

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL



Facultad de Ingeniería en Electricidad Y Computación

Maestría En Seguridad Informática Aplicada

“PROPUESTA DE REDISEÑO DE LA INFRAESTRUCTURA DE RED
PARA MEJORAR LA SEGURIDAD DE LOS DATOS
EN UNA EMPRESA PÚBLICA DE AGUA”

EXAMEN DE GRADO (COMPLEXIVO)

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

MAGÍSTER EN SEGURIDAD INFORMÁTICA APLICADA

HÉCTOR FABRICIO RAMOS MÉNDEZ

GUAYAQUIL – ECUADOR

AÑO 2016

AGRADECIMIENTO

Agradezco al Creador Nuestro Padre Dios por permitirme vivir y culminar con éxitos este proceso de Educación Superior.

A mi familia y amigos que me ayudaron mucho con sus consejos de superación y sobre todo el apoyo para lograr mi objetivo.

DEDICATORIA

Dedico este trabajo a mis Esposa Nohely Vera Balón, a mi Hija Samira Ramos Vera, a mis padres Méndez Ortega Ofelia y Ramos Guale Héctor, y a mi primo Cruz Méndez Carlos por su paciencia y por su apoyo incondicional para llegar a cumplir con esta meta educativa.

A mis familiares y amigos que estuvieron dispuestos a ayudarme en esta ardua tarea de lograr un título de maestría, permitiéndome responder a la sociedad como un buen elemento responsable de trabajo.

TRIBUNAL DE SUSTENTACIÓN

MGS. LENIN FREIRE COBO
PROFESOR DELEGADO
POR LA UNIDAD ACADÉMICA

ING. JUAN CARLOS GARCIA
PROFESOR DELEGADO
POR LA UNIDAD ACADÉMICA

RESUMEN

El objetivo principal de este trabajo, es hacer conocer a la empresa sobre los últimos modelos de seguridad en lo que respecta a infraestructura de red y que pueden ser aplicados en la misma.

El rediseño de la infraestructura de red, estará enfocados en el cumplimiento de las tres fases de la seguridad de la información como son: la integridad, disponibilidad y confidencialidad.

La utilización de equipos CISCO es esencial para el rediseño de la infraestructura de red de la empresa, debido a la variedad de servicios confiable que esta ofrece en comunicación y seguridad, además por ser una de las marcas más reconocida a nivel mundial.

El rediseño de la infraestructura de red, tendrá el análisis correspondiente con el personal de tecnología de la empresa. El objetivo de este análisis es verificar si se está cumpliendo con la mejoras de seguridad en la red de borde, red interna y perimetral para la empresa. Se concluye con un informe abstracto de las vulnerabilidades y las soluciones correspondiente en infraestructura.

ÍNDICE GENERAL

AGRADECIMIENTO	II
DEDICATORIA	III
TRIBUNAL DE SUSTENTACIÓN.....	IV
RESUMEN	V
ÍNDICE GENERAL.....	VI
ABREVIATURAS Y SIMBOLOGÍAS	VII
ÍNDICE DE FIGURAS	VIII
INTRODUCCIÓN	IX
1. GENERALIDADES.....	1
1.1. Descripción del problema.....	1
1.2. Solución de la propuesta.....	2
2. METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN	4
2.1. Análisis y Diseño de la red Interna Actual.....	4
2.2. Análisis y Diseño de la red Perimetral Actual	7
2.3. Análisis y Diseño de la red Externa Actual	8
2.4. Análisis de Dispositivos de Seguridad en la red Actual.	10
2.5. Análisis de Dispositivos CISCO a contemplar para el rediseño de la red... 11	
2.6. Propuesta del rediseño de la infraestructura de Red	13
3. ANÁLISIS DE RESULTADOS.....	24
3.1. Validación de la seguridad de la red de borde propuesto con el personal de infraestructura de la organización.....	24
3.2. Validación de la seguridad de la red interna propuesto con el personal de infraestructura de la organización.....	25
3.3. Validación de la seguridad de la red perimetral propuesto con el personal de infraestructura de la organización.....	27
3.4. Informe final del rediseño de la red Propuesta.....	28
CONCLUSIONES Y RECOMENDACIONES	30
BIBLIOGRAFÍA.....	32

ABREVIATURAS Y SIMBOLOGÍAS

ASA	Dispositivo de Seguridad adaptable
DHCP	Protocolo de comunicación dinámica de host
DMZ	Zona desmilitarizada
IDS	Sistema de detección de intruso
LAN	Red de área Local
SNMP	Protocolo simple de administración de red
SQUID	Servidor proxy para web
VACL	Lista de control de acceso VLAN
VLAN	Virtual LAN
VPN	Red Privada Virtual
WAN	Red de área amplia
WEB	World Wide Web (red informática mundial)

ÍNDICE DE FIGURAS

Figura 2.1 Diseño Físico de la red Interna Actual	5
Figura 2.2 Single-homed bastion host	5
Figura 2.3 Diagrama físico del sector de la Planta de Agua	6
Figura 2.4 Screened-subnet firewall system.....	8
Figura 2.5 Diagrama WAN de la Empresa.....	8
Figura 2.6 Diagrama de enlace Matriz- Planta de Agua	9
Figura 2.7 Modelo Jerárquico de una Red.....	14
Figura 2.8 Ambientes de la Red propuesta a analizar	15
Figura 2.9 Diagrama Lógico WAN propuesto	16
Figura 2.10 Diagrama Físico WAN propuesto.....	16
Figura 2.11 Diagrama Físico DMZ Propuesto	19
Figura 2.12 Diagrama Físico (Matriz) de la red Interna propuesto.....	21
Figura 2.13 Diagrama Físico (Planta de Agua) de la red Interna propuesto	23

INTRODUCCIÓN

La entidad Pública de agua, tiene objeto de dedicarse a la prestación de servicios públicos y, para llevar el control de sus operaciones técnicas y financieras hacen uso de tecnología de la información.

Una de las tecnologías de la información es el uso dispositivos de red que permite en flujo de datos y la centralización de la misma. Los datos de toda organización son de gran importancia por lo que requieren que siempre estén protegidas de personas no autorizadas.

En este proyecto, se analizara el tipo de arquitectura actual para la protección de los datos así como de los dispositivos utilizados en la misma. El propósito del análisis es para realizar un rediseño de mejoras, aplicando conocimientos de seguridad de redes.

El proceso de análisis se lo realizará en 3 ambientes de red como: ambiente de red externa, de red interna y red perimetral, de igual manera se dará a conocer las mejoras en cada una de ellas. Este proyecto concluirá con un informe general del rediseño propuesto así como también las conclusiones y recomendaciones.

