PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES Y TELECOMUNICACIONES

PERFIL DEL TRABAJO PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

MAGISTER EN REDES Y TELECOMUNICACIONES

TEMA

“ESTUDIO Y PROPUESTA DE DISEÑO PARA LA ARQUITECTURA DE SEGURIDAD PERIMETRAL DE CAMPUS, CASO DE ESTUDIO DATA CENTER PARA EL MUNICIPIO DEL DISTRITO METROPOLITANO DE QUITO"

JUAN FRANCISCO LÓPEZ FIERRO

QUITO - 2016

DEDICATORIA

A toda mi familia que siempre están presentes en los buenos y malos momentos, y que comparten cada momento junto a mí, su apoyo y amor incondicional para alcanzar mis logros personales y profesionales.

ÍNDICE GENERAL

ÍNDICE DE IMÁGENES

ÍNDICE DE TABLAS

CAPÍTULO 1

INTRODUCCIÓN

1.1 Introducción

La llegada de las TICs (Tecnologías de la Información y Comunicación) y la gran expansión que este concepto ha provocado alrededor del mundo, ha permitido que los recursos tecnológicos y la información sean indispensables en la cotidianidad laboral de cada individuo e incluso como parte de la vida diaria, afectando el ámbito económico, social y cultural que nos rodea.

Debido a que la información y los recursos informáticos se encuentran al alcance de un solo clic y esto asociado al crecimiento paulatino que sufren, se vuelven en un elemento crítico y vulnerable que puede ser amenazado o atacado

Es aquí donde la seguridad informática entra a formar parte integral e indispensable en las TIC. Este nuevo concepto implica conocer, diseñar e implementar adecuadamente conceptos, esquemas, diseños, herramientas, metodologías, estándares, mejores prácticas, regulaciones, tendencias y normativas de seguridad en el manejo y utilización de los recursos tecnológicos y la información, con el objetivo de precautelar y garantizar la integridad, disponibilidad y confidencialidad de los recursos tecnológicos y de la información.

Debido a la importancia y dependencia que han alcanzado las TICs, estas pasan a ser un elemento fundamental dentro de una organización pública o privada, la cual debe

tomársela en cuenta, debido a que mientras más crece esta tendencia, las amenazas y ataques crecen en mayor o igual proporción, lo que obliga a estar preparados para mitigar, enfrentar y gestionar estos riesgos, dando continuidad y protección al negocio.

Para poder lograr continuidad y protección del negocio, es necesario disponer de una infraestructura tecnológica sólida, segura y protegida. Para esto se requiere diseñar un nuevo esquema de seguridad, el cual contemple los factores de seguridad más importantes y recomendados para una infraestructura tecnológica de una organización, pensando en el core del negocio y la información que maneja.

Las amenazas o ataques que sufren hoy en día las organizaciones en su infraestructura tecnológica, generan un desequilibrio y una brecha en la infraestructura tecnológica organizacional, lo cual afecta en el correcto funcionamiento de las diferentes herramientas tecnológicas y directamente a la información, afectando la integridad, disponibilidad y confidencialidad de los recursos.

De la misma manera, las amenazas o ataques no provienen únicamente desde afuera. Aquí también hay que considerar que también existen amenazas y ataques que se generan o provienen de adentro, es decir, de la propia infraestructura tecnológica que posee una organización, siendo éstas las mayores vulnerabilidades que existen actualmente.

El nuevo diseño del esquema de seguridad para la infraestructura tecnológica del Municipio del Distrito Metropolitano de Quito permitirá mitigar, enfrentar y

gestionar todos estos riegos, tanto internos como externos, el cual considerará conceptos, herramientas, estándares, equipamiento y mejores prácticas de seguridad.

Al mismo tiempo el nuevo diseño será la base estructural para la implementación de nuevas y mejoradas herramientas y equipamiento para el control y monitoreo de la seguridad de la infraestructura del Municipio del Distrito Metropolitano de Quito. Bajo este criterio es fundamental que el diseño sea sólido e integrable.

1.2 Justificación

El Municipio del Distrito Metropolitano de Quito actualmente atiende a más de 6000 usuarios, distribuidos por diferentes dependencias, y brinda sus servicios aproximadamente a un 60% de la población de todo el Distrito Metropolitano de Quito. El Municipio del Distrito Metropolitano de Quito con el afán de brindar una mejor y rápida atención a sus contribuyentes, ha implementado diferentes servicios como: servicios web, zonas wifi gratuitas, puntos de atención a los contribuyentes, entre otros, los cuales demandan la utilización de los recursos de infraestructura tecnológica que posee la institución.

Adicionalmente, la infraestructura Tecnológica del Municipio del Distrito Metropolitano de Quito brinda servicios a entidades públicas externas y entidades bancarias que combinan sus servicios con los del Municipio del Distrito Metropolitano de Quito, para los diferentes usuarios tanto externos como internos.

Este esquema conlleva a que la infraestructura tecnológica del Municipio del Distrito Metropolitano de Quito sea un punto vulnerable y crítico, que puede ser afectado, lo que causaría que los servicios e información del Municipio del Distrito

Metropolitano de Quito sean amenazados. En este sentido, actualmente la infraestructura tecnológica dispone de un esquema de seguridad que asegura y previene cualquier tipo de amenaza.

Sin embargo, el esquema de seguridad actual, carece de un diseño en alta disponibilidad, políticas de seguridad, buenas prácticas, procedimientos y recursos que optimicen el esquema actual que resguarda la integridad, confidencialidad y disponibilidad de la información, servicios y sistemas que brinda el Municipio del Distrito Metropolitano de Quito.

Considerando lo indicado anteriormente y debido a la importancia de mantener la operatividad y garantizar la disponibilidad de los servicios que brinda el Municipio del Distrito Metropolitano de Quito a sus usuarios, es necesario rediseñar, optimizar, robustecer y mejorar el esquema actual de seguridad para la infraestructura tecnológica del Municipio del Distrito Metropolitano de Quito, que beneficiará a los usuarios y principalmente a la institución.

1.3 Antecedentes

(Barrera, 2011) El Alcalde del Municipio del Distrito Metropolitano de Quito indica que: "La planificación y gestión del desarrollo y del territorio se fundamentan no sólo en el cumplimiento de disposiciones que por Ley competen a la Institución Municipal, sino en las convicciones de la actual Alcaldía Metropolitana para cumplir con la responsabilidad de lograr avances significativos hacia el desarrollo equitativo y sustentable del DMQ y la consecución del Buen Vivir."

Este plan de desarrollo se logra constituyendo una base sólida, no solo en lo administrativo, el desarrollo tecnológico forma parte de estos elementos fundamentales, para el desarrollo del Municipio del Distrito Metropolitano de Quito y la ciudadanía, beneficiando a ambas partes.

(FUOC, 2007) Afirma que en la mayoría de las organizaciones disponen actualmente de mecanismos de prevención y de mecanismos de protección de los datos integrados en sus redes. Sin embargo, aunque estos mecanismos se deben considerar imprescindibles, hay que estudiar como continuar aumentando la seguridad asumida por la organización. Una buena forma de mejorar la seguridad de la red pasa por la instalación de mecanismos de detección, capaces de avisar al administrador de la red en el momento en que se produzcan ataques a la seguridad de la red.

Sistemas desarrollados sobre Internet, se encargan de evaluar diariamente la seguridad perimetral de la red, buscando y generando severas y cientos de ataques diarios. Algunos de estos son simples escaneos que sabemos cómo defendernos, pero otros pueden tomarnos por sorpresa (Northcutt, Zeltser, Winters, Kent, & W. Ritchey, 2005).

Uno de los aspectos más difíciles de asegurar en las redes modernas, son las que exhiben propiedades porosas. Conexiones inalámbricas, dispositivos de almacenamiento externos, sistemas móviles y accesos web ofrecen múltiples caminos donde la información puede ser filtrada o extraída, burlando las defensas. Siendo una de las razones del porque un solo mecanismo de seguridad no es apropiado para proteger la red, pero entre algunos mecanismos pueden hacerlo (Northcutt, Zeltser, Winters, Kent, & W. Ritchey, 2005).

En un reciente estudio de las amenazas persistentes avanzadas (Miller, 2012) se dice que: “Proteger una organización constituye un desafío cada vez más arduo y los ataques son cada vez más complejos, y el avance de las amenazas persistentes avanzadas, que ha hecho que las organizaciones tomen conciencia de su vulnerabilidad ante los ataques”.

Hay que entender que la seguridad informática es un proceso, en el cual intervienen todas las tecnologías, productos, y especialmente, el sentido común de los seres humanos que la gestionan, en las cuales se involucran ámbitos de seguridad como: Seguridad Física, seguridad lógica y gestión de Seguridad (DTe, 2015).

Por tal motivo, la importancia primordial que debe darse a la protección de los sistemas y de los entornos de red y más teniendo en cuenta el incremento masivo de los ataques que se está produciendo en la actualidad. Mantener los recursos de información y telecomunicaciones protegidos contra extraños o intrusos, es una de las principales prioridades para cualquier organización (Giménez, 2008).

Con el incremento de los servicios en línea (Internet), también se ha incrementado el nivel de riesgos y ataques derivados de las vulnerabilidades que acarrea la implementación de nuevas tecnologías, para el intercambio comercial de información. Herramientas que evolucionan paralelamente o mayor al desarrollo tecnológico, orientados a la recolección de información y minería de datos, en ocasiones sin ver comprometido la funcionalidad de los servicios, sistemas o servidores (Flórez R., Arboleda S., & Cadavid A., 2012).

1.4 Objetivos

1.4.1 Objetivo General

Estudiar nuevas tecnologías de seguridad perimetral y proponer un esquema de seguridad para la infraestructura tecnológica del Municipio del Distrito Metropolitano de Quito.

1.4.2 Objetivos Específicos

- Estudiar nuevas tecnologías, buenas prácticas y mecanismos de seguridad que se aplican en la actualidad en el ámbito de seguridad de infraestructura tecnológica.
- Determinar y analizar nuevas amenazas, vulnerabilidades y ataques que afectan a una infraestructura tecnológica
- Conocer y analizar la infraestructura actual del Municipio del Distrito Estudiar nuevas tecnologías de seguridad perimetral y proponer un esquema de seguridad para la infraestructura tecnológica del Municipio del Distrito Metropolitano de Quito para determinar las falencias y carencias del esquema de seguridad.
- Determinar un esquema optimizado, robusto y seguro para la infraestructura tecnológica del Municipio del Distrito Metropolitano de Quito.

1.5 Alcance

Estudiar nuevas tecnologías, buenas prácticas, amenazas, vulnerabilidades, ataques y mecanismos de seguridad actuales, con el fin de proponer una arquitectura de seguridad, más segura y simplificada, bajo el diseño y arquitectura actual del Distrito Metropolitano de Quito. El análisis de los diferentes aspectos a estudiar es el complemento para entender y aplicar el funcionamiento u operatividad de estos, de forma correcta y eficiente, para así estructurar la mejor opción para el MDMQ.

Tantos aspectos físicos como lógicos serán incluidos en el análisis de los diferentes puntos de estudio, aspectos que se encuentran implementados y probados en arquitecturas de seguridad de terceros, que servirán como ejemplo de funcionamiento e integración de los diferentes elementos que comprende una arquitectura de seguridad completa y segura.

El diseño a proponer contemplará la redistribución del equipamiento de seguridad en base a la arquitectura de red que maneja el MDMQ, precautelando el menor impacto en los servicios que brinda a la ciudadanía y al usuario, así mismo, el equipamiento sugerido para la compra, que brindaran un complemento clave para robustecer y mejorar la seguridad de la arquitectura de campus del MDMQ.

La base del diseño de seguridad será la arquitectura actual del MDMQ, la cual sufrirá modificaciones en base al estudio realizado, modificaciones que cubrirán aspectos importantes de seguridad actuales, y que incluye equipamiento de seguridad como también aspectos lógicos de seguridad.

El análisis y estudio de la arquitectura de seguridad actual del MDMQ, tendrá como fin entender el funcionamiento de la arquitectura y los mecanismos de seguridad que actualmente emplea, en base a esto, determinar las brechas y falencias de seguridad que posee la arquitectura, precautelando y garantizando la confidencialidad de la información del Distrito Metropolitano de Quito.

1.6 Resumen

ESTUDIO Y PROPUESTA DE DISEÑO PARA LA ARQUITECTURA DE SEGURIDAD PERIMETRAL DE CAMPUS, CASO DE ESTUDIO DATA CENTER PARA EL MUNICIPIO DEL DISTRITO METROPOLITANO DE QUITO.

CAPÍTULO 2

MARCO TEÓRICO

2.1 Seguridades

2.1.1 Infraestructura Tecnológica y Seguridades

2.1.1.1 Infraestructura Tecnológica

La infraestructura tecnológica es la base que definirá el éxito, el límite y la eficiencia de una organización, como también su crecimiento y desarrollo. Una infraestructura tecnológica está conformada de un conjunto de hardware y software interconectados y en fluida interacción, bajo arquitecturas solidas de alto rendimiento, almacenamiento, flexibles, escalables y redundantes, cuyo objetivo es disponer de los servicios de la organización para usuarios internos y externos.

Es de suma importancia que una organización mantenga una sostenida inversión en IT, ya que (Laudon & Laudon, 2012) indican que: Una infraestructura también es un conjunto de servicios a nivel empresarial presupuestado por la gerencia, que abarca las capacidades tanto humanas como técnicas. Los servicios que una empresa es capaz de proveer a sus clientes, proveedores y empleados son una función directa de su infraestructura de TI. En un plano ideal, esta infraestructura debería apoyar la estrategia de negocios y sistemas de información de la empresa. Las nuevas tecnologías de información tienen un potente impacto en las estrategias de negocios y de TI, así como en los servicios que se pueden ofrecer a los clientes.

Una infraestructura tecnológica coherente y que se encuentre a la par de las TI, debe constituirse de los siguientes elementos:

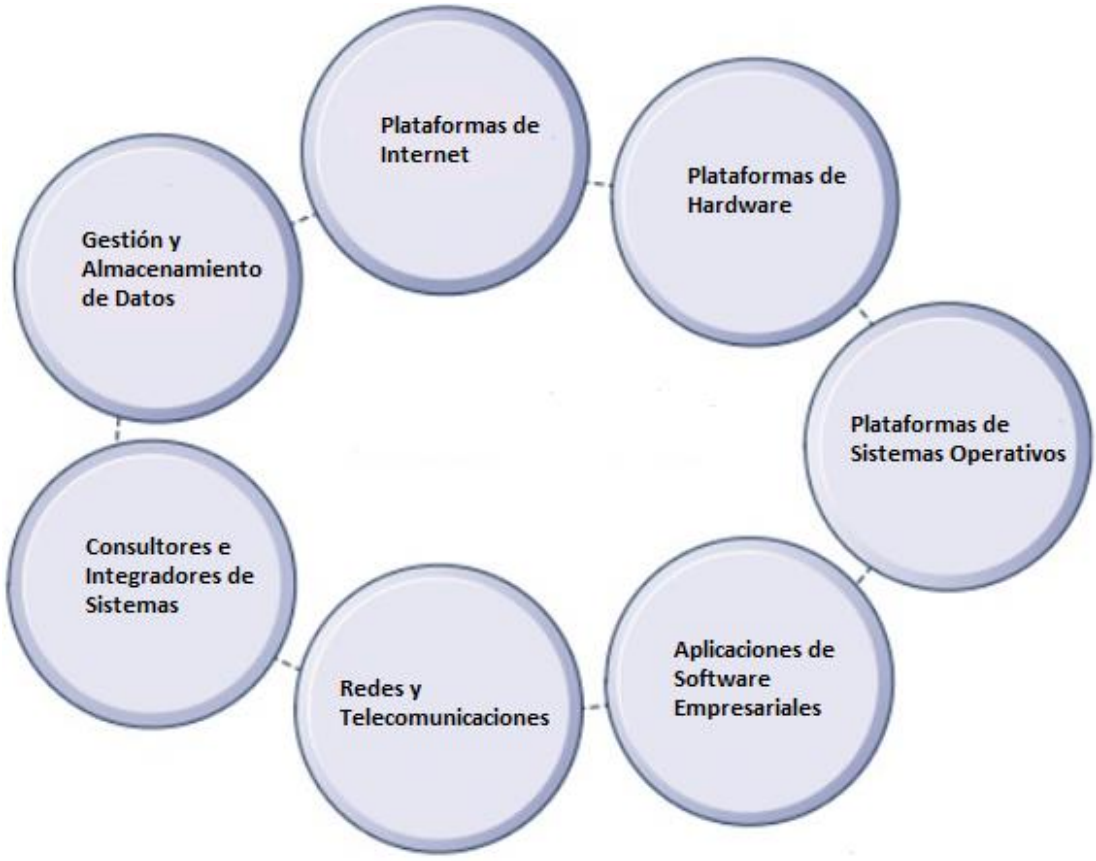

Ilustración 1. (Laudon & Laudon, 2012). Elementos de una Infraestructura TI

2.1.1.1.1 Plataformas de Hardware

Existen gran variedad de plataformas de hardware en la línea de computadoras y servidores, que varían según la tecnología y las características a utilizar. Es fundamental que exista una armonía y compatibilidad entre la plataforma de hardware y la plataforma de software, ya que esto definirá la estabilidad de las funcionalidades y servicios que se implementen.

