

Diseño de seguridad perimetral: Infraestructura de Red del Ayuntamiento Municipal de Teteles de Ávila Castillo

Designing perimeter security for the network infrastructure of the Municipal Council of Teteles de Ávila Castillo

Adriana Pérez-López^{1*}, Héctor Vicenteño-Rivera², Marco Antonio Aguilar-Cortés³, María Elisa Mariano-Ramos⁴

1 Instituto Tecnológico Superior de Teziutlán

2 Instituto Tecnológico Superior de Teziutlán

3 Instituto Tecnológico Superior de Teziutlán

4 Profesionalista independiente.

***Corresponding author:** adriana.pl@teziutlan.tecnm.mx

Resumen

El presente trabajo presenta el diseño a medida de un sistema de seguridad perimetral para la infraestructura de telecomunicaciones del H. Ayuntamiento Municipal de Teteles de Ávila Castillo, Puebla; el cual busca disminuir los riesgos a los que están expuestos los sistemas de información que manejan a través del uso de la red. Si bien, la estrategia del gobierno digital tiene como objetivo aprovechar al máximo el uso de las TIC (Tecnologías de la Información y comunicación) en el funcionamiento de las dependencias y entidades en la Administración Pública, para así agilizar los trámites que realizan los ciudadanos; no se han destinados los suficientes recursos económicos al tema de la seguridad, por considerarlo un programa secundario. Por lo anterior, la propuesta dentro de este trabajo, se enfoca al uso de herramientas de software libre para la implementación de un esquema de seguridad robusto que apoye la información del gobierno y los ciudadanos.

Palabras clave: seguridad, redes, software libre, gobierno.

Abstract

This work presents the custom design of a perimeter security system for the telecommunications infrastructure of the H. Municipal Council of Teteles de Ávila Castillo, Puebla; which seeks to reduce the risks to which the information systems managed through the use of the network are exposed. Although, the digital government strategy aims to make the most of the use of ICT (Information and communication technologies) in the operation of agencies and entities in the Public Administration, in order to streamline the procedures carried out by citizens; Not enough financial resources have been allocated to the issue of security, as it is considered a secondary program. Therefore, the proposal within this work focuses on the use of free software tools for the implementation of a robust security scheme that supports the information of the government and citizens.

Keywords: security, networks, open source, government.

1. Introducción

En la actualidad, el uso de técnicas, tecnologías, recursos y sistemas de información para llevar a cabo de manera eficaz y eficiente las tareas gubernamentales, se han convertido en una necesidad básica y con estricto apego a la confidencialidad de la información, de y para la sociedad. La modernización y transformación de las TIC impelen a una mejora continua de los servicios que el gobierno provee, misma mejora que debe poner en primer plano a la seguridad de la información.

Zúñiga et al., 2015 mencionan que el gobierno electrónico (e-gobierno) es una nueva forma de gobierno que utiliza las TIC con modalidades para la gestión, planificación y administración, por medio de portales en Internet con información referente a las dependencias de la administración pública, órganos de gobierno, poderes, legislación de los tres niveles de gobierno, así como servicios y trámites para permitir a la sociedad lograr un mayor contacto con la administración pública. Con esto, el gobierno pretende acercarse más a los ciudadanos aprovechando el impulso dado internacionalmente a las tecnologías de la información y comunicación. Con ello, la brecha digital ha brindado accesibilidad al gobierno electrónico en su gestión misma.

Gobierno electrónico: son todas las actividades apoyadas en las tecnologías informáticas, en específico la Internet, que los Gobiernos desarrollan para acrecentar la eficiencia de los servicios públicos y con ello mejorar las acciones del gobierno a los ciudadanos, en un marco más transparente

El Gobierno Digital promueve el uso intensivo de sistemas digitales en especial de Internet mediante siete líneas de acción:

1. Instalación y aprovechamiento de Infraestructura tecnológica gubernamental.
2. Promoción y aplicación de la administración del conocimiento y la colaboración digital.
3. Mejora y rediseño de procesos con tecnologías de información.