CAPÍTULO

1. GENERALIDADES

1.1. Descripción del problema

La entidad Pública de agua, tiene objeto de dedicarse a la prestación de servicios públicos de alcantarillado sanitario, alcantarillado pluvial, tratamientos de aguas servidas y de agua potable. Dicha entidad, se encuentra distribuida en 2 sectores Matriz (Administración) y una sucursal (Tratado de Agua). Por los servicios antes mencionado, ocasiona que se generen otros servicios al usuario entre los más utilizados están: cobro de planillas de agua, solicitudes de medidores, pago de empleados, otros. En general, todas las actividades que lo ameritan, hacen uso de una infraestructura de red que permite acceder a los servidores para lectura y escritura de datos. Internamente, los servidores como la red interna, se encuentran protegidos de la red externa (Internet) por un sistema firewall y, el acceso de la red interna con los servidores es controlado por reglas en el mismo firewall, esto conlleva a tener un solo firewall de seguridad para toda

la infraestructura de red. La falla de este único sistema de protección, provocaría a que los servidores como la propia red interna queden expuestos a vulnerabilidades.

Otros de los problemas están relacionados con la utilización de equipos de conexión inalámbrica, en el caso de la Matriz, la existencia de una conexión inalámbrica sin brindar la seguridad a la red interna de la organización. En el caso de la sucursal, la existencia de problemas de conectividad recurrente entre áreas de trabajo.

Uno de los puntos de gran importancia tratados con la entidad, es que, en vista del crecimiento de la organización, necesitan tener una infraestructura de red que sea escalable, y sobre todo segura tanto en el perímetro, como el en borde empresarial. Se dio a conocer de igual manera, que su enlace entre los 2 sectores es a través de un solo medio y por un solo proveedor. Dado estas sugerencias para rediseñar la red, se puede deducir que la empresa no dispone en su infraestructura de red, escalabilidad, disponibilidad y sobre todo seguridad de red de borde y de red interna.

1.2. Solución de la propuesta

Debido a que la empresa pública de agua potable, maneja gran cantidad de información administrativa, operativa y financiera, deben contar con una infraestructura de red que brinde todas las fases de la seguridad de la información como lo son: integridad, disponibilidad y confidencialidad.

Es por ello que se desea realizar una propuesta de un nuevo rediseño de la infraestructura de red, que permita brindar todas las seguridades de datos, empezando por la seguridad de la red de borde, red perimetral y red Interna, considerando normas y estándares. Para efectos de la propuesta del rediseño en su infraestructura se utilizará equipos CISCO, especificando cada una de sus características y objetivos de su utilización.

Se analizará el tipo de medio eficaz de protección de un sistema local o en red (Firewall) utilizada en la organización, para proponer una mejora de la misma en caso de ser necesario.

Para la red Interna se considera una propuesta de implementar VLAN para mejorar la administración de red, separando segmentos lógicos de una red de área local.

Resumiendo con lo que se desea alcanzar con el rediseño de la infraestructura de red, podemos mencionar: seguridad de la red de borde, seguridad en la red interna, seguridad en la red perimetral, disponer de una red de alta disponibilidad, escalable, y mejorar su administración a través de VLAN.

CAPÍTULO

2. METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

2.1. Análisis y Diseño de la red Interna Actual

La entidad Pública de agua (Matriz), posee una infraestructura de red interna, que es funcional para los usuarios que laboran en ella, pero al mismo tiempo carecen de una seguridad hacia sus servidores. Entre los datos recopilados, se pudo conocer que disponían de 3 servidores de alta demanda. Para la seguridad en dos de los servidores (web y correo), realizan configuraciones a través de una aplicación proxy (SQUID) por cada servidor (web y correo).

En la figura 2.1 se visualiza que la arquitectura de red de la empresa, utiliza un tipo de configuración Screened host firewall system (single-homed bastion host), ya que consta de dos sistemas que son un enrutador de filtrado de paquete y Bastion Host. En enrutador de paquete, sólo los paquetes desde y hacia el Bastion Host se les permiten pasar a través del router. En el caso de

Bastion Host, realiza funciones de autenticación y de servidor proxy (Figura 2.2).

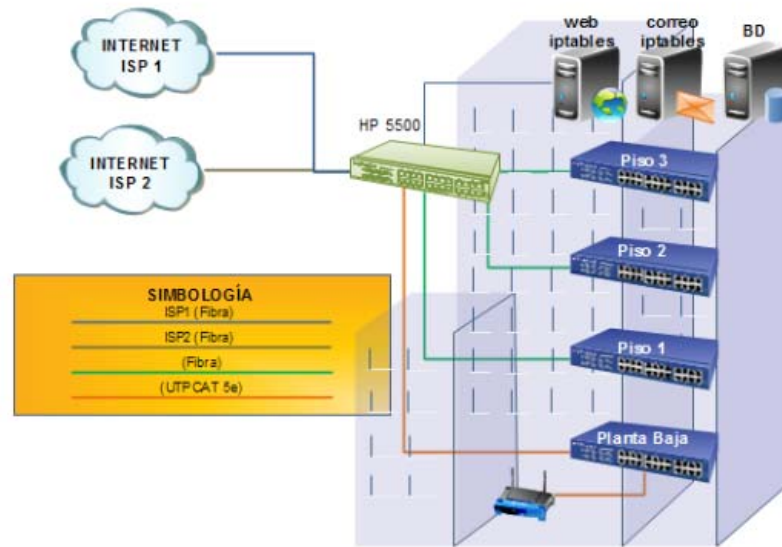


Figura 2.1 Diseño Físico de la red Interna Actual

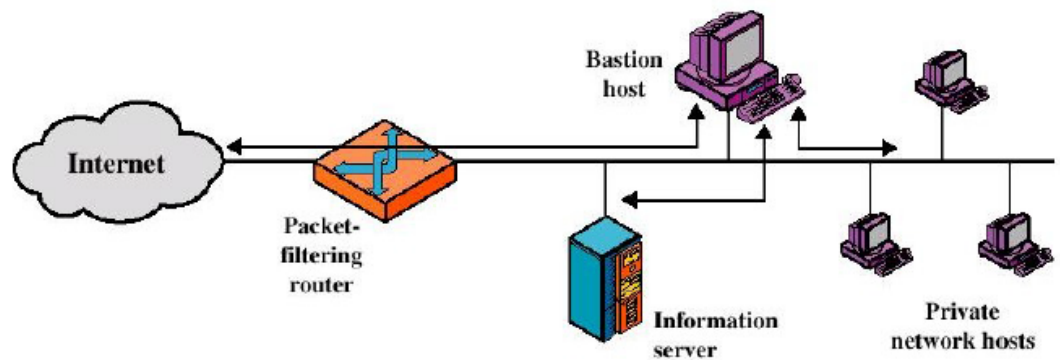


Figura 2.2 Single-homed bastion host

Si bien es cierto, esta configuración, puede ser segura, pero no tan exigentes para lo que necesita una empresa que va creciendo año a año, donde se necesita tener más seguridad desde la parte interna hacia los servidores.