2.1.1.1.2 Plataformas de Sistemas Operativos

Sistemas operativos escalables, compatibles, seguros, confiables y bajos en costos son el primer requisito para una IT. Existe gran variedad de opciones y varía según la arquitectura sobre la cual se requiera implementar los diferentes servicios o funcionalidades. Cada plataforma trae incorporados mecanismos de seguridad a un nivel básico, el cual puede ser repotenciado para aumentar el nivel de seguridad.

2.1.1.1.3 Aplicaciones de Software Empresariales

Las aplicaciones de software son el elemento más importante dentro de una infraestructura tecnológica, ya que a través de estas se puede acceder a los servicios e información que ofrece la organización a los usuarios internos y externos. Las aplicaciones generalmente dentro de una organización se dividen entre: las propias y de terceros, formando un conjunto que trabaja bajo una misma IT y políticas de seguridad que resguardan la integridad de la información y la disponibilidad de los servicios.

2.1.1.1.4 Redes y Telecomunicaciones

Es el elemento que permite que exista una infraestructura tecnológica interconectada e integrada, es el medio por el cual interactúa la información entre todos los elementos que conforman una IT, esto obliga a que sea el elemento más sensible en un IT. Por tal motivo este elemento debe mantenerse en constante renovación y así alinearse a nuevas tecnologías de comunicación.

2.1.1.1.5 Consultores e Integradores de Sistemas

El avance tecnológico de los diferentes elementos que conforman un IT obliga a que el personal (administradores de la IT) tenga la habilidad y el conocimiento para manejarlo y administrarlo, en muchos casos esto no se cumple, lo que obliga a recurrir a consultores e integradores de sistemas con la experiencia necesaria para implementar, mantener y asegurar la IT.

2.1.1.1.6 Gestión de Almacenamiento de Datos

Elemento encargado de organizar y administrar toda la información de la organización de forma ordenada, segura, integra y accesible, mediante equipamiento avanzado y especializado para esta tarea, equipamiento con diversas tecnologías y métodos para realizar su objetivo. El incremento de los elementos de almacenamiento debe ser continúo debido a que la información aumenta vertiginosamente, la seguridad es un punto esencial para este elemento debido a su criticidad e importancia para una organización, punto que debe ser asegurado y reforzado.

2.1.1.1.7 Plataformas de Internet

La Internet es el medio de comunicación más extenso y utilizado en todo el mundo, el cual se relaciona con cada uno de los componentes de una infraestructura tecnológica, tanto en la conectividad como en las plataformas de hardware y software. El internet es el servicio más vulnerable dentro de un IT, ya que es el camino abierto para cualquier vulnerabilidad, ataque o denegación de servicio, ya

que este medio es la herramienta de comunicación de casi todos los servicios de una IT.

2.1.1.2 La Seguridad

El recurso más valioso dentro de una organización, ya sea esta pública o privada, es la información, lo que permite a una organización su desarrollo, ya que el producir, captar, generar y utilizar correctamente la información generan un valor agregado en beneficio de la organización, cumpliendo con los requisitos de confidencialidad, integridad y disponibilidad.

El acelerado crecimiento de la información ha generado un acelerado crecimiento de las vulnerabilidades informáticas en las empresas y los robos de la información han evidenciado actualmente una crisis que no es desconocida, y es que la sofisticación de los atacantes cibernéticos ha permitido filtrar y robar información que pone en riego los servicios informáticos y deja en duda la reputación de las empresas.

La seguridad de la información es el plan de acción para evaluar las amenazas y minimizar los riesgos, bajo normativa o buenas prácticas. Mientras que la seguridad informática son las implementaciones o soluciones técnicas para proteger la información (Computerworld, 2015).

Por esta razón, el camino correcto para alcanzar una seguridad informática es mediante un esquema de seguridad de la información que abarca tecnologías de última generación y de alto rendimiento hechos para precautelar y salvaguardar los datos.

La seguridad hoy en día es una tarea diaria, debido a que la evolución de los ciberdelincuentes avanza a medida que avanzan las diferentes tecnologías de seguridad, a raíz de esto, la importancia de proteger la información sensible cada vez es mayor, tomando en cuenta la sensibilidad de la información que se maneja diariamente en una organización.

2.1.1.3 Tecnologías de Seguridad

Actualmente existen tecnologías de última generación que permiten proteger los perímetros, las plataformas internas, los dispositivos móviles y los procesos de negocios, todos ellos con plataformas de correlación de eventos de seguridad monitoreados, que protegen la información y la infraestructura que la soporta, de tal manera que garantizan su disponibilidad, integridad y confidencialidad.

Tecnologías de alto rendimiento proporcionan un conjunto de funciones entre la seguridad y establecimientos de red, bajo plataformas de seguridad de red de alto rendimiento que entregan una seguridad de nueva generación con rendimientos excepcionales, tiempo de espera muy bajos y protección contra amenazas multi-vector.

Ilustración 2. (Fortinet, 2015). Tecnologías de Seguridad

2.1.1.3.1 Control de Aplicaciones

Tecnología que bajo políticas de seguridad permite identificar, bloquear o limitar el uso (ancho de banda o tiempo) de aplicativos, servicios web, redes sociales, puertos independientes, protocolos o técnicas evasivas utilizadas para penetrar la red, adicional a esto, esta tecnología de seguridad tiene la capacidad de escanear y encriptar trafico SSL seguro, brindando la posibilidad de inspeccionar y proteger el contenido.

2.1.1.3.2 Anti Malware

Método por el cual se detecta y elimina malwares eficientemente, usando firmas para identificar el malware (virus, spyware, keystroke, loggers, trojans y rootkits) mediante un escaneo sobre el dispositivo. Este tipo de herramienta protege y previene la infección del dispositivo final.

2.1.1.3.3 Firewall

Es una fusión avanzada de tecnologías de software y hardware que comprueba y detiene el tráfico de datos sospechoso o maliciosos que intenta ingresar a la red interna, generalmente procedente de Internet, redes WAN o red WLAN. Un firewall es la base fundamental e ideal para la protección y prevención de una infraestructura de seguridad de red.

Convirtiéndose en un sistema de seguridad de red que controla el ingreso y la salida de tráfico, basándose en un conjunto de reglas definidas para precautelar y salvaguardar los datos de una organización.

2.1.1.3.4 Filtro Web

Software dedicado a restringir sitios web, los cuales poseen contenido malicioso o información restringida, los cuales son categorizados en base a las políticas de seguridad que se definan dentro de una organización para la navegación en Internet, este software es capaz de verificar la URL, contenido, firmas y ejecutables de un sitio web.

2.1.1.3.5 Anti Spam

Tecnología basada en software que brinda protección a la infraestructura de mensajería y correo electrónico interna y externa de una organización, previniendo y defendiendo de una gran variedad de amenazas provenientes del correo electrónico. Posee la facilidad de analizar el contenido del correo electrónico y mensajería e identificar la amenaza antes de ser ejecutada, siendo capaz de retener el mensaje o ser bloqueado antes de que ingrese a la infraestructura de correo electrónico.

2.1.1.3.6 Optimización WAN

Es una solución cuyo objetivo es mejorar el rendimiento de redes hibridas, para la entrega acelerada de paquetes que se transmiten en la red, a través de mecanismos de selección basados en políticas centralizadas y priorizadas según la necesidad u operatividad del negocio. Permite la reducción de costes de infraestructura y ancho de banda, mejora y brinda mayor protección de los datos.

2.1.1.3.7 Optimización de Tráfico

Es una solución que proporciona visibilidad del tráfico de la red, y además permite administrar con eficiencia políticas de QoS que permiten configurar límites de ancho de banda para el tráfico de red, y así garantizar una asignación equitativa de ancho de banda, brinda un panorama preciso del tráfico de red en tiempo real, facilitando la supervisión y medición; y al mismo tiempo limita el impacto del tráfico no deseado hacia la red mejorando

el rendimiento y los tiempos de respuesta, identifica trafico comprimible y aplica tecnológica de compresión, facilitando el trabajo de la red.

2.1.1.3.8 VPN

Software que provee la seguridad necesaria para el acceso a una red privada o pública y a los recursos o servicios que trabajan remotamente, la privacidad y confidencialidad de la información la maneja a través de protocolos especiales basados en TCP/IP, encapsulación y autenticación, todas estas características las reúne y la información viaja de forma segura y protegida a través de redes privadas o públicas.

2.1.1.3.9 IPS

El sistema de prevención de intrusos es una fusión de hardware y software que protegen la información de ataques avanzados sin afectar la productividad y rendimiento en tiempo real y en línea, realizando una continua limpieza del tráfico de red al tomar decisiones de control de acceso en base al contenido del tráfico, firmas y políticas establecidas según la operatividad de la organización y el nivel de seguridad que se desea implementar.

2.1.1.3.10 DLP

Software de detección, supervisión y protección de la información sensible tanto dentro como fuera de la red de la organización, entornos móviles y cloud, contra la fuga o el robo de la información, de forma más completa y

efectiva, extendiendo las políticas de seguridad y cumplimiento más allá de las fronteras de la red organizacional en tiempo real.

2.1.1.3.11 Controlador WIFI

Conjunto de hardware y software que permiten gestionar y administrar el servicio de wifi de una organización, es el medio por el cual se aplican políticas de seguridad y acceso para el servicio de wifi tanto para la red interna como para internet. Este tipo de solución permite limitar el acceso de los dispositivos móviles a la red interna de la organización para detener cualquier tipo de amenaza.

La información se ha vuelto un potencial riesgo que toda empresa u organización privada o pública debe proteger. En este aspecto la información se vuelve el activo más importante que está íntimamente ligado al cumplimiento del conjunto de requisitos de confidencialidad, integridad y disponibilidad.

Aprovechar bien de las tecnologías de la información y comunicación logran cambios importantes y aumentan la competitividad de la organización, pero también aumentan los riegos y amenazas a los factores de origen humano, tecnológico y físico, los cuales abren brechas sensibles por las cuales pueden atentar contra la confidencialidad, integridad y disponibilidad.

2.1.1.4 Acciones y Procedimientos de seguridad

La clave para mantener una infraestructura tecnológica segura es la prevención y detección. Para esto existen diversas acciones o procedimientos que se deben implementar dentro de la empresa, las cuales complementan y refuerzan la seguridad de una empresa.

El aumento de la seguridad de los empleados, es una acción clave dentro de un esquema de seguridad interno para el éxito del mismo. Más del 60% de incidentes se generan internamente, producto de los errores y descuidos de los empleados. Se debe crear una cultura y plan de seguridad interna que se cumpla, inclusive con asesoría especializada externa que garantice el cumplimiento de la acción y actualizada.

Que hacer antes, durante y después. Es imprescindible disponer de un procedimiento de contingencia ante cualquier evento que afecte a la seguridad de la empresa, donde los empleados son el principal protagonista, integrando soluciones tecnológicas y estrategias de recursos humanos. Entre más rápida y mejor sea la respuesta ante una eventualidad, más rápido se solucionará.

Con la proliferación de la tecnología inteligente, se debe pensar en la forma de controlar estos dispositivos que forman parte de la cotidianidad laboral de los empleados, más allá de las estaciones de trabajo, se vuelven una herramienta indispensable dentro de una empresa. Para ello se requiere de una acción para el seguimiento de accesos.

Protección de los datos, procedimientos para la entrega cautelosa de información, es vital dentro de la empresa. Estos procedimientos dependiendo de la criticidad de la

información deben venir acompañados con acuerdos de confidencialidad que especifiquen su uso y que sean firmados por los empleados que usen esa información.

Organización empresarial inteligente. Es aquí donde se aplican procedimientos de almacenamiento y análisis de la información, los cuales permitan crear un registro y seguimiento de los datos que permitan evidenciar y alertar un comportamiento sospechoso dentro de la empresa.

2.1.1.5 Políticas y Normas de Seguridad

Las políticas y normas de seguridad ayudan a una organización a proteger y mantener los recursos y servicios de la misma, así como también garantizar que la información este protegido, y así la integridad, la confidencialidad y la disponibilidad de esta, minimizando los riesgos y las amenazas a la privacidad de los datos o amenazas a la seguridad, las cuales pueden traer efectos negativos para la organización.

Una política de seguridad es la definición de las reglas a seguir para acceder a la información, así como también, a las herramientas que la contiene; Las normas pasan a ser un complemento para el cumplimiento de una política, las cuales contienen recomendaciones, controles y lineamientos a seguir, con el objetivo de cumplir la política.

Una política de seguridad debe cumplir un objetivo específico, es decir, la protección de la información y la infraestructura que la soporta, de tal manera que garantice su

disponibilidad, integridad y confidencialidad, mediante los mecanismos correctos para hacerlo.

El estándar RFC2196 para la práctica de la seguridad de la información (Piraquive, 2008), establece algunos aspectos a tomar en cuenta en la constitución de las políticas de seguridad.

- **Políticas de privacidad. -** Definen aspectos relacionados a: filtrado de contenido web y control de aplicaciones, correo electrónico, acceso a archivos, telefonía, mensajería, etc.
- **Políticas de acceso. -** Definen aspectos relacionados a: Acceso de dispositivos externos, privilegios y derechos de acceso a información, software externo, comunicación interna de la información, acceso de usuarios internos y externos a recursos de la información, etc.
- **Políticas de responsabilidad. -** Definen responsabilidades de los usuarios, administradores, operadores y otro personal, en base a sus funciones y competencias.
- **Políticas de autenticación. -** Se establecen mecanismos de autenticación de acceso seguro, tiempos de vigencia y generación de claves.
- **Políticas de mantenimiento (hardware y software). -** Definen acciones sobre el mantenimiento tanto del software como del hardware, autores externos e internos, accesos internos y externos, mecanismos de control, etc.
- **Políticas de informes de incidentes o violaciones de seguridad. -** Definen las acciones a realizar e informar.

- **Políticas de adquisición. -** Definen pautas apegadas a un modelo de gestión para la adquisición de tecnología.
- **Información de apoyo. -** Ayuda a los usuarios, administradores, operadores y demás, con información de contacto, referencia y aspectos legales a tomar en cuenta ante una incidencia de seguridad.

Para que una política pueda ser ejecutada dentro de una organización requiere de la aprobación de los directivos de la organización con el debido respaldo legal. Para alcanzar una amplia aceptación de una política es importante que esta sea revisada y analizada por un grupo de personas que cumplen diferentes roles dentro de la organización, roles como: administrador, operador, usuario, abogado, auditor y especialista de hardware y software, ya que estos conocen y saben que se puede y que no se puede realizar, así como también las implicaciones legales.

(Piraquive, 2008) indica que una política debe ser lo bastante consistente para responder a las necesidades y al mismo tiempo simple para que no sea un obstáculo en el normal desarrollo de las actividades de la empresa o institución.

Para crear un esquema seguro dentro de la organización, se requiere de políticas estructuradas en base a elementos que se enfoquen en el manejo y acceso a la información, como:

- **Autenticación:** Elemento que identifica la identidad de quien use los recursos de la información.
- **Autorización:** Una vez identificado, este elemento da permisos a quien va a usar o no la información.