4. Mayor cobertura de los servicios y trámites electrónicos (e-Servicios) del Gobierno Federal.

5. Consolidación del Portal Ciudadano del Gobierno Federal.

6. Ampliación de mecanismos como e-Democracia y participación ciudadana.

7. Promoción de políticas de información, comunicaciones y organización para el Gobierno Digital (Gobierno Digital, 2015)

El gobierno electrónico ha revolucionado la forma de entregar servicios y mejorar las relaciones con los ciudadanos como empresas y empleados, logrando ser visto a través de cuatro tipos de relaciones:

G2C: Gobierno a Ciudadano (Government to Citizen)

G2B: Gobierno a Empresa (Government to Business)

G2E: Gobierno a Empleado (Government to Employee)

G2G: Gobierno a Gobierno (Government to Government)

Durante 2014, las administraciones públicas municipales y delegacionales atendieron distintos tipos de trámites solicitados por los ciudadanos. De los 15 trámites más atendidos (de un listado de 24 trámites seleccionados) se puede ver que, mayoritariamente, 35,045,602 trámites correspondieron al pago de derechos por suministro de agua potable; el segundo trámite atendido con mayor frecuencia fue el pago de impuesto predial, con 19,321,627 casos; en tercer lugar se ubicaron las copias certificadas de actas del registro civil, con 6,447,167 trámites; en cuarto lugar se situó el trámite por consulta médica con 4,218,378 solicitudes; y en quinto lugar el pago de infracción de tránsito con 2,721,316 acciones. (egob, 2021)

Ante los retos impuestos por la pandemia de COVID 19, sus consecuencias y las nuevas normalidades que se avecinan, los municipios en México deberán implementar estrategias innovadoras de gobierno electrónico para acercar al ciudadano los servicios públicos municipales y asegurar que sus gestiones sean exitosas, contribuyendo con el desarrollo sostenible y el bienestar de la población.

En el año 2020, México concentró el 34% en intentos de ciberataques en América Latina, representadas por 14 billones de amenazas, según lo reportado por la firma de ciberseguridad Fortinet; dicha empresa comentó que la pandemia por SARS-Cov-2 fue el pretexto ideal para abrir la llave a los hackers a empresas y dependencias públicas. Las empresas de gobierno conforman el 42% de organizaciones que están dispuestas a pagar rescates a los hackers por recuperar su información. (Gutiérrez, 2021)

Los gobiernos municipales están sujetos a recursos económicos que son recibidos a través de lo que se conoce como “participaciones” y con la captación de ingresos propios, mediante el cobro de diversos impuestos; dichos recursos son utilizados para la realización de proyectos que produzcan mayores beneficios a la población, descuidando la seguridad en las áreas tecnológicas que son el eje principal para la realización de todas las actividades; ello por no contar en su planeación con tácticas e inversión en la seguridad, no tener equipos de TI (Tecnologías de Información) y las herramientas especializadas para responder apropiadamente a cualquier tipo de incidente, de la misma forma en no poseer políticas de seguridad, entre las principales acciones a implementar. (Nordstern Techbologies, 2021)

Por lo anteriormente expuesto, se propone un esquema de seguridad perimetral para la infraestructura de red del H. Ayuntamiento de Teteles de Ávila Castillo, Puebla, que genere la protección informática que se requiere dentro del mismo; con el fin de establecer una línea de defensa (firewall) a través de herramientas basadas en software libre, capaces de proveer niveles altos de seguridad, comparados con herramientas propietarias de costos elevados. La gestión unificada de amenazas, es básicamente un cortafuegos de red que está integrado por varios servicios en un mismo equipo, para protección perimetral de una red de datos, a través de inspección de paquetes, redes privadas virtuales, antispam, antispymware y antiphishing, filtrado de contenidos, antivirus y detección y prevención de intrusos. (Root Solutions, 2017)

Un trabajo relacionado es el que llevó a cabo en el Ministerio del Poder Popular para la educación, en Venezuela, donde se diseñó un sistema de Seguridad para redes de datos, esto debido a la carencia de una seguridad de la información que

establezca las políticas, normas, procedimientos y la estructura organizacional adecuada; de modo que permitiera implementar métodos y mejores prácticas en TIC; logrando minimizar y erradicar varios de los problemas de seguridad originados por las amenazas y vulnerabilidades a las redes de datos de esa institución.

Otro trabajo similar 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.

