayuntamiento de Teteles de Ávila Castillo

3.4. Comprobación de la Hipótesis

Del análisis de los resultados obtenidos mediante las encuestas realizadas hacia los usuarios de los recursos tecnológicos del ayuntamiento de Teteles, se deriva el cumplimiento de la hipótesis "**El diseño de un mecanismo de seguridad perimetral, contribuirá positivamente en la administración de los sistemas de información en el H. Ayuntamiento de Teteles de Ávila Castillo, Pue."** planteada desde el inicio, con relación a las respuestas obtenidas y la observación del estado actual de las instalaciones, se comprueba que un diseño de mecanismo de seguridad perimetral, en efecto, contribuirá positivamente en la administración de los sistemas y recursos de información en el ayuntamiento de Teteles.

Esto fue comprobado, con la aportación de la información que arrojaron las respuestas de los cuestionarios, donde la mayoría de los usuarios están a favor de adquirir un mecanismo de este tipo y confían en el logro de diversos beneficios a lo largo de los procesos administrativos, tecnológicos, de control y seguridad hacia cada una de las áreas de dicha institución de gobierno.

CAPÍTULO IV

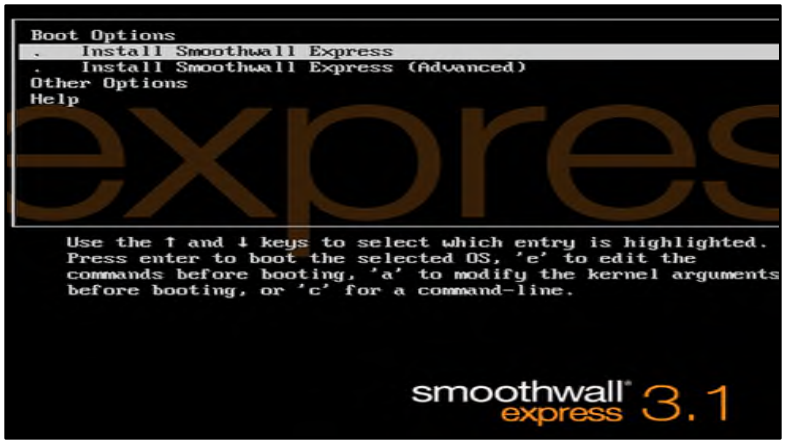
RESULTADOS Y CONCLUSIONES

Diseño y configuración de Smoothwall

Instalación de Smoothwall

Una vez seleccionado smoothwall como el sistema de seguridad perimetral, se procede a demostrar el diseño e instalación del sistema para el ayuntamiento de Teteles. La instalación del firewall smoothwall se llevó a cabo mediante una máquina virtual con el programa Virtualbox, tomando en cuenta características como la capacidad de la computadora, memoria, tomando en cuenta los tipos de adaptadores ya que con ellos la instalación será efectuada correctamente, el resultado se aprecia a continuación:

Paso 1 - Se inicia la instalación del firewall smoothwall con la versión express 3.1.



Fuente 1 Elaboración propia

Paso 2 - Después de aceptar un par de ventanas, cuando se llegue a este punto se seleccionara el idioma del teclado.

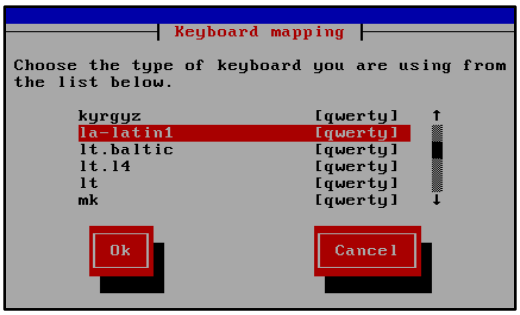


Ilustración 31 Idioma del teclado

Paso 3 - Se dejará abierto el paso a todas las solicitudes entrantes.

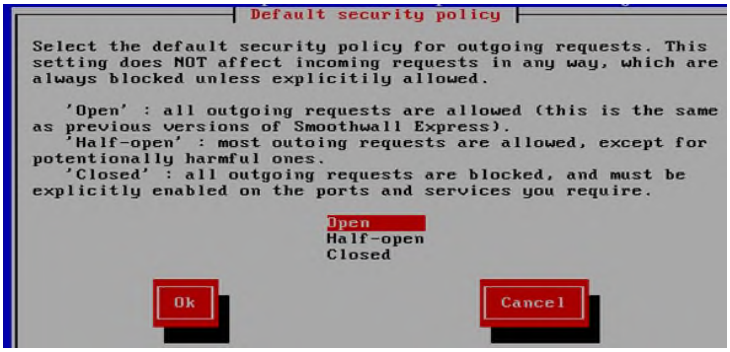


Ilustración 32Solicitudes entrantes open

Paso 4 - Se da paso a la configuración de la red, el tipo de configuración de red será: GREEN - RED. Al seleccionar GREEN se está habilitando la red LAN y RED es para la red WAN.

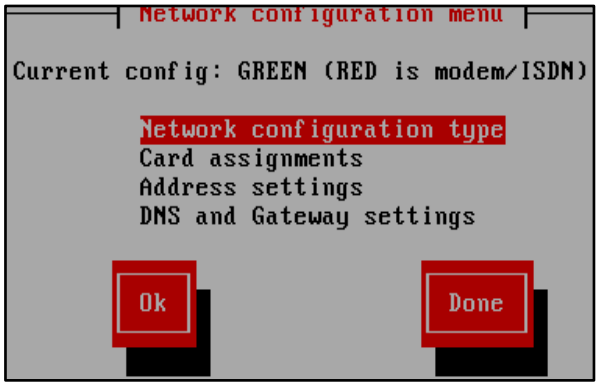


Ilustración 34 Menú configuración de red

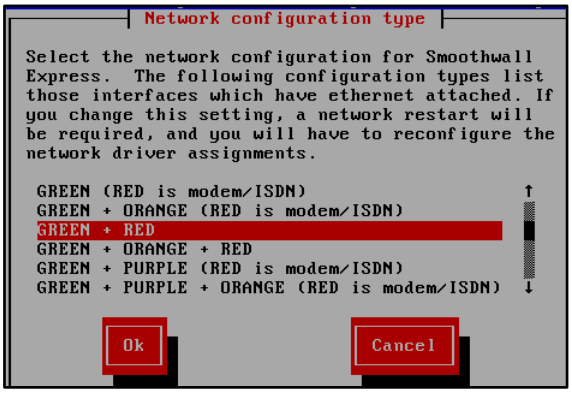


Ilustración 33 Tarjeta Green-Red

Paso 5. Se seleccionarán las tarjetas de red para GREEN y RED.