- **Integridad y confidencialidad:** Elemento que asegura la información, evitando cualquier alteración o divulgación en su contenido.
- **Acceso:** Elemento que determina los mecanismos adecuados y permitidos para acceder a la información.
- **Auditoria:** Elemento que permite el control de la información mediante el registro completo de las acciones realizadas sobre la información.

Existe una norma (ISO/IEC 27001:2005), que brinda un modelo para el establecimiento, implementación, operación, seguimiento, revisión mantenimiento y mejora de un sistema de gestión de seguridad de la información (SGSI). Esta norma establece los requisitos que debe cumplir cualquier organización que desee gestionar la seguridad de su información y demostrar a sus stakeholders (accionistas o inventores) que aplican el cuidado y protección de la información, cuyos pilares se pueden resumir en: Gestión de los Riesgos de seguridad de la información, código de prácticas de seguridad de la información y sistema de gestión (Computerworld, 2015).

Una política de seguridad es el pilar dentro de un SGSI ya que básicamente tiene que reflejar lo que se desea hacer con respecto a la seguridad de la información, tomando en cuenta los requisitos legales, los reglamentos aplicables, los compromisos y los objetivos a obtener.

Existe otro aspecto que debe ser tomado en cuenta, "la clasificación de la información" es el medio por el cual se evalúa la importancia de un activo de información, y el criterio que se maneja se basa en tres características:

- **Confidencialidad**
    - Información pública.
    - Información reservada de uso interno.
    - Información reservada confidencial.
    - Información reservada secreta.
- **Integridad**
    - Modificación no autorizada de la información, reparable y sin afectación.
    - Modificación no autorizada de la información, reparable con pérdidas leves.
    - Modificación no autorizada de la información, compleja reparación con pérdidas significativas.
    - Modificación no autorizada de la información, irreparable con pérdidas graves.
- **Disponibilidad**
    - Información inaccesible que no afecte las actividades.
    - Información inaccesible durante un periodo de tiempo (semanas), causando el paro de las actividades.
    - Información inaccesible durante un periodo de tiempo (días), causando el paro de las actividades.
    - Información inaccesible durante un periodo de tiempo (horas), causando el paro de las actividades.

La seguridad de la información se basa en la capacidad para preservar su integridad, confidencialidad y disponibilidad, por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como de los recursos humanos que utilizan dichos componentes (Oficina Nacional de Tecnologías de Información, 2005).

La política de seguridad del recurso humano ayuda a disminuir los incidentes por error humano y el uso no autorizado e inadecuado de los recursos y de la información. A sí mismo, garantiza que el recurso humano conozca sobre amenazas y a la vez se capacite en herramientas y mecanismos de prevención de incidentes, y se establezcan compromisos de confidencialidad con todo el recurso humano interno y externo.

La política de seguridad física involucra elementos como: instalaciones, equipamiento, cableado, medios de almacenamiento, seguridad perimetral, redes y comunicaciones, etc.; Donde la prevención a daños, la protección del equipamiento e impedimento de accesos no autorizados, bajo medidas de seguridad y controles definidos en la política, garantizan la integridad, confidencialidad y disponibilidad de la información.

Mobility, es el nuevo concepto de "trabajar en cualquier lugar", por medio de dispositivos inteligentes, en la actualidad es posible aplicar esta nueva forma de trabajo, pero al igual que cualquier elemento, están expuestos a amenazas de seguridad informática, por tal motivo, una política de seguridad mobility debe limitar el acceso de los dispositivos inteligentes a la red de la organización, y así, evitar y prevenir cualquier tipo de amenaza.

Cabe recalcar que la seguridad es un proceso continuo, donde se deben mejorar y reforzar las políticas de seguridad, para que estas puedan estar a la par con las nuevas amenazas que aparezcan.

Es necesario que los usuarios incorporen buenas prácticas para proteger el entorno de información, y prevenir aún más la posibilidad de formar parte del conjunto que engloba a las potenciales y eventuales víctimas de cualquiera de las amenazas, que constantemente buscan sacar provecho de las debilidades humanas. Pero para ello inevitablemente se deben conocer los peligros latentes, y cómo detenerlos a través de mecanismos de prevención (Mieres, 2009).

2.1.1.6 Buenas Practicas de Seguridad

"Seguridad de información es determinar que hay que proteger y por qué, de que se debe proteger y como protegerlo" (Piraquive, 2008).

La Implementación de soluciones de seguridad IT que supervise de manera continua la IT, brindan la capacidad de controlar y proteger de manera centralizada la infraestructura de TI, como también la facultad de responder de forma inmediata a cambios que pudieran quebrantar la seguridad IT.

La creación, actualización, el cumplimiento y una clara difusión a los usuarios, administradores y operadores de las políticas de seguridad, donde cada uno de ellos se comprometan a cumplir con las políticas de seguridad mediante una declaración en la cual indique que han leído, comprendido y que están de acuerdo en cumplir las políticas de seguridad, serán un valor agregado valioso para una IT.

Mantener un ambiente seguro no únicamente para el personal del área de seguridad o para el analista de seguridad. Todo el personal involucrado debe realizar un esfuerzo continuo para mantener un ambiente seguro dentro de la organización, cumpliendo y respetando las políticas de seguridad, llegar a sensibilizar a toda la organización sobre la importancia de la protección y seguridad de las TI.

El plan de acción en caso de una incidencia es de gran ayuda para identificar la naturaleza de este, el alcance, la afectación y los pasos lógicos a seguir para responder, contrarrestar y restablecer las condiciones normales, de una mejor manera a una incidencia. El manejo de incidencias debe ser preparado y planeado para evitar que estos ocurran, cabe indicar que es recomendable documentar esta información para una retroalimentación.

Un informe de IDG (International Data Group) sugiere 4 principios para mantener seguros los datos de una organización o empresa:

1) **Seguridad de los Empleados**

   Tener un plan y mantener una cultura de seguridad frente a los riesgos de que ocurra un incidente, aumenta la seguridad en los empleados de una organización, ya que el mayor porcentaje de incidencias de seguridad ocurren por errores internos.

2) **Prepararse para responder**

   Planificar qué hacer antes, durante y después de una incidencia es imprescindible, para una respuesta ágil y rápida ante el incidente. Contar con un plan de contingencia hace la diferencia al momento de evaluar el alcance

del incidente, y, sobre todo, el ejercicio de simulacros prueba y refuerzan las habilidades del equipo.

3) **Inventarios de Equipos**

   Debido a la proliferación de la tecnología personal, los dispositivos inteligentes personales se han convertido en una herramienta imprescindible y a la vez una amenaza interna latente, es primordial llevar un inventario para llevar un control en los accesos de estos dispositivos.

4) **Proteja Datos**

   Es importante crear un esquema de acceso y de responsables de la información, los cuales aseguren la confidencialidad de la información, y que esta sea cautelosamente entregada y especificando su uso mediante acuerdos de confidencialidad.

Las mejores prácticas para el manejo integral, estratégico y proactivo de la seguridad van alineadas a las necesidades de cada organización, sin embargo, existen recomendaciones de buenas prácticas aplicables para cualquiera que sea la necesidad.

a) **Objetivos del negocio. -** Una buena práctica de seguridad es analizar y determinar los objetivos, procesos, activos y datos indispensables para la organización, y así, enfocarse en proteger lo realmente crítico y definir las acciones a seguir en base a las metas y requerimientos de la organización.

b) **Mapa de Riesgos. -** La elaboración de un mapa de riesgos conlleva a analizar y determinar los riesgos y vulnerabilidades de la infraestructura tecnológica (IT), procesos y el personal de la organización, con el fin de establecer las amenazas y potenciales pérdidas ocasionadas.

c) **Plan estratégico de seguridad de la TI.-** Elaborar un plan de protección bajo estándares, metas y un ciclo de vida, todos alineados a los objetivos de la organización, y mantener paralelamente el fortalecimiento de la seguridad con la realidad de la organización.

d) **Políticas y lineamientos de seguridad. -** Definir e implementar políticas flexibles de seguridad con reglas y lineamientos del manejo de la información, estableciendo claramente las consecuencias y sanciones en caso de no cumplirlas, tanto para usuarios internos como usuarios externos.

e) **Capacitación. -** La concientización sobre la importancia de cumplir y hacer cumplir las políticas (reglas y lineamientos), capacitar sobre los riesgos, vulnerabilidades y amenazas, como las potenciales consecuencias para la organización, dando prioridad al personal de mayor riesgo, es decir, al personal que maneja la información y activos más críticos.

f) **Equipo de Seguridad. -** Conformar un equipo de especialistas en seguridad de la IT es una buena práctica, ya que estos serán los encargados de fomentar el desarrollo de la seguridad en la organización, como también, el cumplimiento de las políticas de seguridad. También es recomendable y considerado como una buena práctica de seguridad, que se constituya un comité de seguridad, en el cual intervienen representantes de las diferentes áreas y el equipo de seguridad de la organización, y en conjunto analizar, definir y proteger los elementos más importantes.

g) **Aplicaciones Seguras. -** Las aplicaciones que maneja la organización ya sean estas desarrolladas internamente o externamente, deben cumplir con los lineamientos de seguridad necesarios para cubrir las brechas de seguridad que

podrían convertirse en el blanco para cualquier tipo de amenaza. La colaboración e intervención del comité de seguridad es indispensable para delinear temas de seguridad y probar las aplicaciones en la IT.

h) **Outsoursing. -** Aplicar controles a los procesos o actividades de outsoursing no está por demás, ya que "la seguridad no empieza y termina dentro de organización, viene desde los proveedores y abarca a los clientes" (Netmedia, 2016).

i) **Evaluar Niveles de seguridad. -** El avance del plan estratégico de seguridad debe ser medido mediante métricas definidas por el comité de seguridad que permitan evaluar los procesos, políticas, usuarios, la IT y el cumplimento de las metas propuestas en el tema de seguridad, y darle el respectivo seguimiento.

j) **Plan de Acción. -** Definir y establecer un plan de continuidad para el negocio en caso de desastres, en el cual se considere factores como: recuperación de información, sistemas de contingencia física y lógica, impactos, respaldo de la información, niveles de servicios, tiempos de tolerancia, personal calificado, entre otros; Debido a su importancia y criticidad, el plan de acción debe ser primordial e indispensable dentro de una organización que se preocupa de la seguridad de las TI.

2.1.2 Vulnerabilidades de una Infraestructura Tecnológica

La revista (Computerworld, 2015) indica que en la actualidad nadie se salva de caer en la trampa y contraer un virus que infecte su sistema informático personal o empresarial.

2.1.2.1 Vulnerabilidades

Es muy importan dentro de la administración de la IT, realizar una evaluación de las principales amenazas y vulnerabilidades relativas a la información y a las instalaciones, la probabilidad de que ocurra algún incidente y el impacto en la operación de la organización. Con esto identificar, controlar, mitigar, minimizar o eliminar los riesgos en la IT y principalmente garantizar la integridad, confidencialidad y disponibilidad de la información.

(Ayala G. & Gómez, 2011) Desde el punto de la vulnerabilidad de la información, la definen como:

- **AMENAZA:** Acción o evento que puede ocasionar consecuencias adversas en los datos.
- **ATAQUE:** Tipo y naturaleza de inestabilidad en la seguridad.

Las vulnerabilidades se derivan de factores técnicos, organizacionales y ambientales, las cuales pasan a ser una amenaza latente y abre la posibilidad de que ocurra cualquier tipo de evento o acción que puede producir daños irreversibles en la IT y la información. Las vulnerabilidades deben ser catalogadas de acuerdo a su nivel de criticidad como alto, medio y bajo, con el fin de priorizar la acción a realizar.

2.1.2.2 Amenazas

Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (Symantec, 2016).

Entre las amenazas más frecuentes tenemos:

- **INGENIERIA SOCIAL. -** Conocida como la suplantación de identidad.
- **PHISHING. -** Uso de sitios web falsos.
- **PHARMING. -** Redirección de servicios o sitios web a sitios falsos.
- **MALWARE. -** Software con código malicioso para recolectar información o denegación de servicio.
- **MAN IN THE MIDDLE. -** En el cual interviene un hacker entre la comunicación de las partes involucradas.
- **MAN IN THE BROWSER. -** Hacker que manipula el navegador para ocultar información.

El malware empresarial se ha convertido en la amenaza más popular de los últimos años, entre estos están los códigos maliciosos como botnets y ransomware. Sin embargo, el único objetivo de este tipo de amenaza es generar ganancias económicas para los atacantes, mas no, en causar daños como lo hacían antes, mediante el:

- Robo de información
- Secuestro de información
- DDoS (denegación de servicios).

Entre los medios de propagación tenemos:

- Dispositivos externos
- Correo electrónico
- Puertas de acceso
- Internet, etc.

Botnets. - Conjunto de equipos bajo el control de un bot maestro, a través de un canal de mando y control. Estos equipos normalmente se distribuyen a través de Internet y se utilizan para actividades malintencionadas, como el envío de spam y ataques distribuidos de negación de servicio. Las botnet se crean al infectar las computadoras con malware, lo cual da al atacante acceso a las máquinas. Los propietarios de computadoras infectadas generalmente ignoran que su máquina forma parte de una botnet, a menos que tengan software de seguridad que les informe acerca de la infección (Symantec, 2016).

Ransomware. - Tiene un sistema novedoso que infecta el sistema y cifra los archivos para exigir un pago como rescate, generando un secuestro de datos (Computerworld, 2015).

En la actualidad existen nuevas tendencias en temas de amenazas, en los cuales se centralizarán las amenazas, temas como: IoT (Internet de las cosas), crimeware y BYOD (Bring Your Own Device).

- Un blanco fácil y vulnerable es la tendencia del IoT, el cual con el transcurrir de los días, se unen más y más objetos (dispositivos, aparatos, electrodomésticos, etc.) inteligentes a las redes mundiales (internet), permitiendo el intercambio de información y a la vez abriendo brechas vulnerables para la IT.
- BYOD método de conexión cada vez más popularizado dentro de las organizaciones, para brindar flexibilidad laboral, pero a la vez, una gran amenaza a la infraestructura tecnológica de la organización, si no se toman las medidas y mecanismos de protección necesarios.
- Crimeware es llamado así a todo el ámbito que engloba los crímenes cibernéticos, donde, se usa herramientas de software nocivos para cometer un acto criminal.

Existes nuevas tecnologías que permiten detectar, mitigar y prevenir amenazas, La BIG DATA es una nueva opción de seguridad de la información, esta herramienta permite procesar y analizar grandes volúmenes de información, donde:

- Captura y procesa datos de servicios y dispositivos de la red empresarial.
- Visualiza los flujos de datos para identificar eventos y movimientos sospechosos o información alterada.
- Aplica técnicas de aprendizaje automáticos para identificar nuevos eventos de seguridad y alertar sobre estos.

2.1.2.3 Ataques

Un ataque es el método por el cual se puede aprovechar una vulnerabilidad de la infraestructura tecnológica (hardware y software) y el RR-HH que opera o tiene acceso a él.

(Netmedia, 2016) Señala que, según los expertos, habrá un claro aumento en el uso de malware y ataques híbridos, donde empleados deshonestos ayudarán a que programas maliciosos puedan evadir los sistemas de seguridad de las empresas, Otro de los aspectos a considerar, será el surgimiento de ataques más complejos de ransomware, donde el desafío se encuentra en cómo garantizar la disponibilidad de la información, además de la detección y eliminación de este tipo de ataques.

MALWARES. - Es el software malicioso que puede ocasionar diferentes tipos de daños al objeto infectado, que dependerán del tipo de malware, de la función y actividad del malware, rutinas de propagación, la clase del objeto

infectado, de la naturaleza de los datos almacenados en el objeto y del acceso a este.

(Kaspersky Lab, 2016) Clasifica a los malwares de la siguiente manera, donde los tipos de comportamiento que plantean la menor amenaza se muestran en el área inferior del diagrama y los tipos de comportamiento que plantean una amenaza mayor se muestran en el área superior del diagrama.