La implementación de esquemas de seguridad perimetral basados en software libre ha permitido a usuarios finales el poseer mecanismos que protejan su infraestructura de TI. Al hacer uso de herramientas de software libre la adquisición de una licencia está cubierta esto en base a la GPL (General Public License) misma que permite el uso de forma libre para todos los usuarios de la aplicación o del software que cuente con este tipo de licencia, siendo el rubro financiero el principal obstáculo que en muchas ocasiones impide la implementación de este tipo de esquemas de seguridad.

Este tipo de solución no se limita a controlar el contenido que los usuarios consultan en internet (filtro de contenido), adicionalmente se puede hacer uso de:

- Control de ancho de banda
- Portal de autenticación
- Implementación de VPN (Virtual Private Network)
- Uso de VLANs (Virtual Local Area Network)
- Servidores DHCP (Dinamic Host Configuration Protocol)
- Reenvío de puertos

Se describen a continuación las etapas de la metodología llevada a cabo, que permitió identificar las necesidades de los usuarios de la infraestructura de red, lo que llevó a los resultados obtenidos, logrando el diseño lógico de un esquema de seguridad perimetral, que podría fortalecer las actividades tecnológicas de este y cualquier otro gobierno municipal, tomándolo como prototipo, por lo que el trabajo a futuro será la implementación el mismo en el H. Ayuntamiento citado.

2. Métodos o Metodología

La figura 1 presenta un esquema general de la metodología de trabajo para el desarrollo del presente proyecto, marcado en fases 4 diferentes fases.

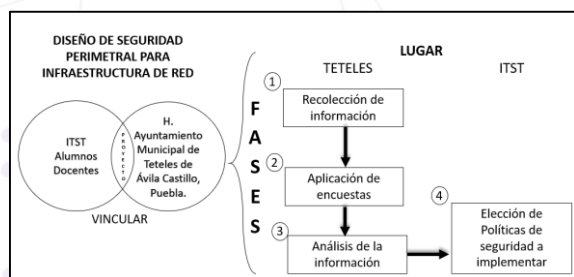


Figura 8. Metodología para el diseño de seguridad perimetral de la infraestructura de red

2.1.1 Vinculación

Para llevar a cabo la vinculación y poder iniciar los trabajos entre el Instituto Tecnológico y el Gobierno Municipal de Teteles de Ávila Castillo, se realiza la firma de un convenio que facilite el acceso a la información por ambas partes para que el proyecto propuesta sea lo más acertado y a la medida de las necesidades del organismo beneficiado y el correcto desempeño del recurso estudiantil participante.

2.1.2 Recolección de la información

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 mismas; de manera general y con información proporcionada por personal del Palacio Municipal, se tuvo información de los recursos informáticos que son parte de la organización. El primer dato de importancia es que la red que utilizan para los servicios de la organización y los personales, es inalámbrica.

La tabla 1 muestra un concentrado de los equipos tecnológicos dentro del Ayuntamiento, en lo que corresponde a las instalaciones del Palacio Municipal. Cabe destacar que los Smartphones, aunque son propiedad de cada empleado, se contabilizaron porque éstos hacen uso de la red de la organización.

Tabla 1. Lista de equipos tecnológicos

Recursos Informáticos activos en el H. Ayuntamiento de Teteles						
Área	Equipo	Marca	Tipo de red		Cantidad	Usuarios
			LAN	WAN		
Presidencia	Laptop			X	1	1
Secretaría	Módem	Telmex		X	1	
	Computador a de escritorio			X	1	1
	Impresora			X	1	
Juzgado	Módem	TP Link		X	1	
	Computador a de escritorio			X	2	10
Registro civil	Computador a de escritorio		X		1	1
Contraloría	Laptop			X	1	1
	Impresora		X		1	
Tesorería	All-in-one			X	1	1
	Laptop			X	2	2
	Copiadora		X		1	
	Impresora		X		2	
Regidurías	All-in-one			X	1	1
	Impresora			X	1	
Oficina de cultura	Computador a de escritorio			X	1	1
Obras públicas	Computador a de escritorio			X	2	2
	All-in-one			X	1	1
	Módem	TP Link			1	
	Impresora		X		1	
DIF	All-in-one			X	1	1
	Computador a de escritorio			X	1	1
	Laptop			X	1	1
	Copiadora		X		1	
	Módem	Telmex			1	
Total					29	25

Las áreas que se encuentran del Palacio Municipal, son en total 9, las que cuentan en su totalidad con 25 empleados, mismos que hacen uso de la red, así como de personal temporal (proveedores, prestantes de servicio social, residentes profesionales) tal como se clasifica en la Tabla 2.