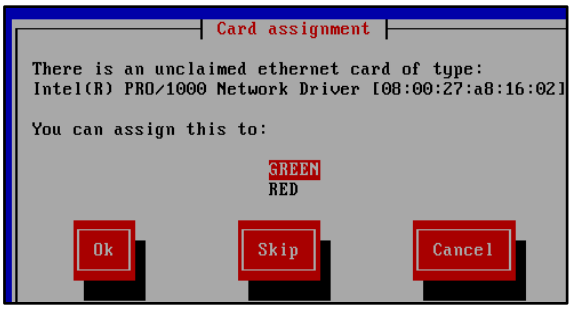


Ilustración 35 Asignación tarheta Green

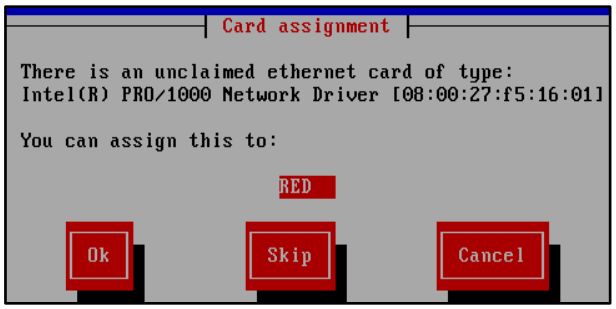


Ilustración 36 Asignación tarjeta Red

Paso 6. Agregar la dirección IP y máscara de subred a la interfaz GREEN.

Ilustración 37 Interface Green

Paso 7. Ahora dar paso a la configuración de la interfaz RED, que en este caso será DHCP.

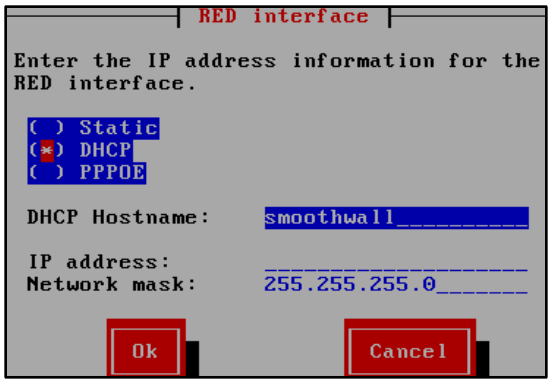


Ilustración 38 Interfaz Red

Paso 8. Habilitar la configuración del servidor DHCP.

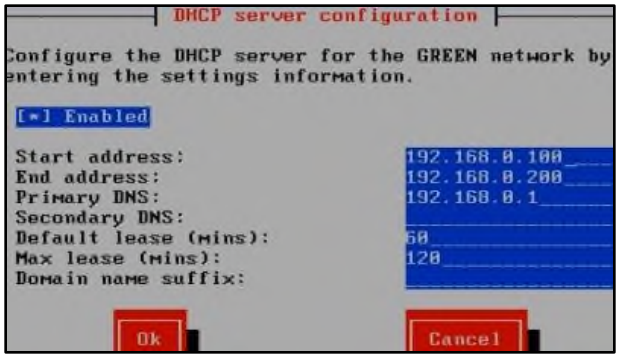


Ilustración 39 Configuración servidor DHCP

Paso 9: Después de estos pasos se asignan las contraseñas para usuario admin y usuario root.

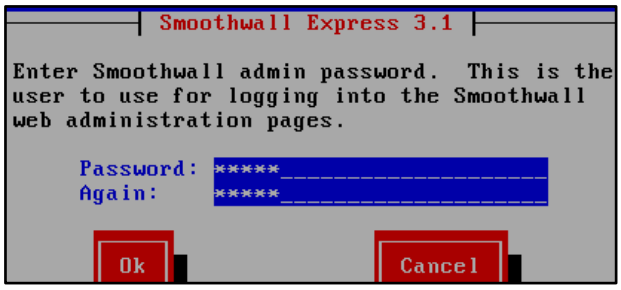


Ilustración 40 Password admin

Ilustración 41 Password root

Es así como se finaliza correctamente la instalación del sistema y automáticamente se reiniciará para ingresar en modo consola, a su vez solicitará la contraseña root, con ello se da paso a ingresar en un navegador de internet en una de las terminales de la red.

Ilustración 43 Finalización de instalación

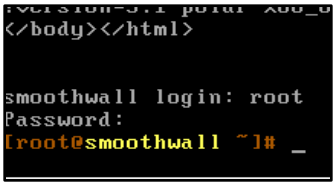


Ilustración 42 Ingreso como usuario root

Paso 10. A continuación se ingresará al navegador y colocar la siguiente dirección con el puerto 81 o 441: http://192.168.0.1:81 o http://192.168.0.1:441, al instante de ingresar se solicitaran el usuario y contraseña, que anteriormente fue configurado.

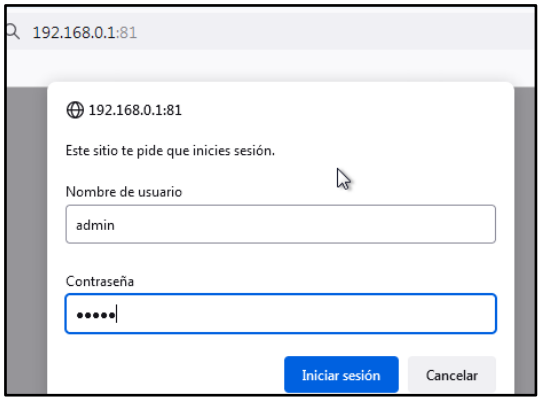


Ilustración 44Ingreso a Smoothwall

Paso 11. Se muestra la pantalla de inicio de Smoothwall 3.1

Ilustración 45 Home Smoothwall

Paso 12. Seleccionar el apartado Services y a su vez la opción de remote access para marcar las dos casillas que se muestran en la ventana.