Esto basándose en una encuesta sobre seguridad informática realizada a un grupo de empresarios en el Reino Unido, cuando se les preguntó quiénes eran los atacantes se obtuvieron estas cifras: externos 25%, internos 75% [1]. Estas vulnerabilidades internas pueden deberse a varios factores, como por ejemplo, la falla de un empleado, sea intencional o no, o por un "hacker" que logró traspasar las primeras barreras de seguridad de la empresa, etc.

Una de las soluciones para mejorar la seguridad en la red interna, es teniendo un tipo de configuración Screened-subnet firewall system, ya que esta posee 3 niveles de seguridad.

En la red Interna (Planta de Agua), el caso es similar, ya que poseen el mismo esquema, con una única diferencia de las existencias de redes inalámbricas para las conexiones entre edificios. Se pudo evidenciar que también disponen de un concentrador no administrable y de bajo rendimiento para la convergencia entre voz y datos.

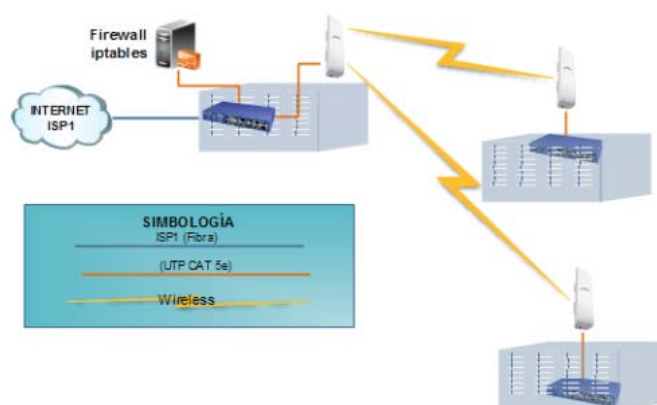


Figura 2.3 Diagrama físico del sector de la Planta de Agua

En este sector los problemas comunes es la pérdida de comunicación de un edificio con la Matriz. Para este caso, la mitigación de este problema se considerara el cambio de equipos de red que permitan mejorar el rendimiento y seguridad, ya que se tiene previsto aumentar el número de usuarios en este sector.

2.2. Análisis y Diseño de la red Perimetral Actual

Como se pudo evidenciar en la Figura 2.1, los servidores existentes en la matriz, no poseen toda la seguridad necesaria. La inseguridad, se encuentra expuesta debido a que no poseen una debida configuración de red para la protección de los servidores. Además se puede evidenciar la existencia de una baja disponibilidad en caso de que el único concentrador de datos falle.

Dentro de la arquitectura de firewall que ellos manejan se encontró, que realmente no disponen de una DMZ (Zona Desmilitarizada), y que la única política de seguridad está en los mismos servidores. Se pretende con el rediseño de la red, crear una DMZ aplicando un tipo de arquitectura de firewall como Screened-subnet firewall system.

Con la utilización de la configuración Screened-subnet firewall system, se podrá tener un nivel de seguridad más alto, debido a que se tendría dispositivos internos y externos con filtrado de paquete, creación de DMZ (Zona desmilitarizada) que puede consistir en un simple bastion Host o más servidores públicos. Los router o dispositivos firewall solo permitirán el tráfico hacia o desde la subred DMZ.

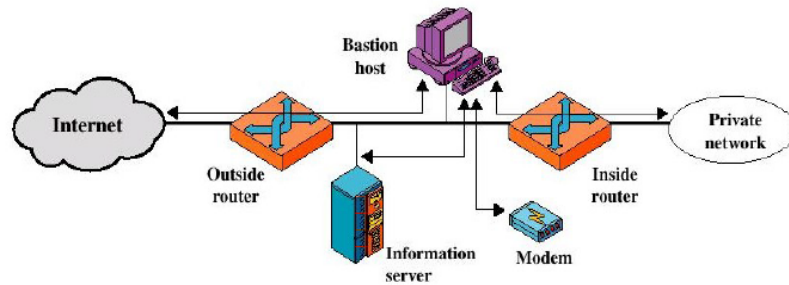


Figura 2.4 Screened-subnet firewall system

2.3. Análisis y Diseño de la red Externa Actual

Para el análisis de la red externa actual, se pudo diseñar con los datos proporcionados por la persona encargada de infraestructura de red de la empresa. Se dio a conocer que aparte de contar con un segundo sector (Planta de tratado de agua), disponían de 4 agencias, que estaban conectados a través del servicio de internet de un solo proveedor.

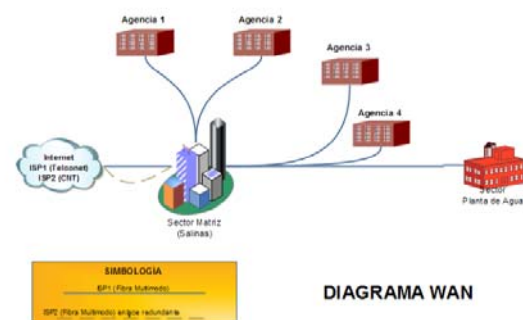


Figura 2.5 Diagrama WAN de la Empresa

En la figura 1.4, Se puede observar que la red WAN, solo dispone de una sola redundancia en el sector Matriz, dando como lugar a que en caso de fallar o perder el servicio del proveedor principal (ISP1), las agencias quedarían incomunicadas. Estas agencias por lo general brindan servicios a sus clientes para que realicen los pagos correspondientes a los consumos mensuales por el servicio de agua. En efectos, las agencias son uno de los puntos importantes para la empresa en la recopilación de valores y sobre todo para el cliente como punto más cercano para cumplir con sus obligaciones con la entidad.

Para la mitigación de la misma es necesario que se cree redundancia con las agencias para no tener problemas de disponibilidad, ya que esta es una de las fases más importante en la seguridad de la información.