Área	Usuarios de la Red por área
Presidencia Municipal	1
Secretaría del Ayuntamiento	1
Juzgado	10
Registro Civil	1
Contraloría	1
Tesorería	3
Obras Públicas	3
DIF	3
Regidurías	2
Total de usuarios	25

Tabla 2. Áreas y usuarios del H. Ayuntamiento

2.1.1 Aplicación de encuestas

Se realizó como herramienta de recolección de información, un cuestionario de 15 preguntas, para saber el grado de importancia que los usuarios le dan a las TIC, en cuanto a seguridad informática y red de datos, y el estado actual de su servicio de internet; el cual se aplicó mediante una encuesta apoyada de un formulario de Google.

Las preguntas de forma general iban enfocadas a 3 áreas:

- Conocimiento general acerca de los riesgos del mal uso de los equipos de cómputo, identificación de ataque por virus y plan de prevención de riesgos.
- Capacitación del personal en áreas de TIC.
- Desempeño del servicio de red e internet para realizar las actividades cotidianas.

2.1.4 Análisis de información

En el recorrido por las diferentes áreas del Palacio Municipal, se observó como primera necesidad la de realizar el diseño y la instalación de una LAN (Local Area Network) bajo los estándares de cableado estructurado, ya que el acceso a la red es en un 95% de forma inalámbrica, algunos de los usuarios comentaron acerca de las fallas de internet y que en ocasiones no se lograban realizar de manera eficiente los servicios que se otorgan a la ciudadanía. Además, se cuenta con acceso a internet para cualquier usuario que desee conectarse, aunque sea provisionalmente, sin modificar posteriormente las credenciales de acceso a la misma. Tampoco se tienen restricciones o alguna política de 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.

En cuanto a las respuestas obtenidas en la encuesta aplicada al personal usuarios de la red del Palacio Municipal, se identificó la siguiente información.

En las preguntas correspondientes al área de conocimiento general acerca del mal uso de los equipos, identificación de ataques y prevención de riesgos: el 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, tal como se refleja en la figura 2.

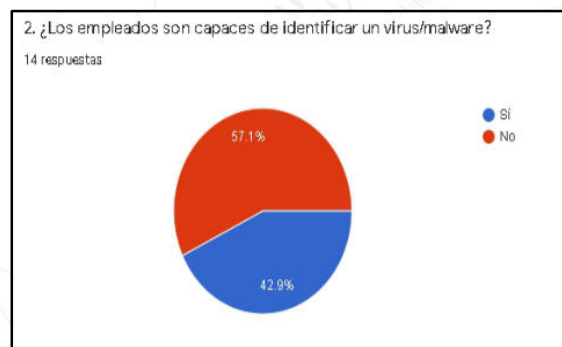


Figura 2. Identificación de virus

En la figura número 3, se aprecia que el 21.45% de los empleados desconoce los riesgos que se presentan debido a un mal uso de los equipos de cómputo.



Figura 3. Riesgos del mal uso de los equipos

En relación a la capacitación a los empleados en áreas de seguridad informática, el 50% de los usuarios mencionan que no cuentan con tal enseñanza que aporte conocimientos mínimos para la solución de un problema menor en materia de seguridad de los datos, ni en el uso de las TIC, reflejado en la figura 4.



Figura 4. Formación de prevención de riesgos informáticos

En relación a los resultados de la figura 4, se les preguntó a los empleados acerca de recibir capacitación, por parte del H. Ayuntamiento, para subsanar dicha carencia de conocimientos sobre seguridad informática básica y manejo adecuado de los equipos de cómputo, los resultados se pueden apreciar en la figura 5.



Figura 5. Cursos de seguridad informática

Sobre el desempeño de la red, el 69.2% de los empleados utilizan servicios de streaming, que se conforma de redes sociales, audio y video, lo cual es un motivo del bajo rendimiento que existe en la velocidad de internet y que afecta a otros usuarios en la realización de sus tareas administrativas, tal como se aprecia en la figura número 6.