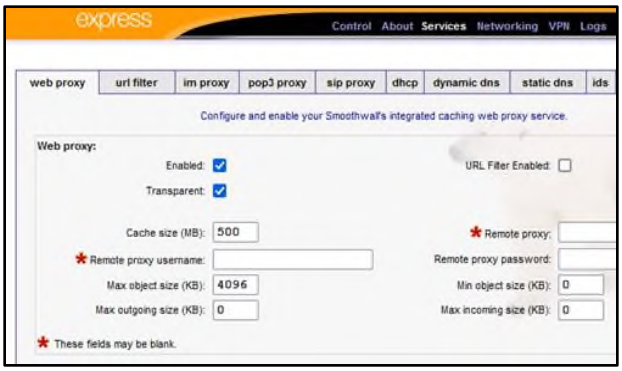


Ilustración 46 Web proxy

Paso 13. Se requiere trabajar con el programa de nombre putty, dicha utilidad se trabajará en consola. Una vez conectados con putty se debe configurar, colocando la dirección 192.168.0.1 y el puerto 222, como se mostró anteriormente.

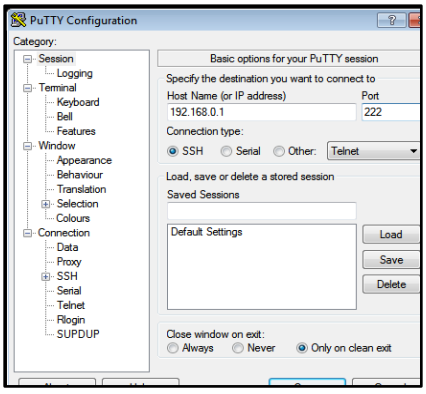


Ilustración 47 Configuración PuTTY

Aceptar el certificado de conexión segura.

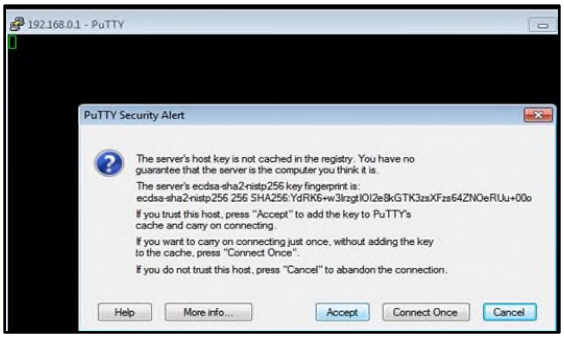


Ilustración 48 Conexión segura PuTTY

Ahora ingresar como usuario root ingresando la contraseña.

Paso 14. Se va a requerir descargar un URL filter desde una página de confianza para la versión del sistema smoothwall, se copia el link y se sepga en la consola, pero antes colocando el comando wget + el enlace copiado y dar enter, esto descargara el paquete.

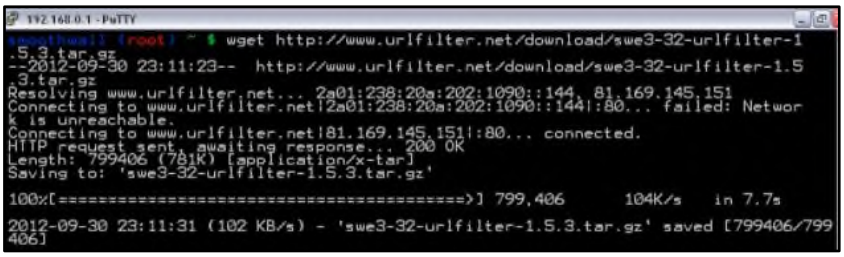


Ilustración 49Descargar Urlfilter

Ahora a descomprimir con el comando tar xvzf.

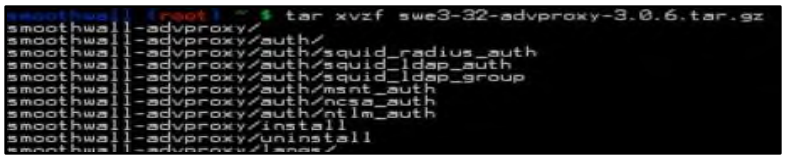


Ilustración 50 Descomprimir Urlfilter

Ingresar a la carpeta del filtro url mediante el comando cd - nombre ce de la carpeta e instalar con el comando script ./install.

Ilustración 51 Instalar Urlfilter

Finalizando la instalación, hay que ingresar nuevamente a la página de configuración web del sistema.

Proxy

Proxy como ya se sabe es un servicio utilizado para el filtrado de contenido, es el encargado de interceptar, almacenar y analizar cada uno de los paquetes entrantes, funciona como bloqueo de los paquetes, adición a ello, funciona como caché, almacenando información de manera local, a su vez solicita un servicio, que puede ser respondido rápidamente, ayudando a la experiencia del usuario que esté navegando. Para este diseño, se establece el puerto proxy 800.

Filtro de Contenido

Este sistema contiene diversas categorías con listas actualizadas URLs, de manera que se clasifican acorde a las necesidades de la organización y su contenido, seleccionando el contenido a bloquear, se recomienda activar la actualización del sistema de manera continua para que siempre esté en la versión más reciente. El filtrado se divide en excepciones por nombre Listas negras y Listas blancas, las primeras se refieren al bloqueo de urls para evitar su ingreso como los servicios de streaming y las blancas son para dar acceso a las urls y que no sean bloqueadas.

Para ingresar al apartado de proxy hay que seleccionar Services donde se podrá observar el tipo de proxy que existe, activar la interfaz Green, colocar un puerto proxy 800, el lenguaje de los mensajes de error en español.

Ilustración 52 Advanced proxy

Así mismo se puede activar o desactivar el filtro url.

Ilustración 53Activación url filter

Configurar el contenido de filtrado por categorías.

Ilustración 54Filtrado por categorías

Configuración de urls por dominios lista negra.