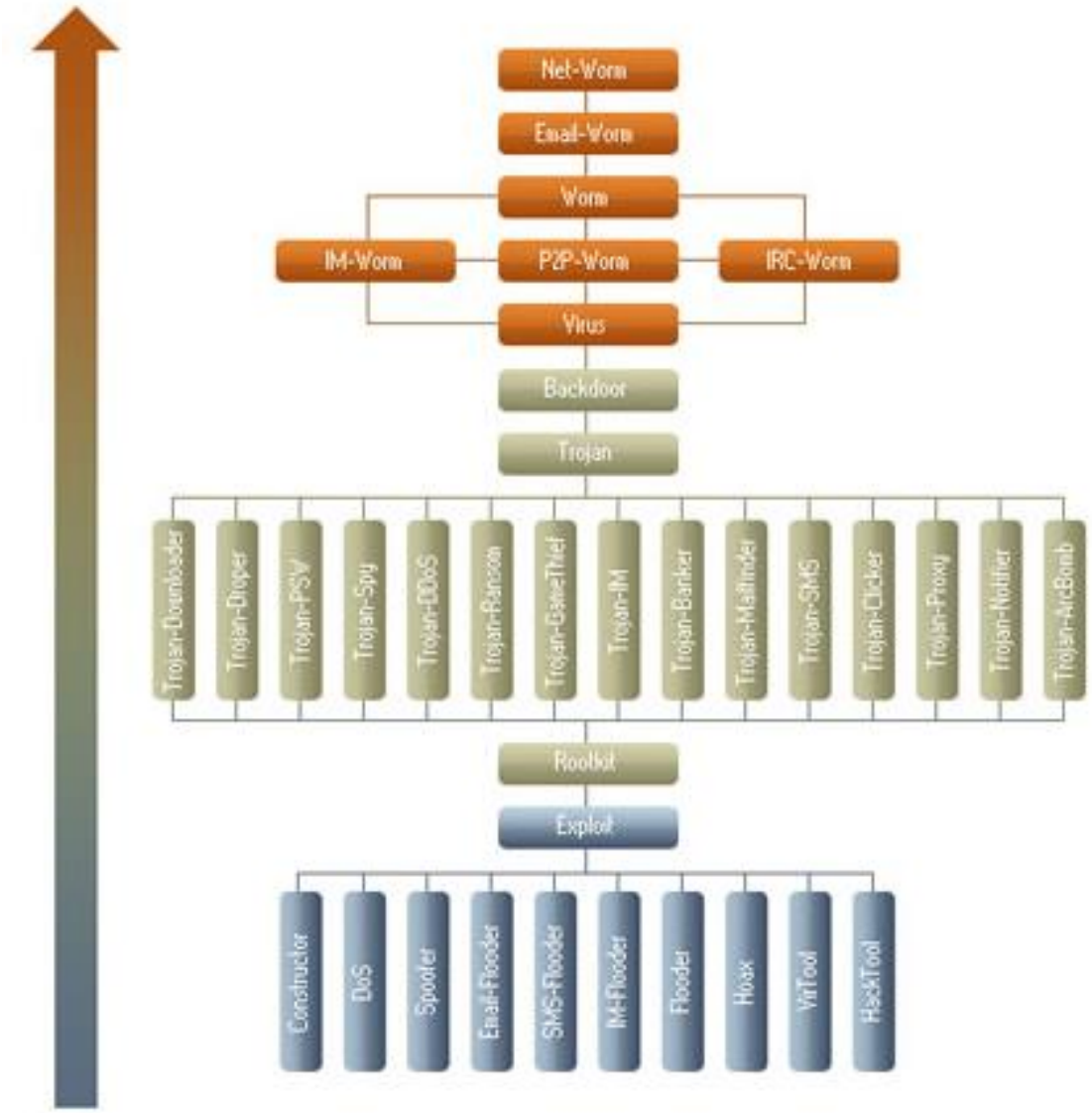

Ilustración 3. (Kaspersky Lab, 2016). Amenazas de seguridad en Internet.

ZERO-DAY. - Conocido también como ataque ZETA o día cero, su función consiste en atacar una vulnerabilidad de un sistema antes de que este sea conocido por su creador, el ataque es realizado el mismo día en que fue informada la vulnerabilidad, por diferentes medios por los usuarios del sistema.

Ataques híbridos. - Este tipo de ataques son unas combinaciones letales para una organización ya que son producidas con la ayuda del personal de la organización, una fusión de malware y usuario interno, aumentan a gran escala la efectividad del ataque, evadiendo así cualquier tipo de seguridad sin ser detectado.

DDOs. - Los ataques de red distribuidos a menudo se conocen como ataques de denegación distribuida de servicio (DDoS). Este tipo de ataque aprovecha los límites de capacidad específicos que aplican a cualquier recurso de red, estos recursos de red tienen un límite finito de cantidad de solicitudes que pueden atender al mismo tiempo. Además del límite de capacidad del servidor, siempre que la cantidad de solicitudes sobrepase los límites de capacidad de cualquiera de los componentes de la infraestructura, evitará el funcionamiento normal del recurso, causando una "denegación" total del servicio (Kaspersky Lab, 2016).

(Netmedia, 2016) Señala siete directrices para minimizar y erradicar los ciberataques, o para saber cómo actuar ante esto.

1) **Establecer prioridades. -** Analizar y detallar los principales servicios de una organización para determinar el nivel de tolerancia ante riesgos, para que en el momento en que se produzca un ciberataque, los servicios de menor riesgo para la organización puedan ser suspendidos, evitando así la expansión del ataque, evitando un mayor impacto en la organización.
2) **Establecer el mando. -** Es imprescindible designar el grupo de personas que llevaran la rienda y toma de decisiones durante un ciberataque en base al plan de acción.
3) **Tomar medidas holísticas. -** Asegurarse de que cada cosa este en su sitio, es decir, que la organización cuente con personal, equipamiento, políticas de seguridad, procesos, etc., para que la IT y los datos estén seguros.
4) **Equipo externo de análisis. -** Tener un apoyo externo no está por demás si lo que deseamos es minimizar y erradicar los ciberataques, un equipo externo capaz de manejar y analizar un incidente.
5) **Manejo de casos. -** La confidencialidad y la integridad de la evidencia de un ataque, es un tema que debe ser manejado de forma adecuada y más si este se deriva en acciones legales.
6) **Enfoque en los hallazgos. -** Ajustar y acelerar el ciclo OODA: observar, orientar, decidir y actuar, utilizando personas, procesos y tecnología para ser más rápidos que los atacantes.
7) **Reunión. -** La evaluación y análisis del ataque por parte del equipo responsable es parte vital para evitar una incidencia similar.

2.1.2.4 Riesgos

La identificación de riesgos dentro de una infraestructura tecnológica es esencial para minimizar amenazas y ataques, la evaluación de cada uno de los riesgos permite medir el impacto que este puede tener para la organización y ayudan a priorizar el riesgo a mitigar.

Con el creciente panorama de amenazas y ataques que enfrentan las organizaciones a su infraestructura tecnológica y a la información, ponen en riesgo la estabilidad, integridad y disponibilidad de los servicios e información de la organización.

El principal riesgo de una organización son sus propios empleados, debido a que practican hábitos inseguros de seguridad, los cuales ponen en riesgo a ellos mismos y a la organización. La falta de una cultura segura dentro de la organización conforma el complemento perfecto para que los mismos empleados abran brechas de seguridad por el desconocimiento de la misma.

2.1.2.4.1 Administración de Riesgos

(TIC, 2015) Señala que es importante preparar a la organización para eventos de riesgos, para que ayuden a tomar medidas y decisiones correctas durante una incidencia. Para esto es necesario determinar y analizar los siguientes aspectos:

- Determinar y definir los procesos de la organización como:
    - Procesos de alto impacto.
    - Procesos de mediano impacto.
    - Procesos de bajo impacto.

- Identificación y categorización de los riesgos:

Categoría	Descripción
Gestión	Riesgos relacionados con la ausencia o aplicación incorrecta de métodos de gestión de las tecnologías de información y comunicaciones.
Operación	Incumplimiento de políticas, directrices, procedimientos y metodologías y estándares en los procesos operativos de la organización
Infraestructura	Riesgos relacionados con las fallas potenciales de la infraestructura tecnológica utilizada por la organización.
Seguridad	Eventos que atentan contra la confidencialidad, integridad y disponibilidad de la información.
Recurso humano	Relacionados con el desempeño y regularidad de los recursos humanos.

Tabla 1. (TIC, 2015) Evaluación de Riesgos en Tecnologías de Información.

- Determinar criterios de evaluación de los riesgos.

a) Probabilidad

- Casi seguro.
- Muy probable.
- Probable.
- Poco probable.
- Raro

b) Impacto

- Mayor
- Importante
- Significativo
- Regular
- Menor

c) Severidad

- Extrema
- Alta
- Moderada
- Baja

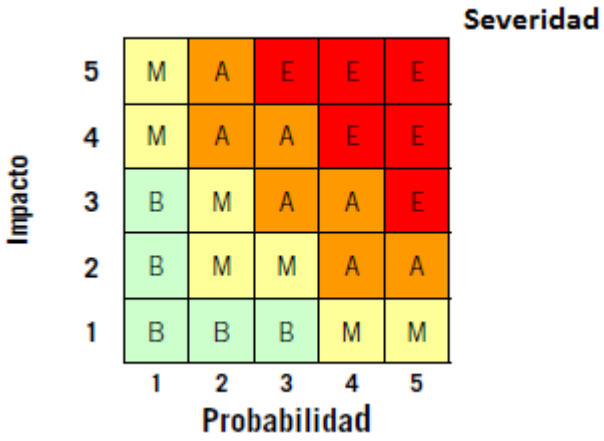

Ilustración 4. (TIC, 2015) Evaluación de Riesgos en Tecnologías de Información.

2.1.2.5 Intrusos, Hackers o Atacantes

Un hacker es un individuo que intenta obtener acceso sin autorización a un sistema computacional. Dentro de la comunidad de hackers, el término cracker se utiliza con frecuencia para denotar a un hacker con intención criminal, aunque en la prensa pública los términos hacker y cracker se utilizan sin distinción. Los hackers y los crackers obtienen acceso sin autorización al encontrar debilidades en las protecciones de seguridad y los sistemas computacionales (Piraquive, 2008).

Sin embargo los hackers también son considerados también como individuos que investigan el funcionamiento de los sistemas sin intensiones delictivas, con amplios

conocimientos de informática e Internet, incluso dedican su habilidad para tapar vulnerabilidades de la infraestructura tecnológica.

El evadir las seguridades implementadas en las organizaciones en su infraestructura tecnológica, y el acceso a información confidencial sin autorización, ha cambiado la reputación de estos individuos, y sus acciones se consideran como un delito. A pesar de que no produzca ningún daño en los sistemas y redes informáticas, las actividades de un hacker comprometen sistemas e infraestructuras tecnológicas, dejan "backdoors" que pueden ser aprovechados por aquellos individuos "crackers" que buscan hacer daño o simplemente obligan a la organización a dedicar más tiempo y recursos en detectar y recuperar lo comprometido.

Los llamados crackers motivados por intereses económicos, políticos o religiosos atacan infraestructuras tecnológicas o sistemas informáticos para causar daños, y sacar ventaja de forma ilegal.

Entre las herramientas y medios más usados por los hackers o crackers tenemos:

- Internet
- Scaners de puertos.
- Sniffers
- Exploits
- Backdoors kits
- Rootkits
- Redes de telecomunicaciones
- Auto-rooters

- Password crackers
- Técnicas de spoofing
- Herramientas de cifrado y protocolos criptográficos.

CAPÍTULO 3

MUNICIPIO DEL DISTRITO METROPOLITANO DE QUITO

3.1 Infraestructura Tecnológica del MDMQ.

3.1.1 Generalidades

3.1.1.1 Misión

Es un órgano de gobierno que actúa como facilitador de los esfuerzos de la comunidad en la planificación, ejecución, generación, distribución y uso de los servicios que hacen posible la realización de sus aspiraciones sociales (Rodas, 2014).

3.1.1.2 Visión

Quito ciudad de futuro, viva, alegre, incluyente, integrada, mezclada, activa, conciliadora, solidaria, segura y a la altura de todos los quiteños. Una ciudad en la que se puede vivir mejor (Rodas, 2014).

3.1.1.3 Servicios

El Municipio del Distrito Metropolitano de Quito actualmente atiende a más de 6000 usuarios internos, distribuidos por diferentes dependencias, y brinda sus servicios aproximadamente al 60% de la población de todo el Distrito Metropolitano de Quito, servicios como: servicios web, zonas wifi gratuitas, puntos de atención a los contribuyentes, puntos de recaudación, servicios a entidades públicas y entidades bancarias, entre otros.

Uno de los servicios que presta el MQMD a la población es el de recaudación, considerado como el servicio más crítico para el municipio, debido a que a través de este, el MDMQ financia el presupuesto, con el cual se podrá ejecutar el plan operativo anual, servicio que debe ser cuidadosamente planificado y ejecutado, bajo medidas de seguridad de la información, que garanticen la integridad y confidencialidad de la información, así como la disponibilidad del servicio.

Sin embargo el servicio de zonas wifi gratuitas de Internet, comparte la misma criticidad ya que a través de este servicio todos los ciudadanos tendrán acceso gratuito a internet inalámbrico a través de una red municipal implementada en parques y plazas más concurridos, en cada barrio y parroquia, estaciones de bus del Sistema de Transporte Público Metropolitano, etc..

Gran parte de la infraestructura tecnológica está enfocada a brindar servicios web, a través de los cuales, los ciudadanos pueden realizar los pagos y trámites relacionados al Municipio de Quito.

3.1.2 Infraestructura Tecnológica

3.1.2.1 Infraestructura de Red

La infraestructura de red del MDMQ está dividida en 4 partes: Infraestructura LAN, infraestructura Cloud, infraestructura Wireless infraestructura WAN e Internet, las cuales contemplan diferentes esquemas de conectividad, esquemas basados en la ubicación geográfica, distancias, servicios, edificación, accesibilidad, distribución de estaciones de trabajo, distribución de los racks de comunicación, etc., de las

diferentes administraciones zonales, empresas metropolitanas, secretarias, agencias, institutos y otras dependencias.

Toda la infraestructura de red que posee el MDMQ, se concentra en un solo punto, el cual sostiene toda la comunicación hacia todos los puntos internos y externos de la red municipal. Este punto central tiene un NOC (Network Operation Center), el cual cuenta con equipamiento, elementos y características de un centro de datos (datacenter).

3.1.2.1.1 Infraestructura WAN

El MDMQ posee una infraestructura externa muy peculiar, debido a que la mayor parte de sus dependencias se encuentran distribuidas en un mismo sector, donde el esquema de conectividad implementado posee un cierto grado de complejidad.

Debido a que las diferentes dependencias del MDMQ se encuentran cercanas, y para conectarlas entre ellas, se implementó una red en estrella de fibra óptica a 1GB, donde el concentrador principal se encuentra en el NOC, pero la red en estrella se concentra en un punto central entre estas dependencias, y está a la vez se comunica al NOC a través de un enlace punto a punto de fibra entre estos; cabe recalcar que esta red fue implementada entre las dependencias que en ese entonces existían (Ilustración 5).