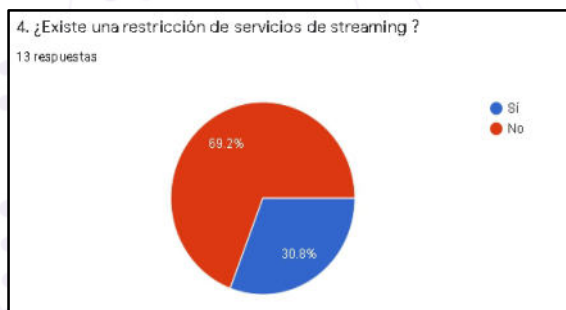


Figura 6. Servicios de streaming

En la figura 7 se observa que, con base en el porcentaje de usuarios en servicios de streaming, la valoración de los mismos hacia la calidad de internet que ofrece el ayuntamiento para sus funciones administrativas, es 7.1% en excelente y el mismo porcentaje en malo, el 42.9% lo evalúan en bueno y otro 42.9% regular.

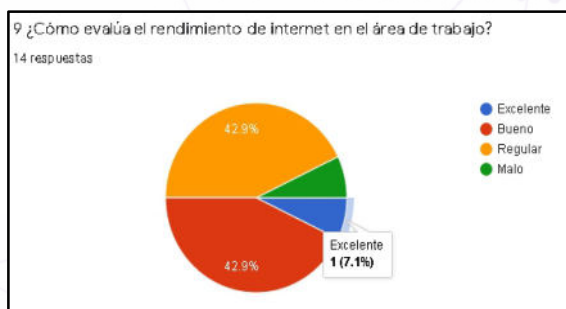


Figura 7. Rendimiento de Internet

Por otro lado, la figura 8, muestra que el 57.1% de los usuarios de la red e internet, afirma que no se tiene un programa formal que permita tener un control acerca del manejo seguro a los datos sensibles o confidenciales, por lo que se vuelve imprescindible controlar el flujo de datos y poner énfasis en la seguridad que debe tener cierta información confidencial.



Figura 8. Confidencialidad de los datos

2.1.2 Elección de políticas de seguridad a implementar

La administración de un firewall es la principal actividad que se realiza para asegurar el acceso a los servicios de la organización, es después del diseño lógico, la actividad que debe ser realizada de modo adaptativo, prácticamente representa la actividad que demanda de mayor tiempo en términos de seguimiento y mantenimiento con el objetivo de cumplir los lineamientos establecidos por el gobierno de TI, tomando como base lo anterior, se realizó el diseño lógico de la red de datos del H. Ayuntamiento de Teteles de Ávila Castillo, como se muestra en la figura 9, con un enfoque adaptable a los requerimientos futuros y que necesiten de ajustes en el esquema de seguridad implementado.

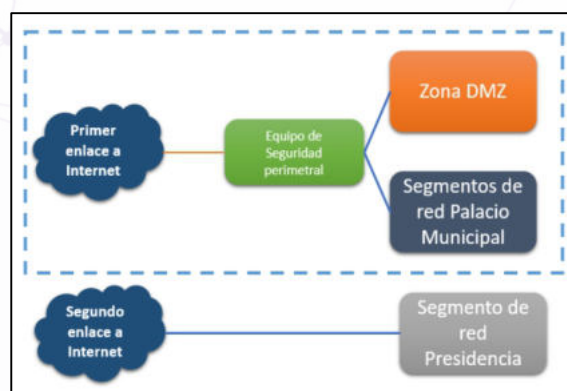


Figura 9. Diseño lógico de la red de datos

La seguridad de perímetro está evolucionando, como todos los demás aspectos de la seguridad de red en los tiempos modernos. Tradicionalmente, el perímetro de red se refiere a la infraestructura periférica que se ubica entre la red corporativa y la Internet pública, crea controles seguros para la información entrante y saliente que pasa entre ellas.

Las políticas o reglas representan un grupo de condiciones usadas para evaluar en forma significativa todas las conexiones de red y todas las acciones asignadas a dichas condiciones. Con las reglas de Firewall, se puede definir la acción a realizar cuando se establecen diferentes tipos de conexiones de red.