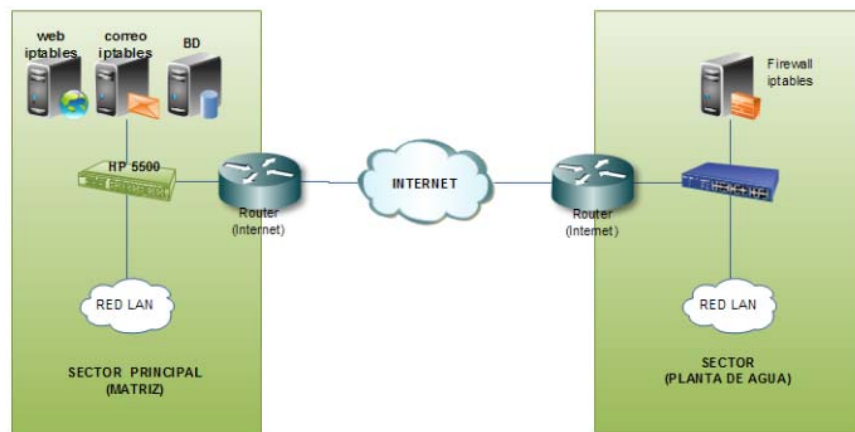


Figura 2.6 Diagrama de enlace Matriz- Planta de Agua

En el análisis más detallado entre los 2 sectores (Matriz y Planta de Agua) se pudo evidenciar lo siguiente: en la matriz, se dispone de un dispositivo Firewall HP 5500, y a este se encuentra conectado los servidores y la red LAN, es decir no dispone de una backup que permita mantener la alta disponibilidad de la red en caso de que fallara este, comprometiendo de igual manera a la red LAN de ataques o Denegación de Servicios.

Es muy similar en el caso del Sector de la Planta de Agua, ya que en este caso, la única seguridad que se tiene hacia la LAN, es a través de un Bastion Host, en caso de un ataque desde el INTERNET a este servidor, queda totalmente comprometida la red LAN del sector. En esta red, se puede evidenciar de igual forma que el Bastion Host, puede estar comprometidos a través de ataques desde la red Interna por el hecho de estar conectada estas a un concentrador de capa 2.

Una de las soluciones que podría ayudar a la protección de la red, es de colocar dispositivos con filtrado de paquete para mejorar la seguridad de la misma.

2.4. Análisis de Dispositivos de Seguridad en la red Actual.

El único dispositivo de seguridad que dispone la empresa en un HP 5500. El dispositivo HP 5500 ofrece capacidades de resiliencia, soporte múltiples en la capa perimetral, seguridad y soporte tanto para las grandes redes de campus y de sucursal. Es un dispositivo que proporciona flexibilidad, escalabilidad, bajo con un conjunto de características compatibles con el

apilamiento IRF, el enrutamiento estático y OSPF, RIP, BGP; IS-IS, PoE+, ACL e IPv6.

2.5. Análisis de Dispositivos CISCO a contemplar para el rediseño de la red.

CISCO ASA 5500-X. Esta edición de Firewall permite a las empresas implementar en forma segura y confiable aplicaciones y redes cruciales. Su exclusivo diseño modular ofrece una protección de la inversión significativa y reduce los costos operativos.

Funciones y ventajas

Disponibles en una amplia variedad de tamaños, los modelos Cisco ASA CX proporcionan el mismo nivel de seguridad que protege las redes de algunas de las empresas más grandes y más preocupadas por la seguridad del mundo. También proporcionan servicios de firewall de próxima generación Cisco ASA serie CX, que incluyen Cisco Application Visibility and Control (AVC), seguridad web, filtrado de botnets y prevención de intrusiones, para que pueda agregar estas características de seguridad a las aplicaciones y dispositivos nuevos de la red [2].

Estos dispositivos firewalls de próxima generación Cisco ASA protegen los recursos críticos de varias maneras por ejemplo, Cisco Web Security Essentials, limita el uso de Internet y de aplicaciones web según la

reputación del sitio, Cisco Security Intelligence Operations preserva la amplia y sólida seguridad de red con el uso de servicios integrados de firewall basados en software y en la nube, facilita un sistema de prevención de intrusiones (IPS) altamente eficaz, incluyen una VPN de alto rendimiento y acceso remoto siempre activo y, brindan servicios adicionales de seguridad de implementación fácil y rápida.

Cisco Catalyst 4500. Es un dispositivo que nos permite agilizar el crecimiento del negocio y sobre todo mejorar la eficiencia. Este Switch Cisco, son dispositivos base para redes empresariales y de mayor expansión en las plataforma modular de la industria para implementaciones de acceso y distribución de campus.

Este dispositivo permite la facilidad de agregar funcionalidades de IDS e IPS, además hace la funcionalidad de Firewall completo a nivel de capa 7.

Cisco Catalyst 3560. Estos switch soportan la tecnología Cisco EnergyWise, que ayuda a las empresas a gestionar el consumo de energía de la infraestructura de red y los dispositivos conectados a la red, lo que reduce sus costos de. Estos dispositivos nos ayudan a maximizar la productividad y proporciona protección de la inversión al permitir una red unificada para datos, voz y video.

Este dispositivo posee muchas características de seguridad, de las cuales solo mencionara las siguientes: IEEE 802.1x permite la seguridad dinámica, basada en el puerto, asignación de VLAN dinámica para un usuario

específico, independientemente de donde se conecta el usuario, acceso a la VLAN de voz, permite políticas específicas de seguridad basadas en la identidad, independientemente de donde se conecta el usuario, ACL VLAN seguridad (VACLs), Filtrado de Unicast MAC, SSHv2, Kerberos y SNMPv3 brindan seguridad de la red mediante la encriptación del tráfico, Private VLAN Edge, asegura el acceso a un puerto de acceso o troncal basada en la dirección MAC, Dinámica ARP Inspection (DAI), DHCP snooping, Seguridad multinivel en el acceso a la consola, BPDU Guardia apaga Protocolo Spanning Tree interfaces de PortFast, Autenticación web para clientes

Cisco Catalyst Express 500 (CE 500). Diseñado para integrar las necesidades de las organizaciones en crecimiento. Es un dispositivo de capa 2 con conexiones Fast Ethernet y Gigabit Ethernet sin bloqueo. Posee un rendimiento a velocidad de cable y facilita una base de red segura para redes de datos e inalámbricas.

Entre las características se puede mencionar que posee una mejora en la eficacia operativa mediante la dispersión de un switch inteligente, simple y seguro. Ofrece un rendimiento a velocidad wirespeed para garantizar que los clientes y servidores de la red operen a máxima eficiencia.