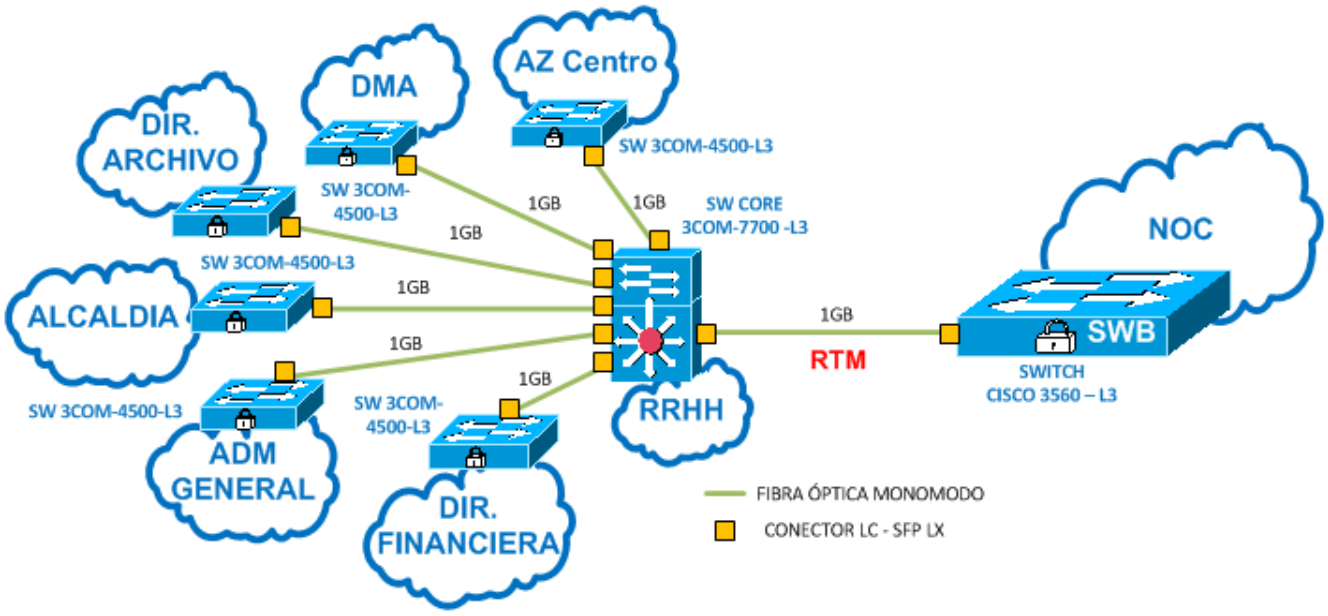

Ilustración 5. (López, 2015) Red en Estrella de Fibra Óptica.

El constante crecimiento y desarrollo del MDMQ y la demanda que los ciudadanos generan, llevó a que se constituyan más dependencias, permitiendo descentralizar áreas claves del municipio y así brindar un mejor servicio a los contribuyentes o ciudadanos del distrito metropolitano de quito.

Por este motivo, el MDMQ implementó un nuevo esquema de conectividad para comunicar las nuevas dependencias y centralizar la comunicación en el NOC, y a través de esto comunicar a todas las dependencias entre ellas. Bajo este objetivo, se construye un esquema de red en anillo en fibra de 1GB, entre todas las dependencias restantes. Adicional a esto también se pensó en reforzar (backup) la comunicación en las dependencias más críticas para el MDMQ, como una medida de contingencia si la red en estrella falla. El esquema de conectividad contempla el uso de protocolos de enrutamiento dinámicos y estáticos (Ilustración 6).

Adicionalmente hay que notar que, dentro de la red en anillo, existen expansiones en la conectividad, debido a que se han creado más dependencias a partir de la implementación del esquema de conectividad, estas expansiones, son creadas baso un esquema en cascada con similares condiciones en cuanto a velocidad y tecnología (Ilustración 6).

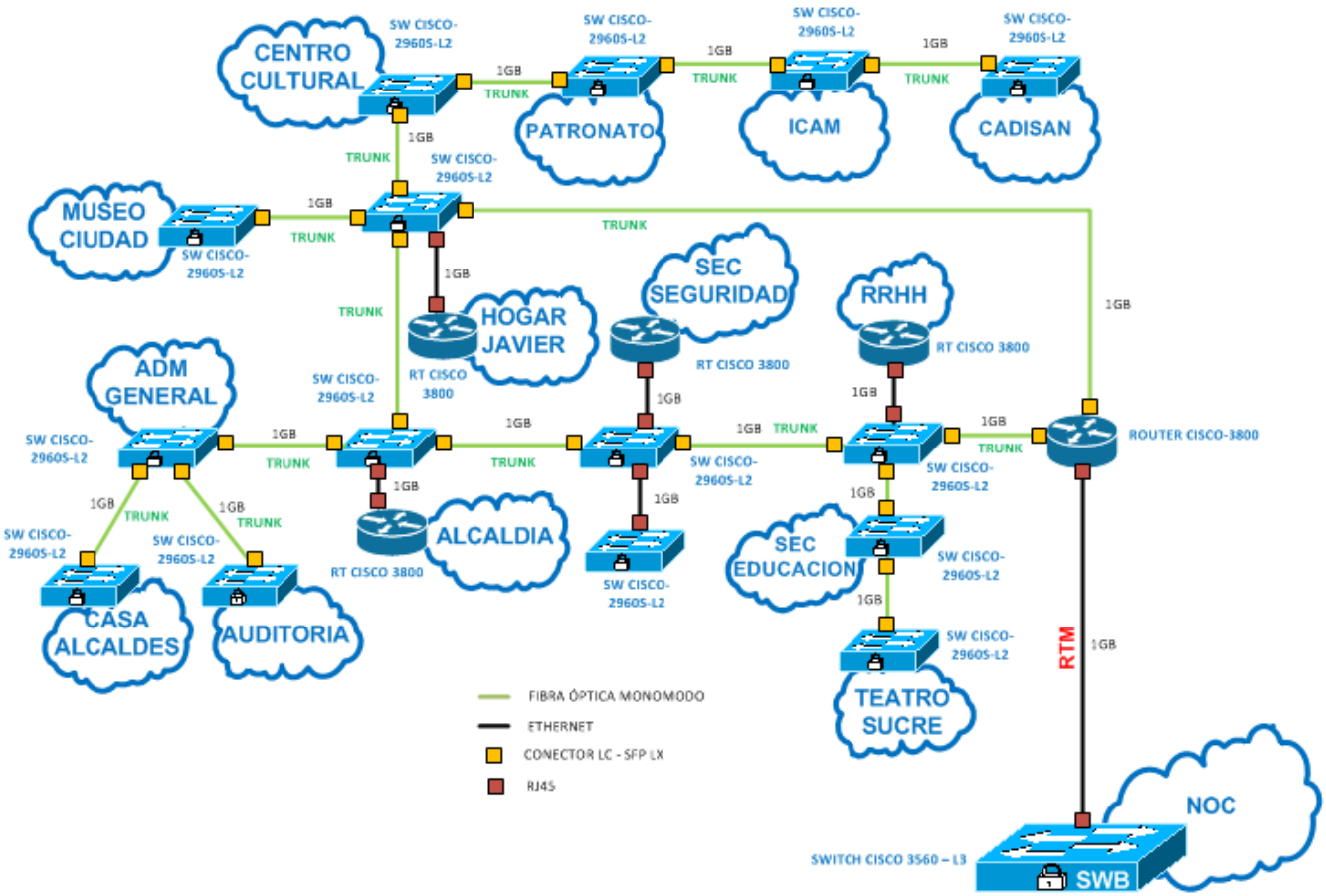

Ilustración 6. (López, 2015) Red en Anillo de Fibra Óptica.

En cuanto a las dependencias que se encuentran en diferentes posiciones geográficas del distrito metropolitano de Quito, el MDMQ maneja alrededor de 200 enlaces de datos con un solo proveedor de servicio de enlace de datos, el cual concentra a todas

estas dependencias en el NOC del MDMQ, estos enlaces punto a punto cuentan con diferente tecnología, protocolos de enrutamiento y capacidades, las cuales dependen de varios factores establecidos por el MDMQ y los alcances del proveedor (Ilustración 7).

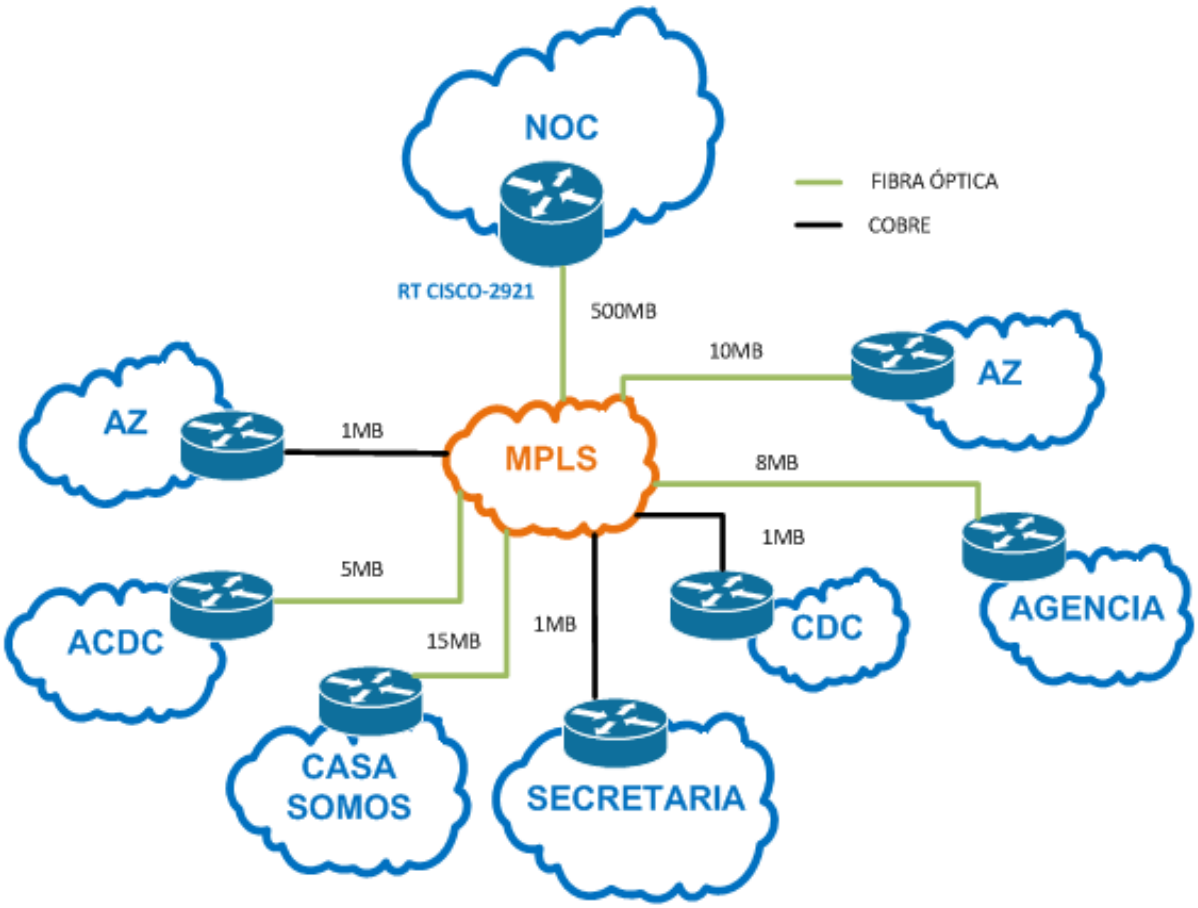

Ilustración 7. (López, 2015) Arquitectura de los Enlaces de datos.

Para la conectividad entre empresas públicas, privadas o instituciones bancarias, se aplica el mismo esquema de conectividad, los diferentes enlaces de datos son implementados a través del proveedor del servicio de datos que maneje la entidad externa, donde las características de estos enlaces dependen de cada entidad y alcance del proveedor del servicio de datos (Ilustración 8). Generalmente el MDMQ

llega a acuerdos con las entidades externas para tener un respaldo legal de la conectividad hacia las entidades externas.

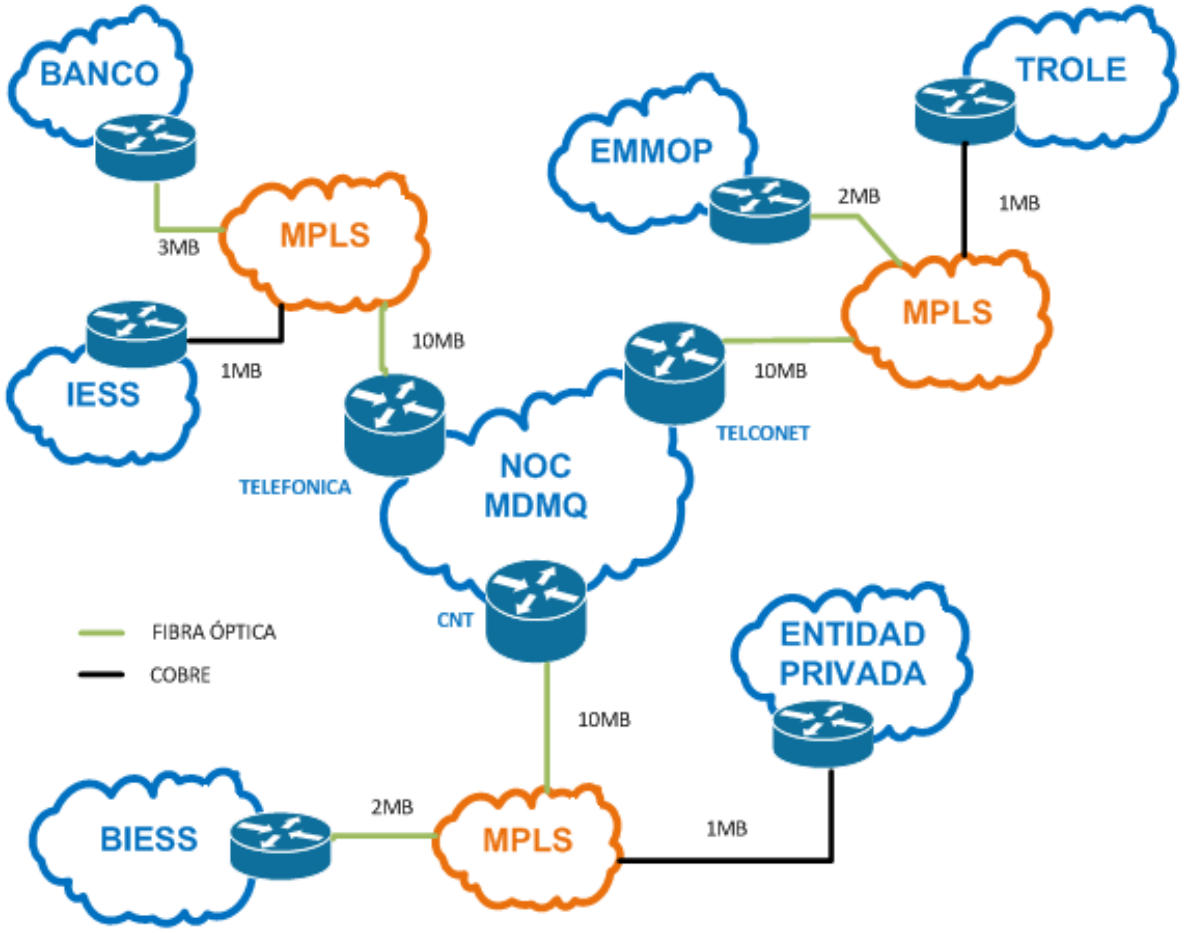

Ilustración 8. (López, 2015) Arquitectura de las Entidades Externas.

3.1.2.1.2 Infraestructura LAN

En cuanto a la infraestructura de red interna, esta se estructura en base al diseño arquitectónico del sitio, sin embargo, cumple los estándares básicos para garantizar la disponibilidad del servicio, un esquema en estrella es el diseño que se ha estandarizado para la red interna, y en ciertos casos, se añaden cascadas al esquema de red (Ilustración 9).

Este esquema interno se ha estandarizado en la mayor parte de las dependencias del MDMQ, donde el punto central de conectividad (switch L3) es el encargado de comunicarse a través del enlace de datos con el NOC del MDMQ, y así habilitar los diferentes servicios que brinda el MDMQ.