Las políticas o reglas las podemos dividir en 3 categorías principalmente:

- Tráfico de entrada (de internet a los equipos de cómputo)
- Tráfico de salida (de los equipos de cómputo a internet)
- Tráfico interno (de segmentos internos de red a segmentos internos de red)

Para el H. Ayuntamiento de Teteles se definieron las siguientes políticas de red, todas ellas con el objetivo mantener un control sobre los servicios que pueden utilizar los usuarios internos y establecer los servicios necesarios que pueden utilizar los usuarios externos, esto permite reducir los objetivos ante posibles ciberataques, así como reforzar la integridad de los datos, sobre la información que allí se maneja.

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 tabletas, 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.

En la Tabla 3 se hace alusión a la interface “Red” que se conecta a internet, donde se origina el tráfico y hacia la interface “Orange” que da acceso a la zona desmilitarizada, hacia las 3 redes internas, con los servicios o aplicaciones que ahí se enlistan.

No.	Interface origen	Dirección origen	Interface destino	Dirección destino	Aplicación o servicio	Acción
1	red	all	orange	100.100.100.0	dns, http, https	accept
2	red	all	green	192.168.15.0	all	drop
3	red	all	green	192.168.20.0	all	drop

Tabla 3. Políticas de entrada

La Tabla 4 es, por el contrario, la especificación del tráfico generado en el interior de la red, desde la zona desmilitarizada conectada a través de la interface “Orange” para el segmento de red 100.100.100.0 y hacia cualquier red “all” en internet. Además de las interfaces “green” que conectan las redes LAN.

No.	interface origen	Dirección origen	Interface destino	Dirección destino	Aplicación o servicio	Acción
1	orange	100.100.100.0	red	all	dns, http, https, imap, pop, pop3, smtp, smtps, ftp	accept
2	green	192.168.15.0	red	all	dns, http, https, imap, pop, pop3, smtp, smtps, ftp	accept
3	green	192.168.20.0	red	all	dns, http, https, imap, pop, pop3, smtp, smtps, ftp	accept

Tabla 4. Políticas de salida

Por último, la Tabla 5, da a conocer el tipo de política para el tráfico generado dentro de la misma red del Ayuntamiento, desde la zona desmilitarizada hacia las redes LAN y viceversa; con las interfaces previamente comentadas, hacia todos los servicios que administra la red y los servidores.

No.	Interface origen	Dirección origen	Interface destino	Dirección destino	Aplicación o servicio	Acción
1	orange	100.100.100.0	green	192.168.15.0	all	accept
2	orange	100.100.100.0	green	192.168.20.0	all	accept
3	green	192.168.15.0	green	192.168.20.0	all	accept
4	green	192.168.20.0	green	192.168.15.0	all	accept
5	green	192.168.15.0	orange	100.100.100.0	all	drop
6	green	192.168.20.0	orange	100.100.100.0	all	drop

3. Resultados

El esquema lógico de la red de datos del H. Ayuntamiento permite el establecimiento de reglas de firewall encaminadas a cumplir el objetivo planeado para asegurar el intercambio de datos tanto de dominio local, como en los temas relacionados al uso de internet.

La figura 10, muestra la configuración que permite acceder a servicio en internet mediante el uso de los principales puertos seguros, entre ellos, navegación por los protocolos HTTP (Hypertext Transfer Protocol), HTTPS (Hypertext Transfer Protocol Secure), y DNS (Domain Name Service), el pool de puertos se puede personalizar en relación a los requerimientos futuros de los usuarios de la red de datos.

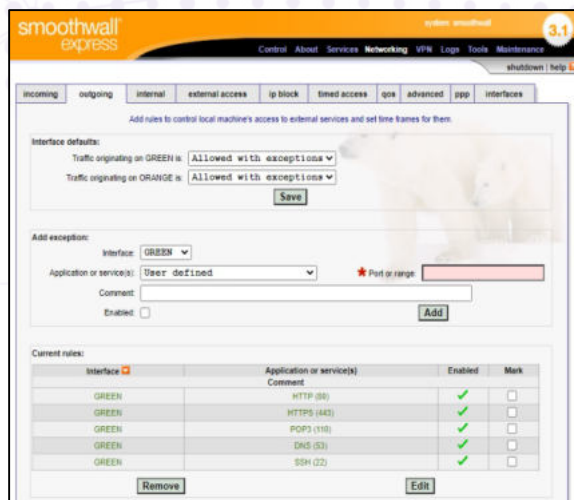


Figura 10. Políticas de tráfico saliente

Para garantizar que los recursos que se encuentran disponibles a los miembros de un mismo segmento de red, es necesario el establecimiento de reglas que permitan controlar es tipo de solicitudes, la figura 11 muestra la configuración donde se permite el intercambio de información entre los diferentes segmentos, pero, solo por puertos de comunicación en específico.