2.6. Propuesta del rediseño de la infraestructura de Red

Para empezar con el rediseño de la red, es importante entender la utilización del modelo jerárquico de 3 capas, ya que tiene muchos beneficios en el diseño de la redes, y nos ayuda hacerlas más predecibles.

Con la utilización de este tipo de modelo nos facilita el diseño, la implementación, el mantenimiento, la escalabilidad de las redes, además, permite mejorar la aislación de fallas [2].

La empresa por basarse en una entidad grande cuyo crecimiento de clientes es de forma ascendente, es necesario que se use este modelo jerárquico, la misma que permitirá un mejor control y flujo de datos de forma eficiente en la red, facilitando de igual manera su administración.

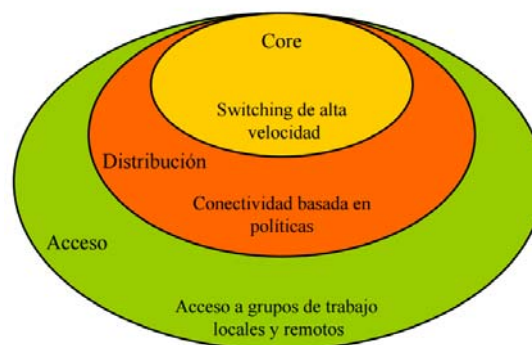


Figura 2.7 Modelo Jerárquico de una Red

En temas de seguridad o protección de los datos y la red como tal, es necesario que se aplique un tipo de configuración **Screened-subnet firewall system**, ya que esta posee 3 niveles de defensas ante intrusos.

Este tipo de configuración permitirá a la empresa mejorar la seguridad tanto a sus servidores como el acceso a su propia red. Esto permitirá tener una mejor administración, ya que admitirá la creación de una DMZ.

El objetivo principal, es para que todo el tráfico externo se comunique solamente con la DMZ. Se puede señalar que, creando una DMZ, no permitirá la comunicación de la red Externa con la red interna, previniendo posibles ataques en caso de algún intruso gane control de la DMZ.

Para el análisis del rediseño de la infraestructura de red y seguridad de la misma, se concentra básicamente en 4 ambientes: INTERNET, DMZ Y RED INTERNA (Red LAN).

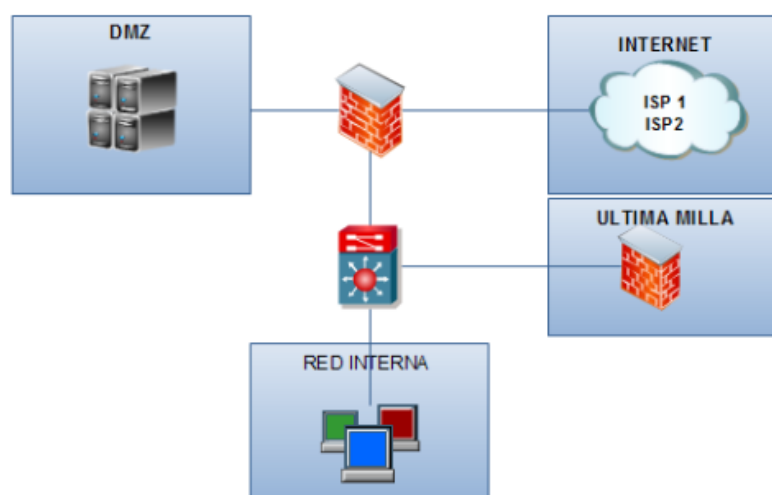


Figura 2.8 Ambientes de la Red propuesta a analizar

MEJORAMIENTO DE LA INFRAESTRUCTURA DE RED EXTERNA

Uno de los factores importantes a considerar es la conectividad entre el Sector Matriz con el sector de Planta de Agua y Agencias, esta última, es de gran importancia, ya que generan información financiera en las recaudaciones de los pagos de clientes con el servicio prestado.

El diagrama WAN contemplado en el rediseño de red, se puede visualizar en la figura 2.9 en la que se agrega la redundancia con las agencias, mitigando de esta manera problemas de disponibilidad.

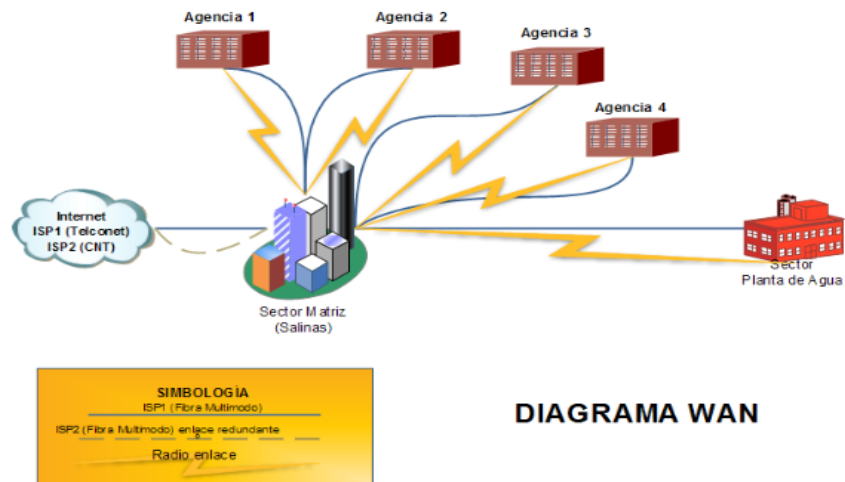


Figura 2.9 Diagrama Lógico WAN propuesto

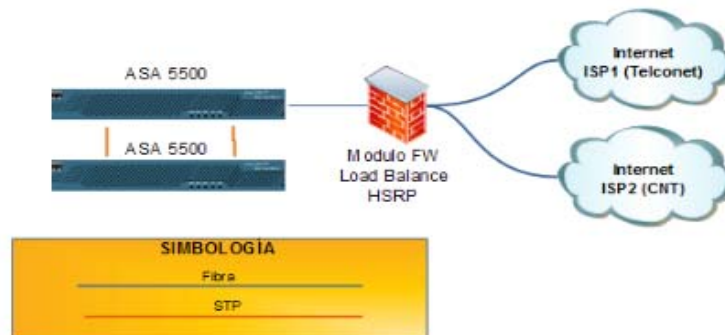


Figura 2.10 Diagrama Físico WAN propuesto

Desglose del rediseño de la comunicación WAN.

El enlace principal entre las agencias, serán cubiertos por un proveedor ISP1, a través de un medio de fibra con un ancho de banda mínimo que permita la operación de la empresa.