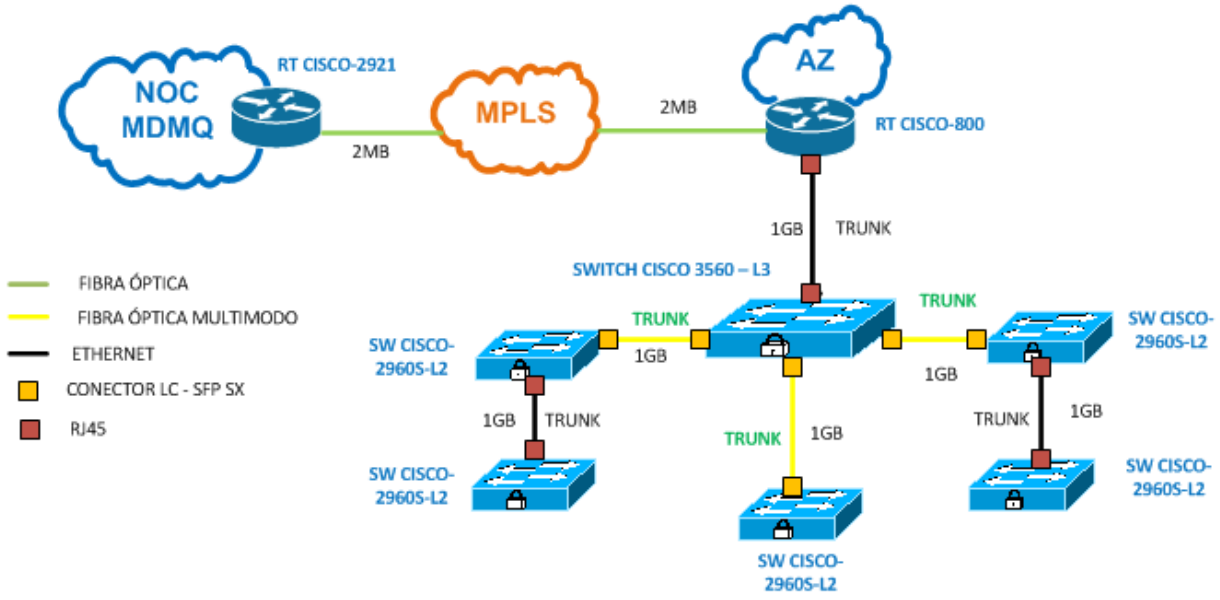

Ilustración 9. (López, 2015) Arquitectura de la Red LAN.

3.1.2.1.3 Infraestructura CLOUD

La gran demanda de los servicios del MDMQ por parte de sus contribuyentes, ha llevado al MDMQ a implementar tecnologías que contribuyan a cubrir con las necesidades de los usuarios y a garantizar la disponibilidad de los servicios.

Para esto el MDMQ ha implementado un esquema de conectividad hacia el Cloud, donde todos los contribuyentes apenas acceden a Internet entran en contacto con el cloud y a los servicios del MDMQ, este esquema es soportado por un proveedor de

servicios cloud, sin embargo el MDMQ mantiene un enlace dedicado hacia su cloud, que le permite administrar y gestionar los recursos del cloud (Ilustración 10).

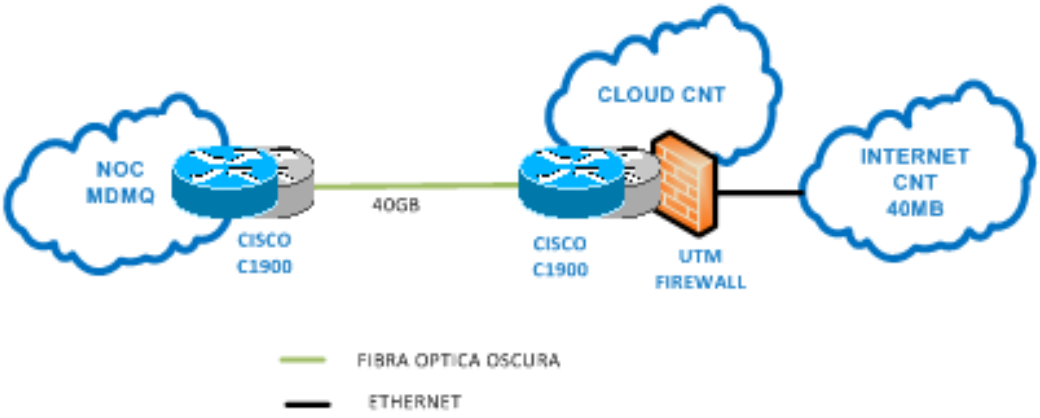

Ilustración 10. (López, 2015) Arquitectura Cloud

3.1.2.1.4 Infraestructura WIRELESS

Uno de los servicios emblemáticos del MDMQ es el servicio de zonas libres de Internet, el cual provee de Internet a los ciudadanos del distrito metropolitano, en sitios como: plazas, parques, estaciones de buses, etc.

El MDMQ cuenta con una infraestructura inalámbrica completa, cuyo esquema de red se conecta a la red municipal para propagar el servicio, a la vez el MDMQ administra y gestiona el servicio, controla y restringe el acceso para garantizar la disponibilidad y seguridad de la infraestructura del servicio.

A la vez esta infraestructura Wireless brinda servicio a los usuarios internos de las diferentes dependencias del MDMQ, haciendo que ambos servicios se propaguen por separado sin afectarse entre estos. Sin embargo la infraestructura para los usuarios internos del MDMQ es más extensa (Ilustración 11).

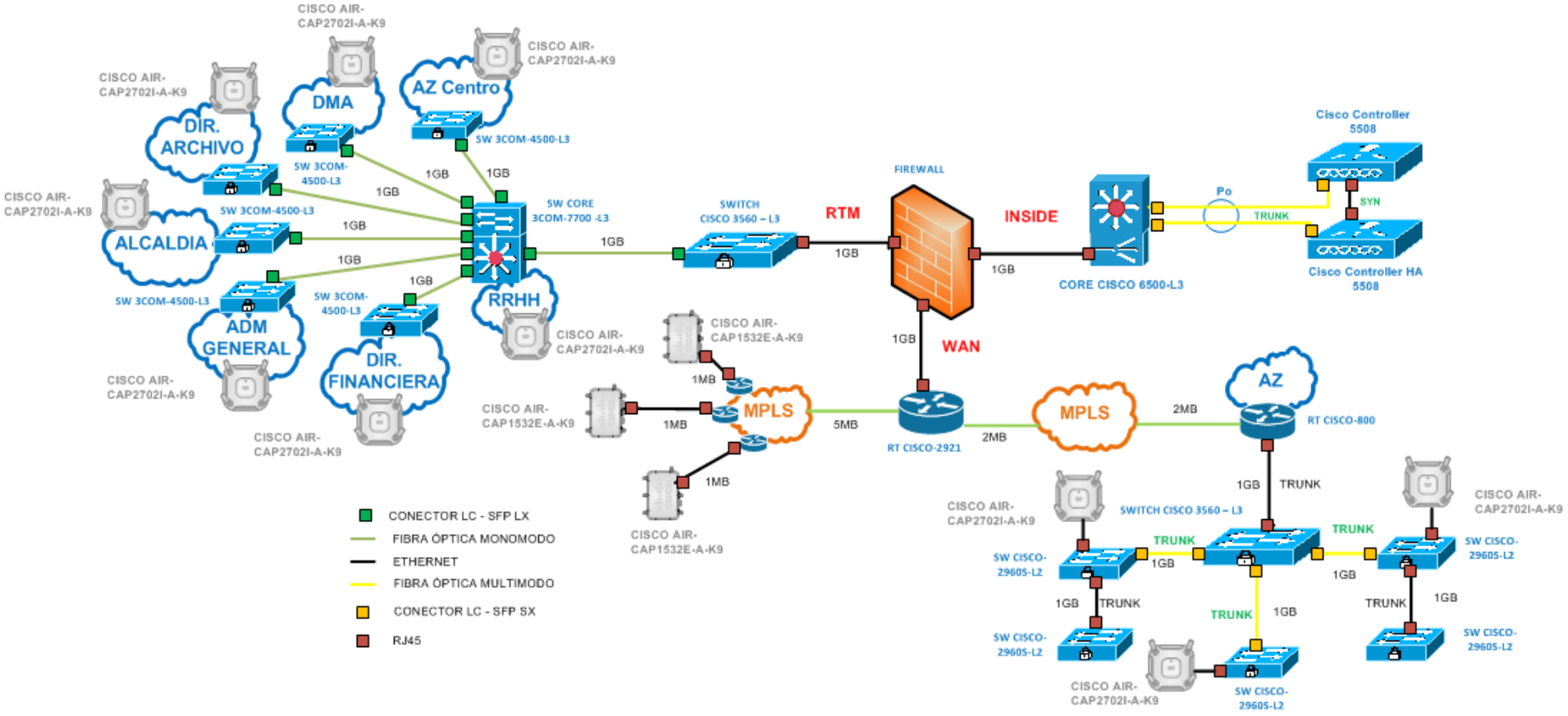

Ilustración 11. (López, 2015) Arquitectura de la Red Wireless

3.1.2.1.5 Infraestructura INTERNET

En la actualidad el servicio de Internet se ha convertido en una herramienta indispensable en las actividades laborales diarias de los usuarios, el MDMQ cuenta con dos proveedores de servicio de Internet, manteniendo un esquema de alta disponibilidad activo-pasivo del servicio, con un enlace principal y un enlace secundario. Este esquema de conectividad, se encuentra implementado y centralizado en el NOC del MDMQ (Ilustración 12).

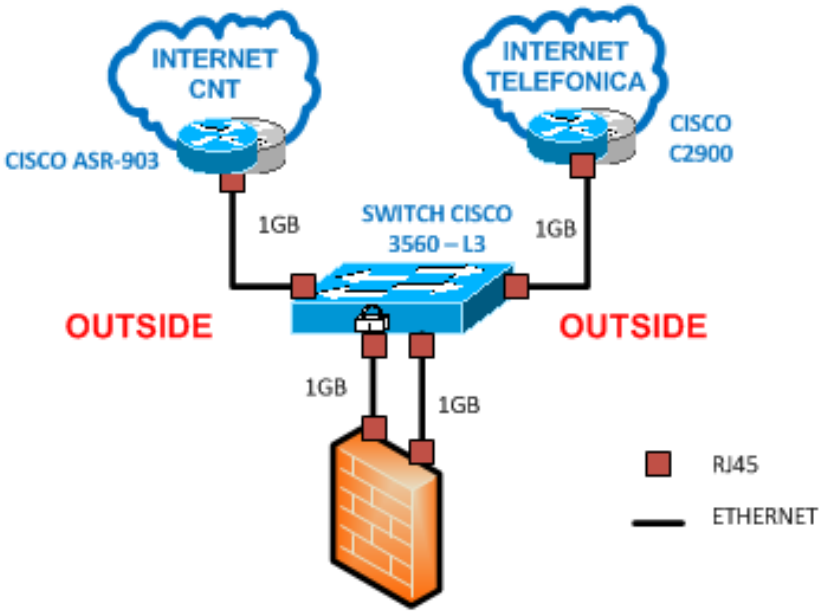

Ilustración 12. (López, 2015) Arquitectura de Internet

3.1.2.2 Esquema de Seguridad Actual

El esquema de seguridad del MDMQ, actualmente soporta la mayor parte de los servicios que brinda el MDMQ, sin embargo, el esquema de seguridad no cuenta con una infraestructura robusta y redundante, siendo un punto sensible para el MDMQ.

Actualmente el esquema de seguridad se encuentra centralizado en el NOC, donde los diferentes componentes de la infraestructura tecnológica convergen, siendo este un punto ideal para manejar el esquema de seguridad y los diferentes elementos que lo conforman.

El punto de partida es el firewall, siendo el equipo principal de enrutamiento, el cual distribuye el tráfico a su destino final, este a la vez realiza el trabajo de analizar el tráfico que cursa por la red, cumpliendo las funcionalidades de un firewall; la infraestructura de red parte de este punto central a los diferentes puntos remotos de comunicación, pertenecientes a las respectivas dependencias y servicios del MDMQ (Ilustración 13).

De la misma forma, el servicio de Internet con el que cuenta el MDMQ para sus usuarios internos y externos, parten de este punto central del esquema de seguridad, el cual soporta la carga total del consumo del servicio.

Una gran ventaja del esquema de seguridad que maneja el MDMQ, es el hecho de que tiene dividido los esquemas de conectividad de la red en: campus, datacenter y cloud, donde el campus, abarca toda la conectividad de la red LAN, WAN, wireless e Internet. El esquema de red para datacenter abarca la inside y dmz, y la parte cloud, como su nombre lo indica, contiene todo el esquema de conectividad del cloud.

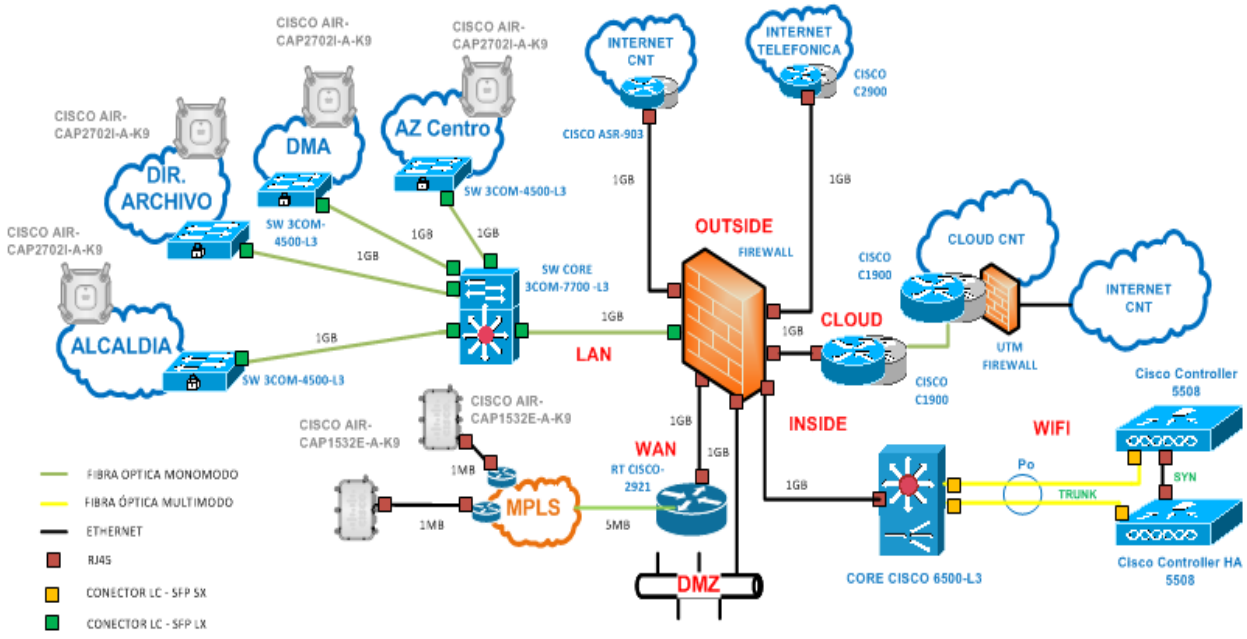

Ilustración 13. (López, 2015) Arquitectura de Seguridad.

Gran parte de la infraestructura del MDMQ está dedicada a brindar servicios a la ciudadanía del Distrito Metropolitano de Quito. Los diferentes servicios web del MDMQ se basan en una misma arquitectura, las cuales están siendo gestionadas y administradas a la interna, es decir, el MDMQ tiene su propio hosting. Su arquitectura está basada en SO Linux y Windows, dependiendo del contenido, funcionalidades y la necesidad de cada uno de estos.

La mayor parte de sitios web del MDMQ (entre 10 y 15) están expuestos al público a través de los puertos http (80) y https (443) y usan protocolos IP, TCP y UDP. Debido al número de aplicativos que el MDMQ posee, y para garantizar la disponibilidad del servicio, el MDMQ cuenta con un balanceador de aplicaciones en su infraestructura tecnológica, el cual, permite distribuir la carga del consumo de los sitios y mejorar el rendimiento y el tiempo de respuesta hacia el usuario final.

Para la red interna, existe varios aplicativos que son de uso exclusivo para los usuarios internos del MDMQ, así mismo, estos aplicativos se encuentran implementados bajo diferentes arquitecturas, dependiendo del tipo de aplicativo, contenido, base de datos, funcionalidades y consumo de recursos. Los aplicativos usan una gran variedad de puertos, entre los más importantes están: 1521 (sql), 1433 (ms-sql), 53 (domain), 8080 (http y https proxy), 22 (ssh), 23 (telnet), 3389 (escritorio remoto), 5432 (Postgres), entre otros. De la misma forma estos usan protocolos TCP y UDP para la comunicación.

Otro servicio emblemático del MDMQ son las zonas de Internet gratuito para la ciudadanía del MDMQ, este servicio es manejado a través de una solución de Wireless, la cual utiliza un rango de puertos bien conocidos y protocolos de comunicación propietario de la marca de la solución.