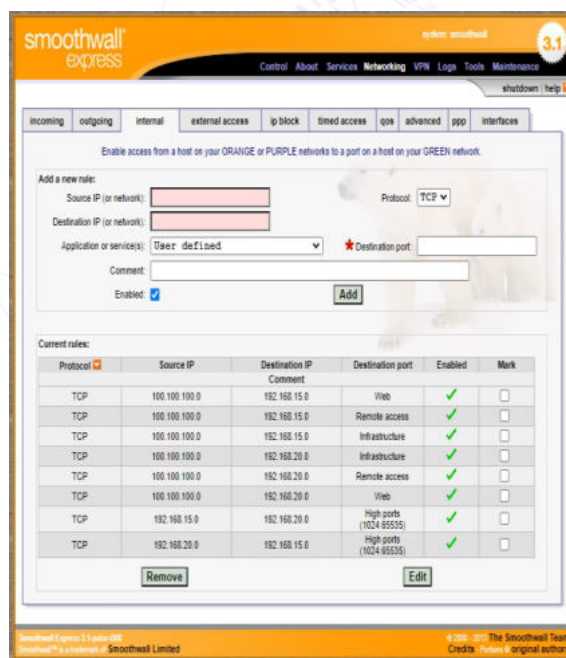


Figura 11. Políticas de tráfico local

Las figuras 12 y 13 muestran políticas de tráfico entrante, la 12, la configuración que permite el acceso remoto desde cualquier punto de internet al portal de administración de smoothwall (firewall), como en cualquier otro equipo de seguridad se recomienda que solo se permite la comunicación mediante el uso de los protocolos HTTPS (443), SSH (Secure Shell) (22) y el portal de administración (113). La figura 13 la configuración de la zona DMZ (Demilitarized Zone), es decir, la zona donde se ubican los equipos que brindan servicios de propósito específico, entre ellos, el sistema de cobro de impuesto por concepto de servicio de agua potable, para garantizar el uso adecuado de estos recursos solo se autoriza el uso de los mismos mediante el uso de protocolos seguros. (Smoothwall, 2016)

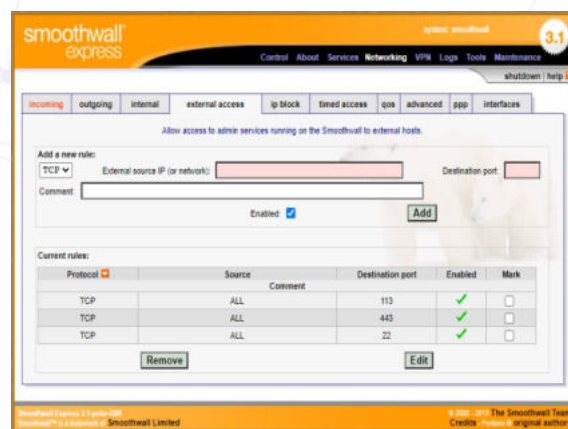


Figura 12. Políticas de tráfico entrante

5. Conclusiones

Con el diseño de un servidor de gestión unificada de amenazas basado en software libre, específicamente Smoothwall, que brinde seguridad perimetral de la red de datos, permitirá adicionalmente el monitorear y generar reportes que ayude la toma de decisión respecto a los servicios que son consumidos por los usuarios, en cuanto a las incidencias que afecten la seguridad de la información, se considera la generación de alertas y sus respectivos bloqueos de acceso. Además, de generar filtrado de contenidos no necesarios para mejorar el rendimiento de los servicios de internet y por ende, el servicio interno que se proporciona a la ciudadanía. 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 como el propuesto, tendrá mejor rendimiento y mayor garantía y fiabilidad, implementado en una red cableada y no sobre la red inalámbrica que actualmente está en uso.