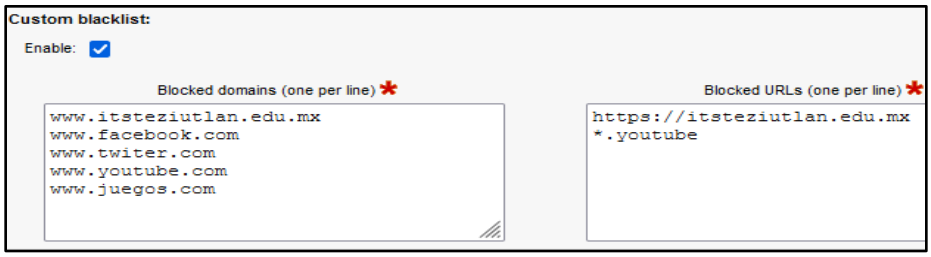


Ilustración 55 Lista negra

Configuración por dominios Lista blanca.

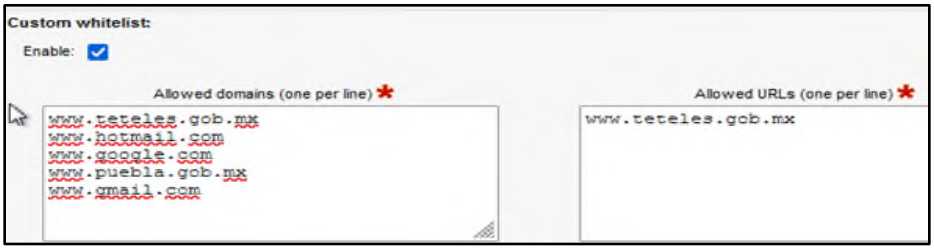


Ilustración 56Lista blanca

Filtrado por expresiones regulares (palabras)

Ilustración 57 Filtrado expresiones regulares

Configuración avanzada de contenido de filtrado

Ilustración 58 Contenido de filtrado avanzado

Asignación de horarios para su funcionamiento donde se seleccionó una actualización semanalmente.

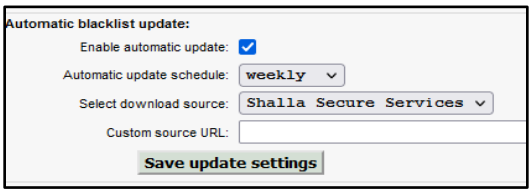


Ilustración 59 Actualización automática

Una recomendación es activar la sección de Automatic blacklist update y seleccionar la frecuencia de actualización automática, una vez activado se comenzará a descargar las listas nuevas, pero hay que esperar a que finalice la actualización.

Es posible configurar el ancho de banda para la conexión que puede ser asignada a cada usuario, se muestra un ejemplo de asignación.

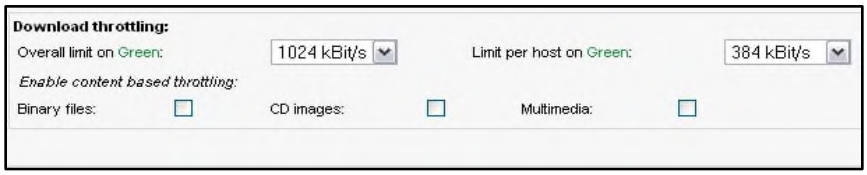


Ilustración 60 Configuración de ancho de banda

Monitoreo

El sistema de seguridad perimetral, tiene añadido el monitoreo de las conexiones que establecen los clientes, donde se pueda visualizar:

- Consumo de ancho de banda: Se puede analizar las conexiones que se encuentran en la red.
- Protocolo: para definir las reglas del firewall a implementar, qué bloquear y qué no.
- Origen/Destino de las peticiones: se puede observar desde y hacia donde se están conectando los usuarios.
- Estado de conexión: permite conocer en tiempo real qué conexiones se encuentran activas, como páginas o servicios web donde los usuarios están navegando.

Se puede visualizar los recursos físicos usados, donde es posible monitorear de manera práctica en el uso de la memoria RAM, se pueden notar las fechas y horas de consumo actual del sistema.

Monitoreo de tráfico interno del Sistema de seguridad perimetral

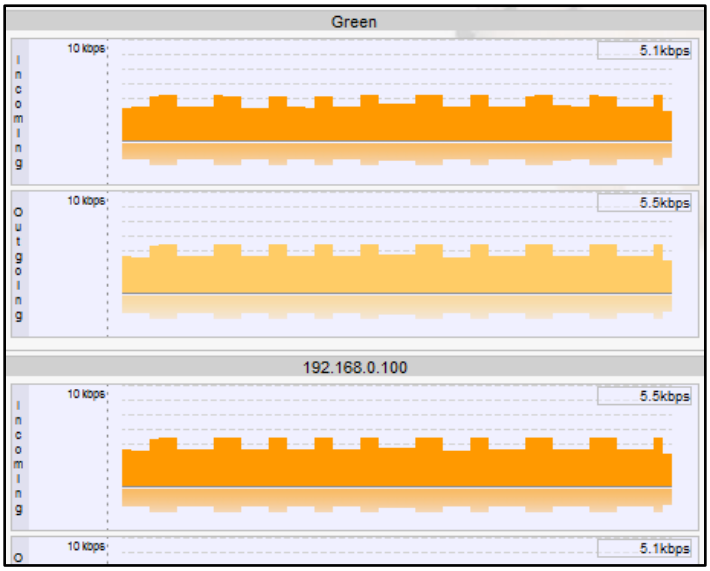


Ilustración 61Monitoreo tráfico interno

Ancho de banda

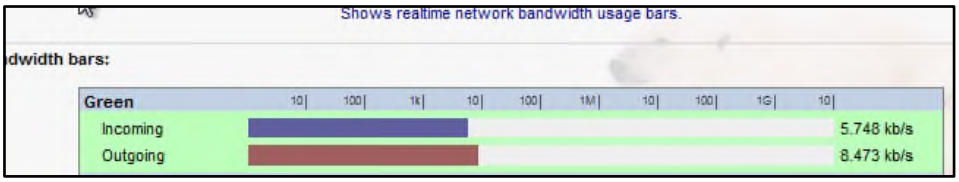


Ilustración 62 Ancho de banda Green

CAPÍTULO IV

Resultados Y Conclusiones

4.1 Resultados

Una vez ingresado las direcciones en la lista negra para bloquear y las demás configuraciones de filtrado, se muestra un ejemplo del bloqueo de la página del ayuntamiento de Teteles.