3.1.2.3 Equipamiento Tecnológico

La infraestructura de seguridad del MDMQ está compuesta por los siguientes elementos:

- **Firewall. -** El MDMQ cuenta con dos firewalls cisco de la serie 5000, con un throughput entre 450 Mbps a 650 Mbps, los cuales se encuentran en estado activo – activo, donde la alta disponibilidad, tanto física como lógica, se la maneja de manera manual. Cabe recalcar que estos firewalls tienen diferentes características, lo que impide construir entre estos un esquema en alta disponibilidad, incluso cuentan con diferente número de interfaces, lo que compromete la comunicación de algunos esquemas de conectividad, mencionados anteriormente.

Uno de los dos firewalls, el de mejor características (ASA 5540), inspecciona todo el tráfico actual de la red, los segmentos LAN, DMZ, INSIDE, CLOUD, WAN y OUTSIDE, están siendo analizados, estos segmentos se encuentran configurados en cada interfaz del firewall, donde ciertos segmentos, cuentan están configurados como trunk, para permitir el paso de más segmentos de red por la misma interfaz, de esta forma se cubre la totalidad de los diferentes segmentos que tiene el MDMQ.

El segundo firewall (ASA 5520), cuenta con un número reducido de interfaces, por tal motivo, tiene configurado los segmentos LAN, DMZ, INSIDE, WAN Y OUTSIDE. En el caso que el primer firewall falle es necesario realizar la conexión física de los diferentes segmentos a las interfaces del segundo firewall y permanecer sin conectividad en los demás segmentos hasta arreglar el problema.

La solución de firewall actual no maneja un esquema integral con los recursos del MDMQ, es decir, no permite integrar otros servicios que interactúen con el firewall. Debido a que la solución de firewall cuenta con una versión obsoleta, no cuenta con mayores funcionalidades las cuales permitan activar características que mejoren su funcionalidad.

Algo que se debe tener muy en cuenta es que esta solución de firewall no posee funcionalidades de filtrado web, control de aplicaciones y balanceo de carga.

- **IPS. -** La infraestructura de seguridad también cuenta con tres ciscos IPS de la serie 4000, los cuales manejan un throughput de 250 Mbps cada uno, de los cuales un solo equipo se encuentra analizando el tráfico que cursa por la

interfaz, esto debido a que los demás equipos se encuentran fuera de servicio por problemas de hardware.

El equipo activo cisco IPS 4260 se encuentra en un modo estándar, es decir, cuenta con una configuración por defecto, y analiza el tráfico en la categoría más baja de inspección, donde las diferentes firmas activas cumplen un nivel mínimo de seguridad.

El IPS cuenta con 4 interfaces de red, manejado por 2 pares IN y OUT, en donde se encuentra configurados 2 segmentos de la infraestructura del MDMQ, en este caso las más VULNERABLES, OUTSIDE Y WAN. De la misma manera que el firewall, la solución de IPS no cuenta con un esquema en alta disponibilidad, lo cual obliga a que si existe un problema, el proceso de cambio debe ser manual.

Como se mencionaba anteriormente, el equipo no cuenta con una configuración avanzada para una inspección minuciosa del tráfico, un perfil por defecto no garantiza y alto nivel de seguridad, y menos aún, cuando el equipo ha dejado de actualizar firmas, como en este caso, lo que ocasionaría que nuevas tecnologías de amenazas pasen desapercibidos.

- **AAA. -** Un punto muy favorable dentro de la infraestructura de seguridad del MDMQ es el servicio de Authentication, Authorization, and Accounting, conocido como AAA, servicio activo a través del appliance cisco ACS. Esta seguridad de acceso a la red interna esta aplicado en gran parte del equipamiento activo de red.

  Cisco ACS realiza el control de acceso hacia la red interna a través del Directorio Activo, es decir, el usuario que se conecte a la red interna debe

pertenecer al dominio del MDMQ y a la vez el usuario debe pertenecer a un grupo establecido dentro del directorio activo. El ACS mediante protocolos de autenticación como radius y tacacs realiza la validación del usuario contra el directorio activo, de esta forma se asegura que el usuario que ingresa a la red interna sea un usuario interno del MDMQ.

El AAA a su vez valida el ingreso de cualquier dispositivo a la red interna, por ejemplo: teléfonos IP, impresoras, móviles, etc., De la misma forma, únicamente ingresan los dispositivos registrados como autorizados.

- **Wireless. -** El MDMQ cuenta con una solución de Wireless completa y robusta, construida bajo un esquema en alta disponibilidad, a través de dos equipos cisco wireless controler de la serie 5000, los cuales actualmente soportan alrededor de 200 APs y 30.000 usuarios.

  La solución de Wireless está distribuida en toda la arquitectura de red del MDMQ, centralizada y gestionada en el NOC, bajo políticas de acceso, que garantizan la disponibilidad del servicio.

  Uno de los equipos cisco 5508, está diseñado para trabajar como HA, es decir, su función es para garantizar la alta disponibilidad del servicio, y cuenta con características de hardware diferente al equipo principal.

  El servicio de red inalámbrico se lo da a través de 2 diferentes SSID, donde uno de ellos es para los usuarios del MDMQ y el otro es dedicado para el servicio de internet gratis, lógicamente separadas de los diferentes servicios que se dan en los diferentes segmentos de red de la infraestructura del MDMQ.

- **Core. -** El core de comunicaciones esta sostenida en un robusto VSS, compuesto por equipos cisco de la seria 6000, formando la columna vertebral de la comunicación para el campus, datacenter y cloud.

  Dos equipos switch core 6500, forman el core de comunicaciones, cada uno con las mismas características físicas y lógicas, ambos equipos forman un VSS, lo cual garantiza una alta disponibilidad de los servicios, redundancia en los componentes, alto rendimientos y una administración unificada.

  El core de comunicaciones es el puente para acceder a todos los servicios del MDMQ, por aquí convergen todas las comunicaciones que pasan al datacenter, donde se encuentra alojado la infraestructura que aloja los diferentes servicios. Los sw de core están formados por interfaces de 10GB y 1GB, tanto en fibra (SFP) como ethernet.

- **Equipamiento activo de red. -** El MDMQ cuenta con gran variedad de routers y switchs, los cuales se encuentran distribuidos e implementados, dimensionados en base a las necesidades requeridas, la mayor parte del equipamiento es Cisco, ya que se ha procurado manejar un estándar de equipamiento que simplifique su administración y gestión.

  Entre el equipamiento tenemos modelos como: router Cisco 3800, sw Cisco 3560, router Cisco 2900, sw Cisco 2960, sw core 3750, etc. Todos estos para la infraestructura de Campus, en cuanto a la infraestructura del datacenter, lo conforman equipos como: Nexus 5K, MDS, sw ProCurve, etc.

3.1.2.4 Amenazas y Vulnerabilidades

Con el fin de determinar las amenazas y vulnerabilidades dentro de la infraestructura tecnológica actual del MDMQ, se la puso a prueba a través de la herramienta open source llamada "The Kali Linux". Alonso Eduardo Caballero Quezada (2015) menciona a Kali como una distribución avanzada de pruebas que puede ser aplicado en diferentes plataformas, especializada en penetración, Ethical Hacking y detección de vulnerabilidades.

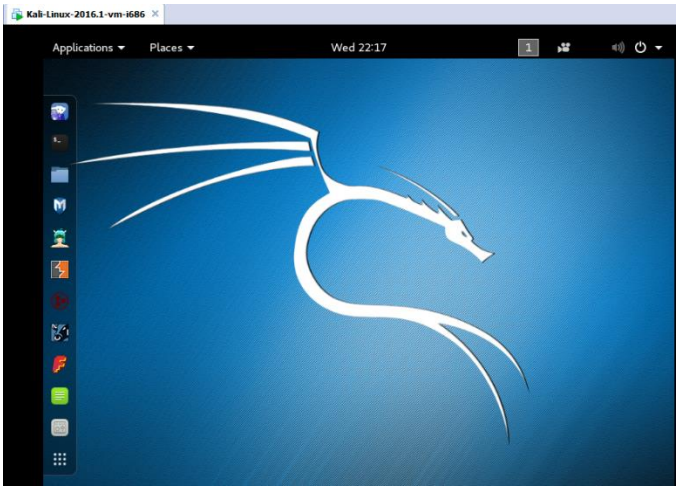

Ilustración 14. (Kali, 2015) Interfaz de usuario Kali Linux

Kali cuenta con una gran variedad de aplicativos con diferentes funcionalidades, las cuales realizan procedimientos o tareas sobre la infraestructura tecnológica para analizar, encontrar y determinar posibles huecos de seguridad, vulnerabilidades de sistemas, amenazas latentes, entre otros resultados.

(Quezada, 2015) Recomienda que para un proceso de hardening se use la herramienta Nmap. “Network Mapper” o Mapeador de Puertos, es una herramienta open source para la exploración de redes y auditorías de seguridad. Ha sido diseñado para escanear velozmente redes de gran envergadura, como también host únicos.

Una vez determinado el objetivo, aplicamos las funcionalidades de la herramienta open source sobre los segmentos de red donde se alojan ciertos servicios del MDMQ, tomando en cuenta que para este paso no fue necesario descubrir los elementos que conforman la infraestructura tecnológica.

3.1.2.4.1 Escaneo de Servicios

3.1.2.4.1.1 Servicios Públicos

El MDMQ tiene publicado sus servicios a través de sitios web, los cuales están siendo publicados a través de un segmento de red público, es decir, en Internet, al alcance de todo el mundo.

Los resultados de la herramienta Nmap sobre la red pública es la siguiente:

Servicio de VPN

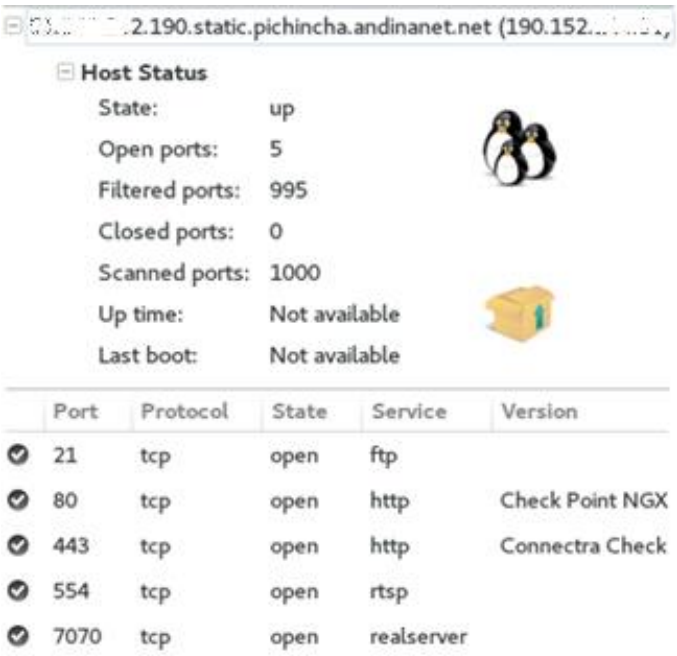

Ilustración 15. (López, 2015) IP pública Servicio de Internet

Sitio Web

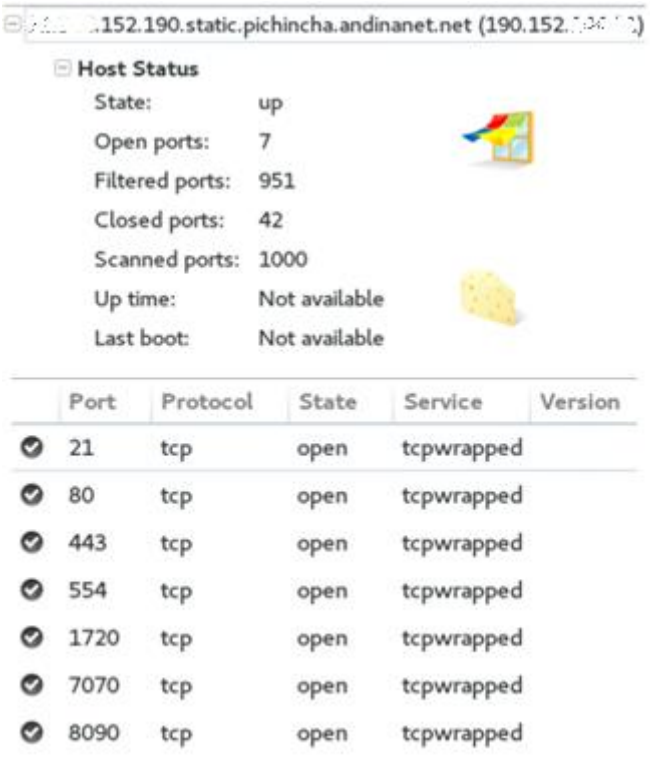

Ilustración 16. (López, 2015) IP pública sitio web

Ilustración 17. (López, 2015) IP pública sitio web 2

Internet

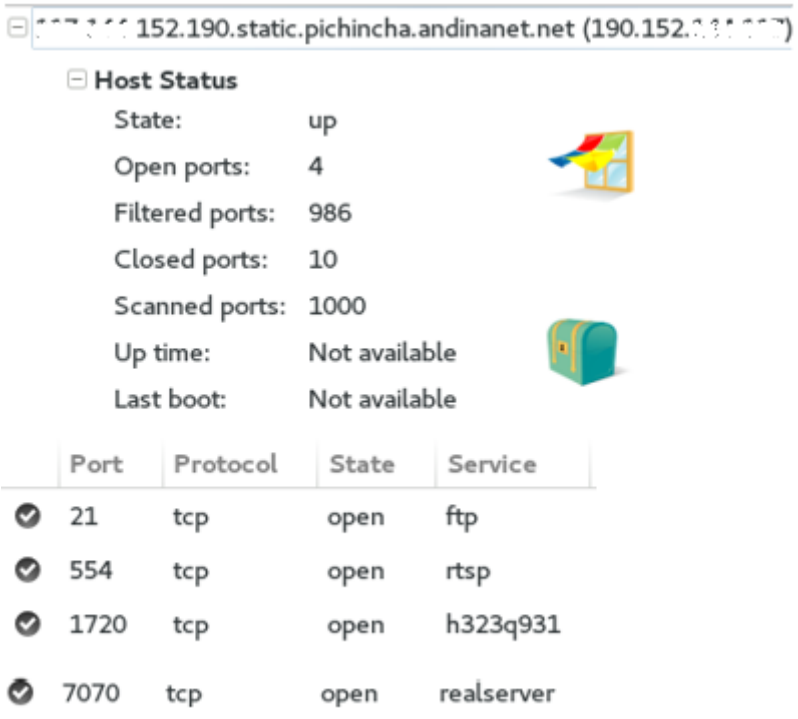

Ilustración 18. (López, 2015) IP pública de Internet

3.1.2.4.1.2 Servicios Privados

De igual forma el MDMQ cuanta con algunos servicios internos, los cuales están publicados en segmentos de red privados, al alcance de los usuarios internos.