Para la redundancia en la comunicación WAN está basada por los radio enlaces siempre y cuando tenga una línea de vista. La utilización de este medio, deberá ser regularizada con la superintendencia de telecomunicaciones.

Para asegurar el perímetro exterior de la red interna (red LAN sector Matriz), se utilizara 2 dispositivo Firewall CISCO ASA 5550. La justificación de estos dispositivos es para que trabajen como redundancia uno en modo Activo y el otro en modo Pasivo, es decir, los 2 dispositivos estarán encendidos, pero solo uno de ellos estará en funcionamiento, en caso de falla en uno de estos, automáticamente se levanta el otro dispositivo ASA 5550 tal como se observa en la figura 2.10

De igual manera, estos dispositivos deberán manejar protocolo HSRP, la que nos permitirá administrar el balance de carga con los 2 proveedores ISP.

Con el uso de este tipo de arquitectura de firewall y usando dispositivos CISCO ASA, permitirá tener un alto rendimiento de redundancia a nivel de la red Externa.

Para el funcionamiento correcto y protección la red de la empresa, se contemplara las siguientes configuraciones firewall: para redes WAN, creación de Intranets, creación de extranets, creación de VLAN, creación de redes y subredes, control de ancho de banda, segmentación de redes, filtros de navegación, filtros de contenido de páginas no deseadas, filtrados de Ips y bloqueo de puertos.

La creación de VPN, es fundamental para la red de la empresa, ya que permitirá tener escalabilidad, debido a que la infraestructura del servicio de internet dentro de los ISP, nos ayudará a la agregación de nuevos usuarios.

En cuestiones de seguridad, las VPN incluirán mecanismo de seguridad mediante protocolos de cifrado y autenticación avanzada para proteger los datos contra los acceso no deseados.

La conectividad entre el sector Matriz y Planta de Agua, deberán poseer seguridad de conexiones a internet, por lo que se recomienda utilizar un tipo de conectividad VPN con IPsec. Esto ayudara a que la información privada se transporte de manera segura a través de la red pública logrando de esta manera confidencialidad e integridad de datos, y autenticación.

MEJORAMIENTO DE LA INFRAESTRUCTURA DE RED PERIMETRAL

Para efectos de este rediseño, cabe recalcar que en la red actual no poseen una DMZ (Zona Desmilitarizada), y con esta propuesta se pretende crearla.

Cabe indicar que los firewall ayudan a definir reglas de acceso entre dos redes. Sin embargo, la empresa en estudio, tienen una sola subred con ciertas reglas de negocio configuradas. Es por eso la necesidad de cambiar la arquitectura firewall de la empresa a Screened-subnet firewall system.

Con esta arquitectura se deberán crear y aislarán las diferentes subredes a considerar en la empresa. Una de estas subredes es básicamente donde se colocara la DMZ. La DMZ, ofrece una zona de seguridad donde los servicios y los datos pueden ser compartidos entre las zonas de producción y Empresa. Además, la DMZ permite una fácil segmentación de control de la organización [3].

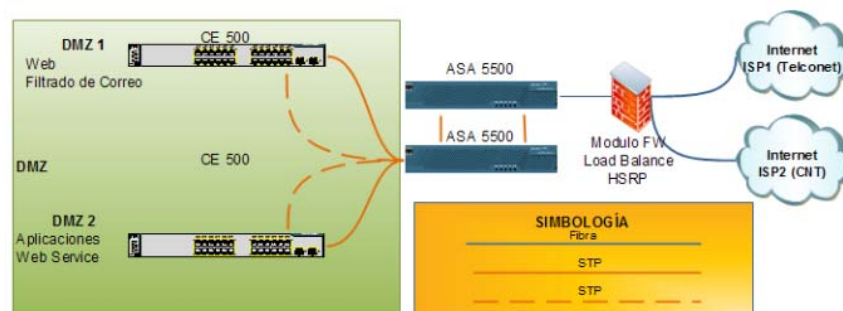


Figura 2.11 Diagrama Físico DMZ Propuesto

Como se puede observar en la figura 2.11, el uso del dispositivo Firewall ASA 5550, permitirá conectar las 2 DMZ, en la que denominaremos DMZ pública y DMZ pública restringida. En la DMZ pública, se alojaran solo los servidores que están expuestos a internet y que por lo general son más vulnerables. (Servidor Web, filtrador de correo electrónico). En la DMZ

publica restringida, estarán alojados servidores para usuarios de la empresa o clientes externos (Servidores de aplicaciones, Web Service).

Las seguridades que aplican en tener 2 DMZ radican en que si uno de los servidores de la DMZ pública son atacadas, no afecten a los otros servidores de la DMZ pública restringida.

De igual manera se considerara redundancia entre el Firewall y las DMZ. El medio de comunicación principal a utilizar será mediante fibra y la redundancia a través de un cable STP Categoría 6a. La justificación del cable STP Cat 6a es porque este medio dispone mayor protección de blindaje, por lo que es menos tolerante a interferencia y ruido, y pueden transmitir hasta 10GB.

En el Dispositivo CE500 de CISCO, se deberán configurara VLAN, según la asignación adecuada para cada servidor.

MEJORAMIENTO DE LA INFRAESTRUCTURA DE RED INTERNA

Para mejorar la seguridad de la red interna de la empresa, se considerar un equipo Switch 4500, ya que tiene la funcionalidad de incorporar IDS (Sistema de detención de intruso) e IPS (Sistema de prevención de intruso). Este equipo también hace las funcionalidades de LAN y Firewall completo, es decir a nivel de capa 7.

Para llevar a efectos de redundancia se deberá disponer de 2 módulos en el Switch 4500, con el objetivo de tener un alto rendimiento en redundancia.

La seguridad para toda la red interna está basada en 2 Dispositivo Firewall de CISCO, como lo son el ASA 5550 y el Switch 4500.

Actualmente la empresa dispone de una conexión inalámbrica, con la finalidad de brindar algún tipo de servicio o conexión a internet a usuarios o clientes. Para efectos de tener seguridad hacia la red empresarial, se considera colocar un dispositivo CE 500 entre el ASA 5550 y el Switch 4500. El objetivo es de no comprometer mi conexión LAN, ya que estos equipos que se conectan de forma inalámbrica y pueden estar infectados, tener algún tipo de software de espionaje, o puede surgir algún tipo de barrido interno de la máquina, etc.