Ilustración 63Bloqueo página Teteles

Bloqueo de redes sociales con Smoothwall

- Facebook

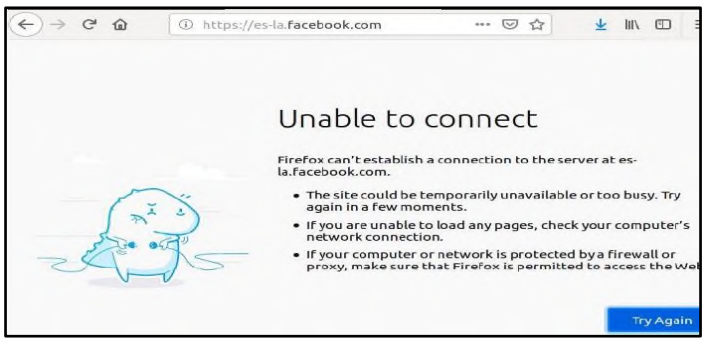


Ilustración 64 Bloqueo facebook

- Twitter

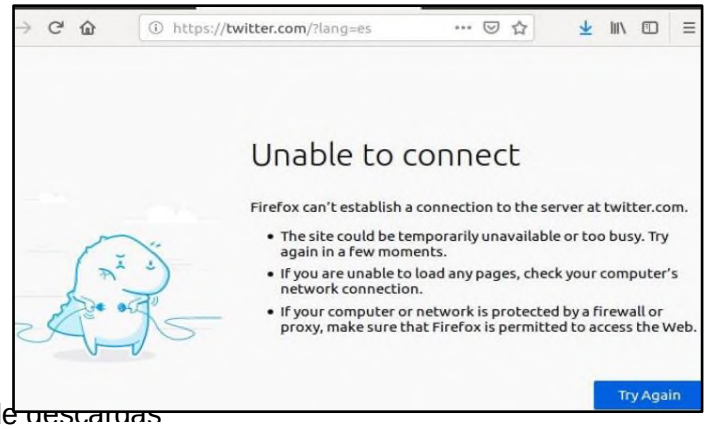


Ilustración 65Bloqueo twitter

Bloqueo de contenido de descargas

- Megafire

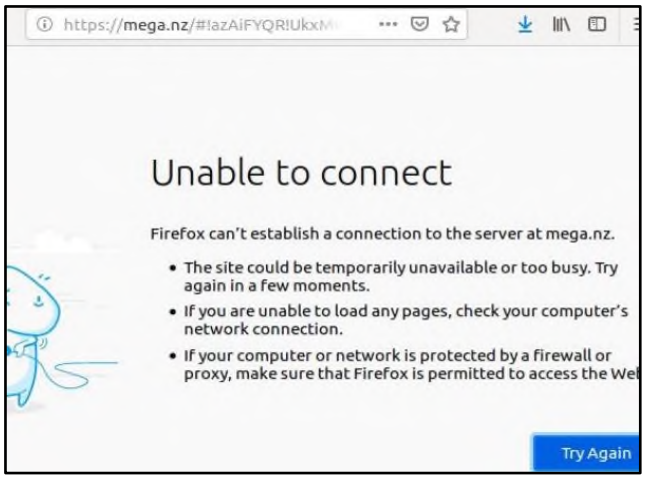


Ilustración 66 Bloqueo Megafire

POLÍTICAS DE SEGURIDAD PROPUESTAS

El propósito de generar la identificación de las acciones, procedimientos y eventualidades que contribuyen al aumento del riesgo frente a la seguridad de la información, se realizó un análisis de la forma de trabajo del ayuntamiento de Teteles de Ávila Castillo y la utilidad que se le dan a los recursos informáticos en las instalaciones de dicha institución, donde se permite identificar los siguientes puntos que deben aplicarse para la seguridad de los recursos tecnológicos:

- ➢ Evitar dejar los equipos de cómputo encendidos en horas no laborales.

- ➢ No permitir el ingreso a personal ajeno al ayuntamiento a las zonas restringidas donde se maneje información sensible.

- ➢ Clasificar la información de acuerdo a su importancia, sensibilidad o nivel de privacidad.

- Contar con sitios especiales para el almacenamiento de información con altos niveles de seguridad física que restrinjan el acceso a estos datos.

- Evitar la instalación de software en los equipos de cómputo que pueda atentar contra los derechos de autor o propiedad intelectual, así como la integridad e información del mismo.

- No guardar o almacenar información ajena al ayuntamiento que tenga alguna restricción para su revisión

- Evitar la conexión de equipos de cómputo portátiles u otros dispositivos electrónicos personales a la red de datos que no pertenezcan al ayuntamiento.

- Privacidad de la información a personas o entidades no autorizadas.

- No otorgar privilegios de acceso a los activos de información a terceras personas no autorizadas o ajenas a la institución.

- Evitar el consumo de alimentos y bebidas en áreas donde se encuentren los recursos informáticos.

- Restringir el acceso a sitios o páginas web que puedan perjudicar a los dispositivos por medio de descargas e instalaciones de software en segundo plano para evitar virus informáticos

Políticas Generales

De la misma manera se deben generar políticas de seguridad física en las instalaciones.

- Será responsabilidad del personal encargado o designado de la seguridad de la información y del personal con acceso a la misma, de manera que se garantice que los controles de seguridad físicos permanezcan cerrados para evitar el acceso a la información por parte de personal no autorizado.

- El área asignada para el almacenamiento de la información, la ubicación del servidor y el sistema de seguridad perimetral se resguardarán, solo ingresara el personal autorizado.

- Monitorear las condiciones tales como la temperatura y humedad, que pueda afectar el correcto funcionamiento del servidor o los equipos de cómputo.

- Es responsabilidad de los usuarios acatar las normas de seguridad y mecanismos de control de acceso del ayuntamiento.

- Los equipos de cómputo que forman parte de la infraestructura tecnológica del ayuntamiento deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daños, robo o acceso de terceras personas.

- Se busca que el ayuntamiento adopte los controles necesarios para mantener a los equipos alejados de sitios que pongan en riesgo de amenazas como fuego, agua, polvo, vibración, entre otros.

- ➢ Los usuarios tendrán la responsabilidad de dar un uso adecuado a los equipos de cómputo que tengan asignados, es fundamental que estos recursos no estén a disposición de terceras personas no autorizadas por el ayuntamiento.