6. Trabajo a futuro

Debido a que existe un convenio con el Ayuntamiento de Teteles, se ha presentado la propuesta del diseño de seguridad para su red de datos y se realizará la implementación de un servidor Smoothwall con las políticas de seguridad aquí planteadas, dicho proyecto será realizado por alumnos y docentes del Instituto Tecnológico Superior de Teziutlán, con la finalidad de fortalecer las áreas de oportunidad en materia de seguridad de los datos y la red detectadas en la inspección visual y en el resultado de las encuestas realizadas al personal de dicha institucional gubernamental; con la intención de conocer la factibilidad del mismo para ser un prototipo para otros ayuntamientos de la región.

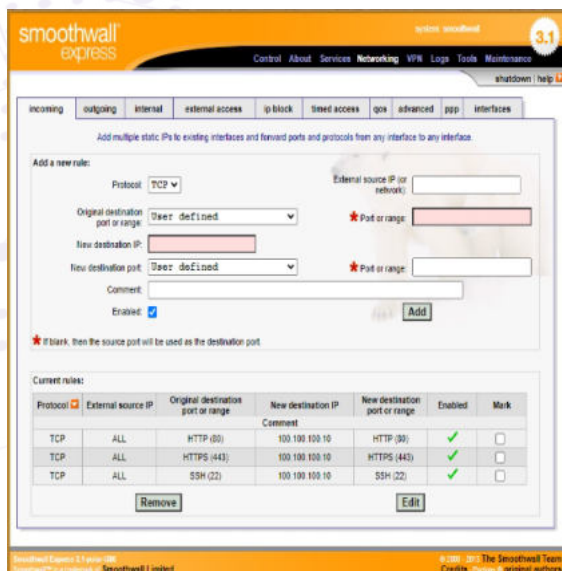


Figura 13. Políticas de tráfico entrante (portal de administración)

4. Discusión

Junto con los procesos de detección, prevención y mitigación de riesgos que 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, se logró identificar la necesidad de contar con una red de área local que sea implementada bajo los estándares de cableado estructurado, ya que la fortaleza de un servidor de seguridad, debe estar respaldado por una conectividad que garantice su disponibilidad y rendimiento, que no genere intermitencia de servicio, como lo hace constantemente la actual red inalámbrica, ya que si bien funciona para servicios básicos de atención a la ciudadanía, los servidores de seguridad que forman parte de este diseño, así como de otros, requieren de mayor desempeño en cuestiones de conectividad, que aseguren consistencia, aislamiento, accesibilidad, disponibilidad y durabilidad.

Referencias bibliográficas

E. (2021, 12 febrero). Gobierno electrónico en el ámbito municipal en México. egob. <https://egob.com/2021/02/12/gobierno-electronico-en-el-ambito-municipal-en-mexico-egob/>

Eset. (s.f.). Eset Internet Security. Recuperado el 08 de Agosto de 2021, de https://help.eset.com/eis/12/es-CL/idh_config_epfw_view_rule.html

Gobierno, B. (2005). 403 4.4 Gobierno Digital. 403–406. www.micasa.gob.mx.

Fortinet. (s.f.). Fortinet. Recuperado el 03 de Agosto de 2021, de <https://www.fortinet.com/lat/solutions/enterprise-midsize-business/network-security>

Gutiérrez, A. L. (29 de junio de 2021). EL FINANCIERO. Recuperado el 24 de julio de 2021, de <https://www.elfinanciero.com.mx/empresas/2021/06/29/acechan-hackers-a-empresas-mexico-concentra-el-34-de-ciberataques-de-al/>

Nordstern Techbologies. (12 de julio de 2021). Nordstern Techbologies. Recuperado el 25 de julio de 2021, de https://www.nordsterntech.com/webinar-ciberseguridad-pymes?fbclid=IwAR0w67hD_DE_L8TePociQ6YrFM8eukfWMosUuswthTNoLlCJM7eUyJ2SP6M

Root Solutions. (20 de julio de 2017). Root Solutions Consultoria IT & Seguridad de la Información. Recuperado el 25 de julio de 2021, de <https://www.rootsolutions.com.ar/tres-firewalls-utm-open-source-encuentra/>

Smoothwall. (22 de mayo de 2016). Smoothwall Org. Recuperado el 07 de Julio de 2021, de <https://my.smoothwall.org/cgi-bin/docs.cgi>

Zúñiga, R. P., & Hernández, E. M. (2016). Año 5, número 9, septiembre 2015-febrero de 2016.