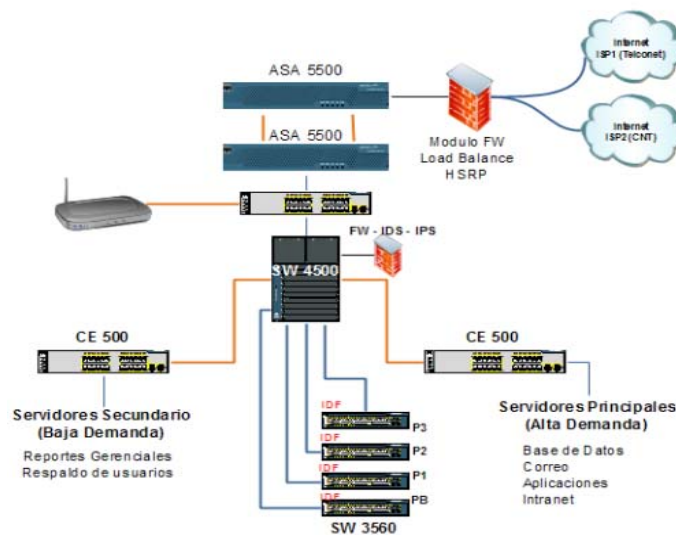


Figura 2.12 Diagrama Físico (Matriz) de la red Interna propuesto

En la conexión LAN del sector de la Planta de Agua, se utilizara un dispositivo 3750, ya que esta permite realizar el enrutamiento de las VLAN, y sobre todo permite colocar módulo de firewall para el filtrado de paquete (Figura 2.13).

Para que tenga un alto rendimiento en redundancia se utilizara un segundo equipo 3750, en caso de la falla de una de ellas, se enciende el de backup.

Las configuraciones que deberá tener este dispositivo, son básicamente políticas de acceso, filtrado de tráfico, así como también las configuraciones correspondientes de VLAN.

La conexión hacia los edificios se los realizará por medio de conexiones inalámbricas, y esta estará conectada a través de un Switch CE 500. Estos dispositivo también deberá tener las configuraciones correspondientes de seguridad y de VLAN según sea la necesidad del área.

Los dispositivos de conexión inalámbrica, deberán ser cambiados por otros dispositivos de mayor alcance y de alto rendimiento.

No se considera disponer de una redundancia en la conexión entre áreas, pero si fuera el caso, se optaría en colocar solo una línea de fibra en una un edificio. El motivo de aquello es por la existencia de 2 usuarios en un edificio (LAN 2), 10 usuarios en otro edificio (LAN 3) y, en la que no se contempla un nivel de crecimiento en este sector (Planta de Agua).

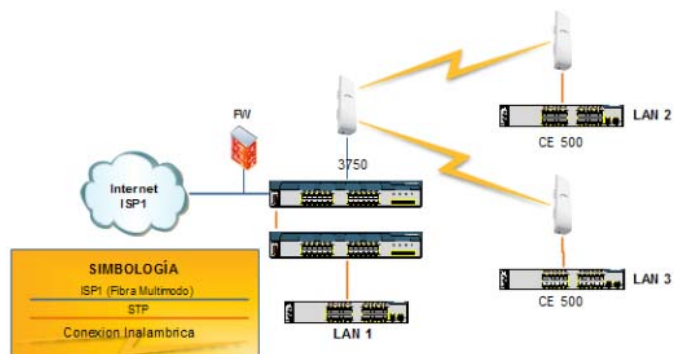


Figura 2.13 Diagrama Físico (Planta de Agua) de la red Interna propuesta

Concluyendo con el rediseño de la infraestructura de red tanto de la red de borde, red perimetral y red externa, se puede lograr el cumplimiento de los objetivos en seguridad de la información como integridad, disponibilidad y confidencialidad.

CAPÍTULO

3. ANÁLISIS DE RESULTADOS

3.1. Validación de la seguridad de la red de borde propuesto con el personal de infraestructura de la organización

Durante la validación de la seguridad analizada con la persona encargada de la infraestructura de red de la organización, se hizo un pequeño análisis del equipo que ellos disponen para la seguridad de borde. El objetivo de este análisis es para ver si brindan los mismos servicios y mayor seguridad en la infraestructura de red que se está proponiendo. Se llegó a la conclusión de que el equipo contemplado en el rediseño para la seguridad de borde, cumple con todas las exigencias de protección y flujo de datos, porque además de ser un dispositivo Firewall, permite realizar un balanceo de carga usando protocolo HSTP, y ésta a la vez dispone de una licencia propia del

mismo fabricante del dispositivo, además dispone de la funcionalidad de IPS (Sistema de Prevención de Intruso).

En asuntos de querer implementar una VPN, se dedujo que se proporcionaría funciones fundamentales como confidencialidad, porque permite el cifrado de los datos antes de ser transmitido por la red, integridad de los datos por la verificación de los datos transmitidos, Autenticación por identificar la identidad del origen de los datos, y protección de antirreproducción por la detección y el rechazo de los paquetes reproducidos con el propósito de prevenir la suplantación de identidad.

Casos de uso relacionado a la utilización de equipos ASA de CISCO. Cisco Borderless Network ayuda a Hotel International Sinaia aumentar las reservas de eficiencia y la elevación de ocio operativos en un 20 a 30 por ciento. Seguridad de la red, una preocupación clave para la industria hotelera, es proporcionada por el Series Adaptive Security Appliance de Cisco ASA 5500 [4].

3.2. Validación de la seguridad de la red interna propuesto con el personal de infraestructura de la organización

Dentro de las soluciones planteadas sobre la configuración de una arquitectura de firewall, se verificó que esta esta solución permitiría aumentar la protección a la red Interna (red LAN) y sobre todo a los servidores de alta demanda de la empresa. De igual manera se puede evidenciar en el rediseño la forma de cómo tener una buena administración a nivel de

servidores de baja y alta demanda. Esta solución planteada, sirvió para que ellos puedan establecer nuevas políticas de seguridad con respecto al acceso a sus aplicaciones.

Se resaltó que en su organización es necesario disponer de esta seguridad interna y que el tipo contemplado en el rediseño cisco 4500, sería una de las mejores soluciones en la empresa ya que permite a nivel de seguridad, configuraciones de filtrado de paquete y sobre todo permite agregar funcionalidades de un IDP E IPS.

El dispositivo de alto rendimiento, ayudara a tener una red convergente, ya que actualmente la empresa comienza hacer uso del servicio de voz y datos. Se justifica de igual manera que este dispositivo ayudará en el crecimiento de la red, la misma que se tiene contemplados en un proyecto futuro de la organización.

Para una mejor administración de la red LAN, es necesario realizar un estudio más detallado de toda la organización y por departamento, con el objetivo de segmentar toda la red y poder crear VLAN. Con la implementación de estas VLAN, se podrá establecer mejores reglas de negocio en los dispositivos.