- ➢ Es fundamental e importante realizar mantenimientos preventivos y correctivos constantemente, que conlleva a cada uno de los recursos informáticos, tomando en cuenta la vida útil de los mismos y si es necesario renovar estos equipos para evitar inconvenientes en los procesos y actividades administrativas a futuro.

Políticas de acceso a la red.

Los equipos de cómputo que se conecten a la red del ayuntamiento deberán ser previamente autorizados por el personal encargado de los sistemas de información, el cual debe realizar una validación previa de las condiciones de seguridad.

- ➢ Esto incluye a equipos móviles como celulares y tablets, equipos de terceros que de igual modo deberán ser autorizados para conectarse a la red de datos.

- ➢ Solo se dará acceso a personal del ayuntamiento que requieran hacer uso de la información y/o aplicaciones en Internet para llevar a cabo sus actividades diarias.

- ➢ El acceso a sitios de Internet no permitidos es responsabilidad del usuario, es solo para uso laboral, considerando las restricciones de la Política de Navegación en Internet.
- ➢ Generar perfiles para cada usuario dependiendo al entorno en que aplican sus actividades diarias.

- ➢ Revisar los accesos y permisos en un plazo determinado, después de cambios mayores o cuando se produzca un incidente referente a la seguridad de la información.
- ➢ Revisar el cableado cada 6 o 12 meses para identificar si existe algún deterioro en las conexiones de red.

Políticas de Seguridad Lógica

Una de las herramientas de trabajo más necesarias hoy en día es el Internet que como se sabe permite un intercambio de información para las distintas actividades laborales y sociales, sin embargo, debe existir un uso adecuado de este servicio, tener un control, que sea verificado y monitoreado, todo esto para generar un aprovechamiento positivo del recurso que va orientado a las diversas actividades y procesos, evitando el ingreso a sitios web explícitos, que no aportan una correcta información o peor aún que implique un delito informático que afecte a la información de los usuarios.

Utilización de otros servicios que estén disponibles a través de Internet que conlleven a establecer conexiones o intercambios no autorizados por el área correspondiente de la seguridad de la información.

La publicación o envío de información confidencial sin la aplicación previa de los controles para salvaguardar la información y sin la previa autorización del personal correspondiente.

Promover o mantener asuntos o negocios externos a la institución.

La descarga, instalación y utilización de software(programas) de aplicación no relacionados con la actividad laboral y que esto afecte los procesos administrativos o de la red de datos.

Navegar en redes sociales en horas laborales, sin el permiso de los jefes de áreas o responsable del área de seguridad de los datos.

Hacer uso de herramientas de mensajería instantánea no autorizadas por el área responsable de las tecnologías de la información.

Impacto

Existe una gran variedad de los beneficios y cambios que aportarán un impacto en cada una de las áreas del ayuntamiento de Teteles de Ávila Castillo, para ello deben ser puesto en marcha las siguientes recomendaciones mencionadas a continuación, que bien son parte fundamental en el ciclo de vida del sistema de seguridad perimetral diseñado.

Será permitido el uso de internet dentro de las restricciones anteriores podrá ser permitido siempre y cuando se utilice de manera ética, razonable, responsable y sin dañar o afectar las actividades no la protección de la información.

Por otro lado, los usuarios de la red inalámbrica deberán ser sometidos a las mismas condiciones de seguridad que las redes cableadas, comenzando por la identificación, autenticación, el control de contenido de Internet, cifrado, etc.

Se realizará un monitoreo constante de los tiempos de navegación y páginas web visitadas por los usuarios que estén autorizados por medio del firewall diseñado. Una ventaja será el bloqueo de conexiones a sitios web no autorizados. A su vez, inspeccionar, registrar e informar de las actividades realizadas durante la navegación.

Se recomienda contar con personal encargado del área de servicios de información para que sea el responsable de validar a quien se le pueden asignar los servicios a través de la red de datos.

Un tema importante es, la asignación de cada uno de los recursos informáticos serán herramientas de trabajo sólo para uso exclusivo de los empleados. Sujetado a las siguientes políticas:

- Los usuarios no deben realizar cambios físicos en los equipos de cómputo, es decir, cambio de ubicación, mantenimientos, modificaciones en su configuración física. esto solo podrá ser realizado por el personal autorizado.
- Solo el personal encargado del área de servicios de información será el responsable de validar la asignación de los servicios a través de redes inalámbricas.

- Es importante que los equipos de cómputo sean suspendidos, apagados o bloqueen la sesión, por sus usuarios, esto cada vez que se retiren de su área de trabajo.

- ➢ Está restringido dejar configuraciones y contraseñas por defecto en los equipos inalámbricos.

- ➢ La instalación de cualquier tipo de software en los equipos de cómputo es responsabilidad del personal encargado de los sistemas de información.

- ➢ Los recursos tecnológicos asignados a los empleados deben ser devueltos al personal asignado de los sistemas de información una vez sean reemplazados por nuevos o cuando el contratista responsable de dicho recurso finalice su vinculación con el ayuntamiento.

Acerca de la protección contra software malicioso se plantea lo siguiente:

- ➢ Cada una de las herramientas y otros mecanismos de seguridad implementados no deberán ser deshabilitados o desinstalados sin previa autorización.

- ➢ Se recomienda realizar cada año un estudio de mercado de las herramientas de software para la prevención de software malicioso que cumpla con las necesidades y costos y otorgue beneficios, con ello, ser instalados en los equipos de cómputo que lo requieran.

- ➢ Está prohibido generar, escribir, escribir, copiar, ejecutar o intentar ingresar cualquier tipo de código de programación diseñado para replicarse, dañar o afectar el desempeño de cualquier equipo o la red de datos.

- ➢ Los equipos de cómputo y la infraestructura de red, comunicación y de seguridad de la información deben ser protegidos mediante herramientas y software de seguridad que apoyen a la prevención del ingreso de código malicioso a la red interna, así como mecanismos para detectar, prevenir y recuperar información.

- ➢ Cada uno de los medios de almacenamiento que se conecten a los equipos de cómputo del ayuntamiento deberán ser escaneados en búsqueda de código malicioso o cualquier elemento que pudiera afectar la seguridad de la información.

- ➢ Los sistemas, equipos e información del ayuntamiento deberán ser revisados periódicamente para verificar que no exista presencia de código malicioso.

Ahora referente a la recuperación y restauración de la información, se plantean las siguientes políticas.

- ➢ Se debe establecer un plan de restauración de copias de seguridad y que este sea probado por intervalos para asegurar que son confiables para casos de emergencia.

- ➢ Las copias de seguridad deben ser responsabilidad del personal encargado de la seguridad de la información.

- ➢ Se recomienda que la información de las copias de seguridad sea almacenada en sitios físicos diferentes donde se encuentran los sistemas de información, que apoye a mitigar el riesgo de pérdida de información en caso de que hubiera un desastre en las instalaciones del ayuntamiento.
- ➢ Es responsabilidad de cada usuario la seguridad que de la información que manipule, en caso de cambio de equipo el empleado será el responsable de realizar la respectiva copia de seguridad de la información que necesita.

Finalmente, se dan a conocer las siguientes políticas para la gestión de vulnerabilidades técnicas.

- ➢ El área encargada de los sistemas de información y de la seguridad de la misma es la responsable de proponer y ejecutar programas de evaluación y gestión de vulnerabilidades que deben ser parte del firewall perimetral del ayuntamiento.

- ➢ El mismo personal llevará la identificación de vulnerabilidades técnicas de las diversas plataformas tecnológicas y para esto se deben definir las herramientas y servicios necesarios para su implementación.

4.2 Conclusión

En conjunto con los procesos de detección, prevención y mitigación de riesgos constituyen estrategias fundamentales y prioritarias que están orientadas a dar a conocer las fortalezas y debilidades de una institución en cuanto a los distintos aspectos de seguridad, y que a partir de ellos se pueden desplegar un conjunto de medidas de control para la protección de activos, en este caso del ayuntamiento de Teteles.

Con el diseño de un UTM basado en Smoothwall en la seguridad perimetral de la red, da paso a poder monitorear y crear reportes de casos que se presenten al momento, en cuanto a las incidencias que afecten la seguridad de la información, con ello, lograr generar alertas y sus respectivos bloqueos de acceso. Sin embargo, otro de los eslabones débiles en la infraestructura de telecomunicaciones dentro de las instalaciones del Palacio Municipal de Teteles de Ávila Castillo, Puebla, es carecer de una red cableada, basada en los estándares de cableado estructurado, por lo que se recomienda considerar el diseño, planeación e implementación de la misma; ya que la instalación del servidor UTM para la seguridad perimetral de la red, tendrá mejor rendimiento y mayor garantía y fiabilidad, implementado en una red cableada y no sobre la red inalámbrica que actualmente está en uso.

El monitoreo del Firewall permite identificar la navegación de sitios por usuario, esto puede permitir la realización de auditorías y los correspondientes seguimientos a la red.

Los cuestionarios realizados a los usuarios, permitió obtener un panorama más amplio de la situación actual del ayuntamiento en cuestión a la seguridad de la información, esto dio paso al análisis de los resultados obtenidos y que fue de ayuda para el seguimiento del presente proyecto.

El manejo de la información por roles y perfiles de acceso, y asegurar que dichas aplicaciones que se manejan en el ayuntamiento, brindarán un control más amplio en el uso diario de la información, y los usuarios tendrán la capacidad de encontrar cualquier brecha adicional relacionada con la seguridad de los datos.

El presente trabajo de tesis tuvo la necesidad de aportar nuevas técnicas y políticas de seguridad en el ayuntamiento de Teteles de Ávila castillo, que a su vez tiene la necesidad de adquirir un sistema robusto que apoye en la seguridad de la información, de la mejora de su infraestructura de red de datos y el conocimiento necesario para una correcta manipulación de los recursos tecnológicos. A partir de ello, se definieron los controles y tratamientos adecuados con el objetivo de reducir, eliminar, actualizar, aceptar o en su caso mitigar a fin de garantizar la correcta continuidad operativa y crear un nivel de protección óptimo en esta institución de gobierno.

Referencias

Al-Shaer, E., & Hamed, H. (12 de February de 2014). Design and implementation of firewall policy advisor tools. *Multimedia Networking Research Laboratory*. Recuperado el 2021, de https://www.researchgate.net/publication/228903389

Corrales Hermoso, A. L., Beltrán Pardo, M., & Guzmán Sacristán, A. (2006). *Diseño e implantación de arquitecturas informáticas seguras.* Madrid: DYKINSON. Recuperado el 2020, de https://books.google.com.mx/books?id=dV23xCtqUPAC&printsec=frontcover&dq=firewall+perimetral&hl=es-419&sa=X&ved=2ahUKEwj8vfrIhursAhURS60KHXNOBOk4ChDoATAGegQIBxAC#v=onepage&q=firewall%20perimetral&f=true

Corrales Hermoso, A. L., Beltrán Pardo, M., & Guzmán Sacristán, A. (2006). *Diseño e implantación de arquitecturas informáticas seguras. Una aproximación Práctica.* Madrid: DYKINSON. Recuperado el 2020, de https://books.google.com.mx/books?id=dV23xCtqUPAC&printsec=frontcover&dq=firewall+perimetral&hl=es-419&sa=X&ved=2ahUKEwj8vfrIhursAhURS60KHXNOBOk4ChDoATAGegQIBxAC#v=onepage&q=firewall%20perimetral&f=true

Costas Santos, J. (2006). *Seguridad y Alta Disponibilidad (GRADO SUPERIOR).* Madrid, España: RA-MA . Recuperado el 2021, de https://books.google.com.mx/books?id=QI-fDwAAQBAJ&hl=es&source=gbs_navlinks_s

de Albuquerque Junior, A., & Marques dos Santos, E. (mayo-agosto de 2015). ADOPTION OF INFORMATION SECURITY MEASURES IN PUBLIC RESEARCH IN PUBLIC RESEARCH INSTITUTES. *JISTEM: Journal of Information Systems and Technology Management, 12*(2), 289-315. Recuperado el 2020, de http://www.redalyc.org/articulo.oa?id=203242219006

Dussan Clavijo, C. A. (2006). Políticas de seguridad informática. *Redalyc*(2), 86-92. Recuperado el 2020, de https://www.redalyc.org/articulo.oa?id=265420388008

Expertos, E. d. (21 de 03 de 2018). *Universidad Internacional de Valencia*. Recuperado el 2020, de viu: https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/