Casos de uso relacionado a la utilización de equipos SWITCH 4500 de CISCO. *“Sky Studios acelera traslado a los flujos de trabajo de medios digitales y establece normas para la eficiencia de la radiodifusión y la sostenibilidad”*. Sky es una parte valiosa de la vida cotidiana en más de 11

millones de hogares. Con una mezcla potente de derechos deportivos exclusivos, películas y entretenimiento. Como la organización Sky creció rápidamente, trajo nuevos edificios en el campus de Osterley en servicio en un plazo relativamente corto. Procesos de producción tradicionales confiados en cintas almacenadas en múltiples ubicaciones en todo el campus Osterley. El equipo de gestión de la conclusión de que esta forma de trabajar era demasiado ineficiente. Se crea una arquitectura IP escalable, que se extiende desde el punto de ingesta contenido a través de todos los aspectos de la edición y la producción, a través de la contribución de vídeo y redes de distribución, y todo el camino a la pantalla del cliente. Consta de más de 200 de Cisco Nexus 7000 y Catalyst 4500 y 6500 Series Switches, la Plataforma de flujo de trabajo de medios forma un tejido de 10 Gbps que protege contra la degradación de vídeo potencial causado por factores como la latencia y jitter. Esta red ayuda asegura paquetes de vídeo siempre llegan en el tiempo y en secuencia [5].

3.3. Validación de la seguridad de la red perimetral propuesto con el personal de infraestructura de la organización

Durante el análisis de seguridad en la red perimetral, se estuvo de acuerdo de que es necesario la creación de una DMZ para evitar comunicación de la Internet con la red interna de la empresa.

Se dieron a conocer sobre una de las ventajas que se tiene al utilizar el dispositivo Cisco ASA 5550 como la posibilidad de tener 2 DMZ y sobre todo

Firewall de alto rendimiento para la seguridad de la misma. La creación de 2 DMZ, ayudaría aún más en la administración y organización de los servidores.

Se establecieron que de igual manera deberían implementarse políticas para la DMZ como prohibiciones, denegaciones y autorizaciones en el tráfico de la red interna y externa.

3.4. Informe final del rediseño de la red Propuesta

En el proceso de análisis de revisión del rediseño propuesto para la empresa pública de agua potable, se realizaron las comparaciones correspondientes con el objetivo de validar los resultados esperados.

Las validaciones para el mejoramiento de la seguridad en cada ambiente de red resultaron favorables y beneficiosas para la empresa, ya que se consideró una de las mejores arquitecturas de firewall. Para el caso del rediseño de la red, no se utilizaron direccionamientos y revisiones de configuraciones de equipos de seguridad por motivos de confidencialidad de la misma.

La red propuesta cumple con los objetivos esperados, como por ejemplo, el colocar alta disponibilidad en redundancia en equipos principales nos permite tener disponibilidad de datos. A través del uso de equipos de alto

rendimiento y servicios de firewall, con una buena configuración, se podrá tener integridad y confidencialidad de los datos.

A través de la creación de DMZ Y VLAN se podrá tener una buena administración y organización de la red y sobre todo establecer reglas de negocio en los dispositivos.

Para complementar y garantizar tener una red segura, es necesario que se establezcan políticas de seguridad en la organización. Estas políticas serán las base de cualquier mecanismo de técnicos, de procedimientos y de organizaciones seguras [6].

CONCLUSIONES Y RECOMENDACIONES

Conclusiones:

1. El objetivo principal del rediseño de la infraestructura de red en empresa pública de agua, es de contribuir y dar a conocer sobre la nueva forma de protección de datos y que pueden ser aplicados en futuros proyectos de mejora.
2. El uso de dispositivos específico y de una sola marca es esencial por la compatibilidad de la misma, para este caso se enfocó en una marca reconocida por su variedad de soluciones de networking, sin desprestigiar a las otras marcas.
3. Para una buena administración y control de los usuarios y clientes conectados, es necesario disponer de subredes, clasificado por el tipo de información que manejen.
4. Un buen diseño de infraestructura de red, no significa que tenga un alto rendimiento en seguridad de la información, ya que estos deben de

complementarse con políticas de seguridad alineadas con estrategia de la empresa.

Recomendaciones:

1. El rediseño de la infraestructura de red debe ser contemplado como mejora para la empresa, por el hecho de que es una entidad en el que manejan un tipo de información muy confiable para la organización.
2. No es necesario el uso de estos dispositivos para el rediseño de la infraestructura de red, pueden usarse otros dispositivos de otra marca siempre y cuando faciliten con el propósito común de tener alta disponibilidad y seguridad de la red y de los datos como tal.
3. La empresa como tal deberán crear VLAN con el único propósito de tener un mejor control y administración de toda red, con esto se reduce tiempo en mantenimiento.
4. La empresa como tal, deberá de establecer políticas de seguridad de la información, con el propósito de tener claro las reglas de negocio al momento de configurar los dispositivos.

BIBLIOGRAFÍA

- [1] G. I. S. Survey, 2004. [En línea]. Available:
<http://trygstad.rice.iit.edu:8000/Articles/2004GlobalInformationSecuritySurvey-Ernst&Young.pdf>.
- [2] CISCO, «Cisco Systems, Inc,» 2015. [En línea]. Available:
http://www.cisco.com/web/LA/assets/pdfs/asa_5500-X_series_next_gen_ds_es_xl.pdf.
- [3] D. S. G. G. R. Niskayuna, «<http://www.ieee802.org/>,» 2012. [En línea]. Available:
<http://www.ieee802.org/1/files/public/docs2012/avb-sextonda-ethernet-for-converged-applications-1112.pdf>.
- [4] C. System, «cisco.com,» 2012. [En línea]. Available:
http://www.cisco.com/c/dam/en/us/products/collateral/switches/catalyst-2960-series-switches/hotel_al_siaia_cs.pdf.
- [5] C. System, «cisco.com,» 2012. [En línea]. Available:
http://www.cisco.com/c/dam/en/us/solutions/collateral/switches/catalyst-6500-series-switches/sky_studios.pdf.
- [6] M. N. A. C. Research, «<https://www.computer.org/>,» 2007. [En línea]. Available:
<https://www.computer.org/csdl/proceedings/hicss/2007/2755/00/27550115a.pdf>.
- [7] Kiokea.net, «ccm.net,» 2014. [En línea]. Available:
<http://es.ccm.net/contents/589-dmz-zona-desmilitarizada>.