Fuertes , W., Rodas, F., & Toscano, D. (julio-diciembre de 2011). Evaluación de ataques UDP Flood utilizando escenarios virtualescomo plataforma. *Facultad de Ingeniería, 20*(31), 37-53. Recuperado el 2020, de http://www.redalyc.org/articulo.oa?id=413940770004

García Moran, J. P., Fernández Hansen, Y., Martínez Sánchez, R., Ochoa Martín, R., & Ramos Varón, A. A. (2011). *Hacking y Seguridad en Internet.* Madrid: RA-MA. Recuperado el 2020, de https://books.google.com.mx/books?id=SI2fDwAAQBAJ&printsec=frontcover&dq=firewall

+perimetral&hl=es-419&sa=X&ved=2ahUKEwil3KX2-unsAhXEAZ0JHTOiAt0Q6AEwCXoECAkQAg#v=onepage&q=firewall%20perimetral&f=true

Hernández Valverde, E. (2004). *Universidad Nacional Autónoma de México.* Recuperado el 2020, de TESIUNAM Digital: http://132.248.9.195/ppt2004/0332340/Index.html

Hurtado Sandoval, M. E., & Mendaño Mendaño, L. (15 de nov de 2016). *Repositorio Digital.* (2. Quito, Ed.) Recuperado el 28 de enero de 2020, de EPN: http://bibdigital.epn.edu.ec/handle/15000/16836

iso27000. (2005). *ISO 27000.ES*. Recuperado el 2020, de ISO IEC 27000: https://www.iso27000.es/sgsi.html

Iván Darío Toro Jaramillo, R. D. (2006). *Método y conocimiento: metodología de la investigación : investigación cualitativa/investigación cuantitativa.* Medellin, Colombia : Universidad Eafit.

Javier Solarte, F. N., Enriquez Rosero, E. R., & Benavides Ruano, M. d. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica ESPOL, 28*(5), 492- 506. Recuperado el 2020, de http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456

Keymur Landeros, H. (2014). *http://132.248.9.195/ptd2014/noviembre/0722065/Index.html.* Recuperado el 2020, de TESIUNAM Digital: http://132.248.9.195/ptd2014/noviembre/0722065/Index.html

Martínez Molina, K. J., Pacheco Meneses, J., & Zuñiga Silgado, I. (julio-diciembre de 2009). Firewall – Linux: Una Solución De Seguridad Informática Para Pymes (Pequeñas Y. *Revista UIS Ingenierías, 8*(2), 155-165. Recuperado el 2020, de http://www.redalyc.org/articulo.oa?id=553756879003

Mendeño Mendeño, L. A., & Hurtado Sandoval, M. E. (noviembre de 2016). *Implementación de ténicas de hacking ético para el descubrimiento y evaluación de vulnerabilidades de la red de una cartera de estado.* Recuperado el 2020, de Implementación de ténicas de hacking ético para el descubrimiento y evaluación de vulnerabilidades de la red de una cartera de estado: https://bibdigital.epn.edu.ec/handle/15000/16836

Navarrete Macías, J. A. (Enero de 2010). *Universidad Autónoma de México.* Recuperado el 2020, de TESIUNAM Digital: http://132.248.9.195/ptd2010/febrero/0654199/Index.html

pfSense. (2020). *pfSense*. Recuperado el 2020, de OPEN SOURCE SECURITY: https://www.pfsense.org

Proaño Escalante, R. A., & Gavilanes Molina, A. F. (marzo de 2018). Estrategia para responder a incidentes de inseguridad informática ambientado en la legalidad ecuatoriana. *Scielo, 9*, 90-101. Recuperado el 2020, de http://dx.doi.org/10.29019/enfoqueute.v9n1.229.

Ramírez Luna, H. E., & Mejia Miranda, J. (febrero de 2015). Propuesta de infraestructura técnica de seguridad para un Equipo de Respuesta ante incidentes de seguridad (CSIRT). *Revista electrónica de computación, informática Biomédica y electrónica, 4*(1). Recuperado el 2020, de http://www.redalyc.org/articulo.oa?id=512251501006

RAULT, R., SCHALKWIJK, L., AGÉ, M., CROCFER, N., CROCFER, R., DUMAS, D., . . . LASSON, S. (2015). *Seguridad informática - Hacking Ético: Conocer el ataque para una mejor defensa.* ENI. Recuperado el 2020, de https://books.google.com.mx/books?id=4X32wbgtNfUC&printsec=frontcover&dq=firewall+perimetral&hl=es-419&sa=X&ved=2ahUKEwir5_rYhursAhVJXq0KHaO_COE4FBDoATABegQIBhAC#v=onepage&q&f=false

Raya Cabrera, J. L. (2014). *Domine Microsoft Windows Server 2012.* España: RA-MA, S.A. Recuperado el 2020, de https://books.google.com.mx/books?id=to2fDwAAQBAJ&pg=PA409&dq=firewall+perimetral&hl=es-419&sa=X&ved=2ahUKEwil3KX2-unsAhXEAZ0JHTOiAt0Q6AEwAnoECAYQAg#v=onepage&q&f=true

Revelo Gordón, D. S., & Pacheco Villamar, R. (mayo de 2018). Análisis de Estrategias de Gestión de Seguridad Informática con Base. *Revista electrónica de Computación, Informática,, 7*(1), 1-21. Recuperado el 2020, de http://www.redalyc.org/articulo.oa?id=512255650001

Robayo López, J. H., & Rodríguez Rodríguez, R. M. (2015). *ASEGURAMIENTO DE LOS SISTEMAS COMPUTACIONALES DE LA EMPRESA SITIOSDIMA.NET.* Tesis, UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD, ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA, Bogotá. Recuperado el 2020, de https://repository.unad.edu.co/bitstream/handle/10596/3818/79626344.pdf?sequence=5&isAllowed=y

Ushmani, A. (6 de november-december de 2018). Ethical Hacking. *International Journal of Information Technology (IJIT), Issue*(4). Recuperado el 2020, de https://www.researchgate.net/publication/331481853

Zapata Molina, L. P. (julio-diciembre de 2012). Evaluación y mitigación de ataques reales a redes IP utilizando tecnologías de. *Ingenius. Revista de Ciencia y Tecnología*(8), 11-19. Recuperado el 2021, de http://www.redalyc.org/articulo.oa?id=505554812002