Directorio Activo

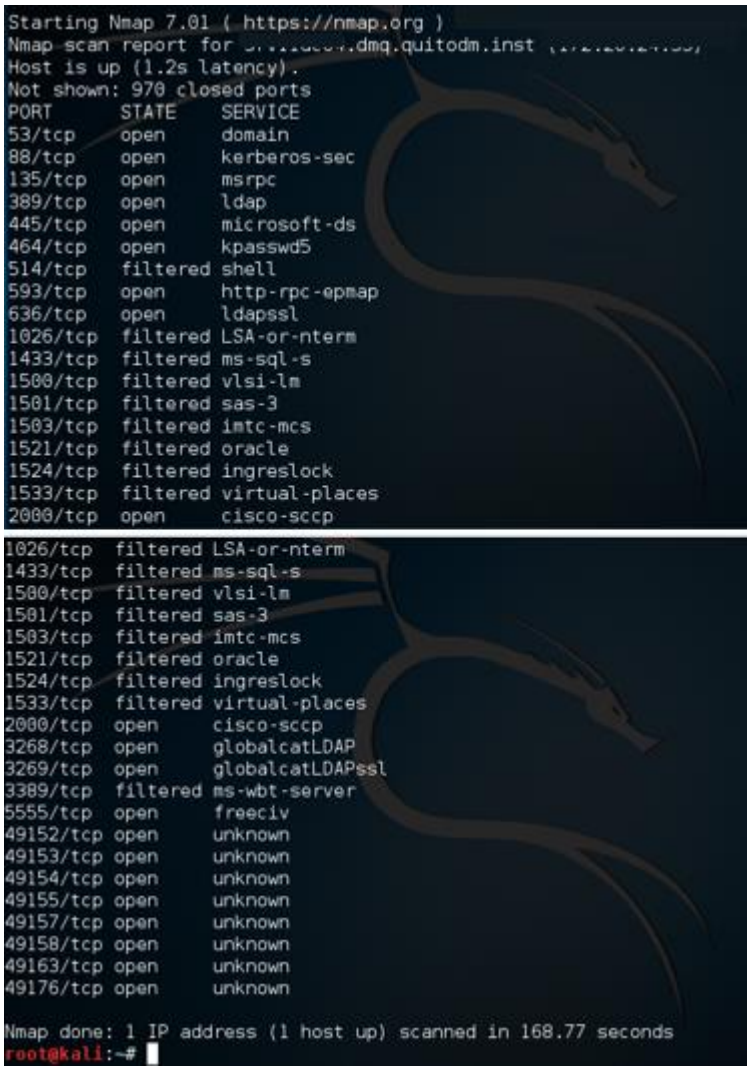

Ilustración 19. (López, 2015) IP Servicio del DA

Monitoreo

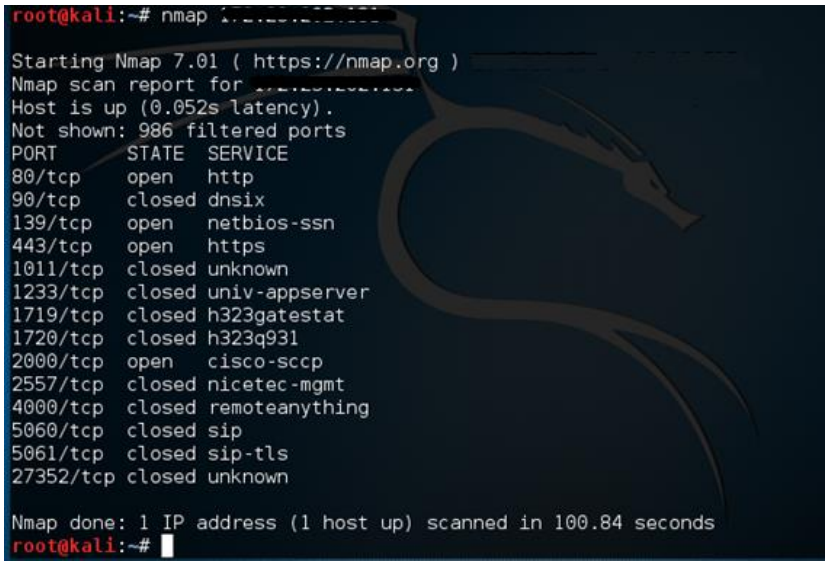

Ilustración 20. (López, 2015) IP Servidor de monitoreo de red

Controladora Wireless

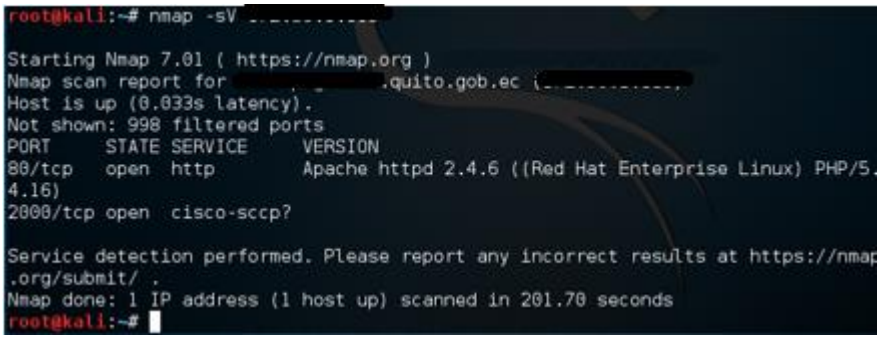

Ilustración 21. (López, 2015) IP Controladora Wireless

Syslog

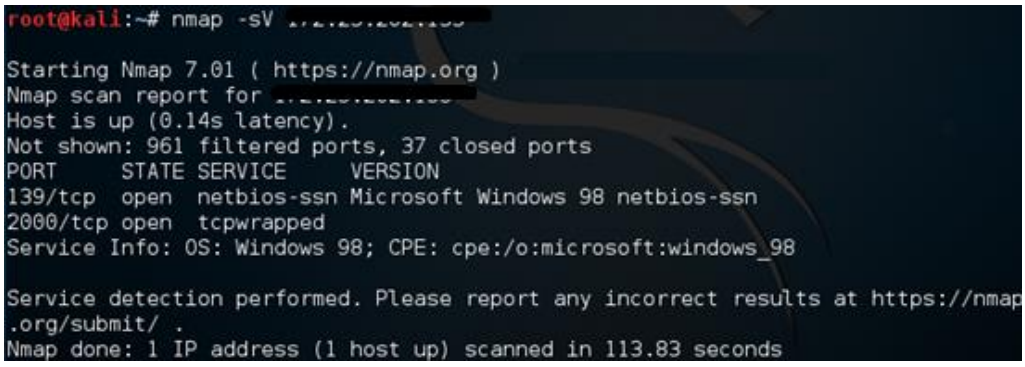

Ilustración 22. (López, 2015) IP Servidor de Syslog

Internet

De la misma forma, se realizó un escaneo en cuanto al servicio de navegación de Internet, es decir, el acceso que tienen los usuarios en la navegación hacia sitios web externos pertenecientes a categorías de alto riesgo, para este procedimiento se contó con la ayuda de una herramienta propia del fabricante de Websense, esta herramienta es conocida en el mercado como un servicio de filtrado web y control de contenido en el uso del Internet.

La información generada cuenta con la siguiente estructura:

ID	Category Name	URL	Result	Block Reason
13186	Malware Files	http://molionia.ru/get/52570	Error	Error
13187	Malware Files	http://molionia.ru/get/55774	Error	Error
13188	Malware Files	http://molionia.ru/get/52602	Error	Error
13193	Malware Files	http://molionia.ru/get/52496	Error	Error
13196	Malware Files	http://hackgame.org/download/HackBauVatCF_1120.exe	Retrieved	Retrieved
13197	Malware Files	http://gunzupdates.universe-gamers.com/patchpublic/License.dll	Retrieved	Retrieved
13198	Malware Files	http://downloadsave.info/?e=ssale&publisher=2017&dd=2&p=http://ca.isohunt.com/download/451204351/argo.torrent?src=saven	Retrieved	Retrieved

Ilustración 23. (López, 2015) Escaneo de la Navegación en Internet

Dónde: El parámetro **result**, indica si el sitio escaneado tiene acceso el usuario (Retrieved) o si está siendo bloqueada (Error) por los elementos de control internos del MDMQ. Los resultados del escaneo se encuentran en el ANEXO #3 documento “Web Content Security Validaton Report before”.

En base a la información obtenida durante el proceso de hardening, el escaneo de puertos, la falta de una cultura de seguridad, procedimientos de seguridad, políticas de seguridad, mecanismos de control y el desempeño de mis funciones en el MDMQ, han permitido identificar las amenazas y vulnerabilidades, así como también las implicancias de seguridad para el

MDMQ que se detallan en el ANEXO #1 documento “Amenazas y Vulnerabilidades del MDMQ”.

3.1.2.5 Análisis de Riesgos

La lista de los posibles riesgos que pueden afectar las operaciones y servicios que brinda el MDMQ, se detallan en el ANEXO #1 “Análisis de Riesgos”, tomando en cuenta el nivel de impacto y la categoría correspondiente.

3.1.2.6 Necesidades y Requerimientos

Como se ha venido describiendo, actualmente la infraestructura tecnológica del MDMQ brinda diferentes servicios tanto a sus usuarios internos como usuarios externos, servicios que pueden ser accesibles desde la red interna, como de la red externa, cada uno dependiendo de su funcionalidad, adicional a esto, el MDMQ brinda servicios a entidades públicas externas y entidades bancarias que combinan sus servicios con los del MDMQ, para los diferentes usuarios.

Este esquema conlleva a que la infraestructura Tecnológica del MDMQ sea un punto vulnerable y crítico, que puede ser afectado, lo que causaría que los servicios e información del MDMQ sean amenazados, en ese sentido la infraestructura tecnológica requiere de un fortalecimiento en su esquema de seguridad, y de la misma forma, un cambio en su esquema de conectividad, que colaboren y se integren a nuevas tecnologías de detección, prevención y control, los cuales aseguran la de confidencialidad, integridad y disponibilidad de la información.

Para alcanzar todas estas características, es necesario tomar en cuenta los siguientes aspectos:

- Solución de firewall de nueva generación.
- Esquema automático de alta disponibilidad solución de firewall.
- Solución de detección y prevención de intrusos de nueva generación.
- Sistemas sofisticados que utilizan analítica y machine learning para predecir y bloquear extraños comportamientos.
- Esquema automático de alta disponibilidad solución de IPS.
- Solución de filtrado web.
- Solución de control de aplicaciones.
- Solución de control de identidad.
- Herramientas para la administración y gestión de la IT.
- Esquema de conectividad de red
- Políticas de seguridad
- Personal capacitado.

CAPÍTULO 4

ESQUEMA DE SEGURIDAD

4.1 Diseño del esquema de seguridad

En vista de las vulnerabilidades, debilidades y necesidades que actualmente tiene el MDMQ en su infraestructura tecnológica, es necesario reconstruir un nuevo esquema de seguridad, el cual elimine las vulnerabilidades, fortalezca las debilidades y cubra con todas las necesidades, y a la vez, este esquema debe integrar todos los demás componentes, sistemas, equipamiento, etc. que conforman la infraestructura tecnológica del municipio.

El nuevo esquema debe contener un punto central donde puedan converger todas las tecnologías de comunicación que tiene la infraestructura tecnológica del municipio, siendo el puente por el cual cursa y converge toda la comunicación, donde se apliquen controles estrictos de seguridad y neutralice cualquier anomalía.

La columna vertebral sobre la cual está diseñado el esquema de seguridad es el firewall, por el cual converge la comunicación, y es el encargado de aplicar las políticas de seguridad y control del tráfico que cursa por la red, es quien permite o bloquea el tráfico y es el que soporta la carga de los sistemas y servicios que el MDMQ brinda a sus usuarios internos y externos este esquema a más de mejorar, asegurar, resguardar, actualizar y robustecer la seguridad de la infraestructura tecnológica del MDMQ.

Este nuevo esquema está construido en base a una nueva solución de firewall, el cual cuenta con un mecanismo automático que garantiza la alta disponibilidad (HA), contra caídas o fallas lógicas o físicas, así mismo, la solución dispone de un mecanismo de control de aplicaciones y filtrado web que optimiza y protege el servicio de Internet mediante políticas de seguridad y controles de navegación que evitan el mal uso del servicio y saturación del canal de Internet.

Adicional a la solución de firewall como la base sólida del esquema de seguridad, también se contempla como componente adicional a la arquitectura de seguridad, una nueva solución de prevención y detección de intrusos IPS, que incluye tecnología que garantiza la alta disponibilidad de la solución, así como también, tecnología de última generación para la detección, prevención y neutralización de vulnerabilidades, amenazas o ataques a la infraestructura tecnológica.

Debido a que este nuevo diseño obliga a que toda la comunicación converja en un solo punto, es necesario rediseñar el esquema de red tanto para el esquema de campus, datacenter y cloud, donde las diferentes redes municipales LAN, WAN y Wireless se concentren y partan de un mismo punto, en este caso, el firewall.

Es importan tomar en cuenta los demás elementos que conforman la infraestructura tecnológica del municipio, ya que estos deben acoplarse al nuevo esquema, sin afectar sus funcionalidades, aquí también se incluye el nuevo equipamiento de administración y gestión de las soluciones indicadas.

Tomando en cuenta todos los elementos que describimos y parte del esquema actual, el nuevo esquema de seguridad y conectividad del municipio se define de la siguiente forma:

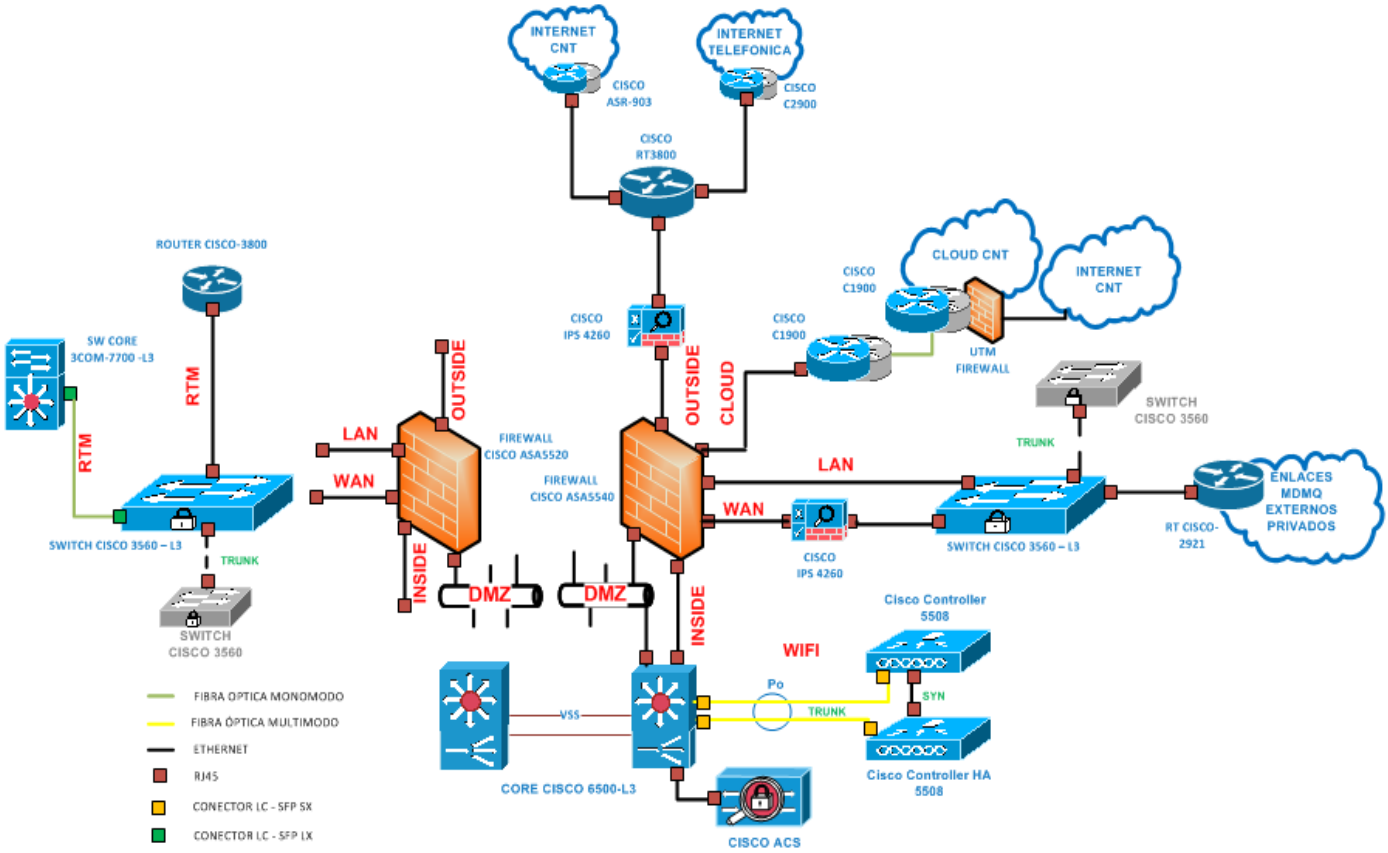

Ilustración 24. (López, 2015) Arquitectura del Esquema actual de Seguridad

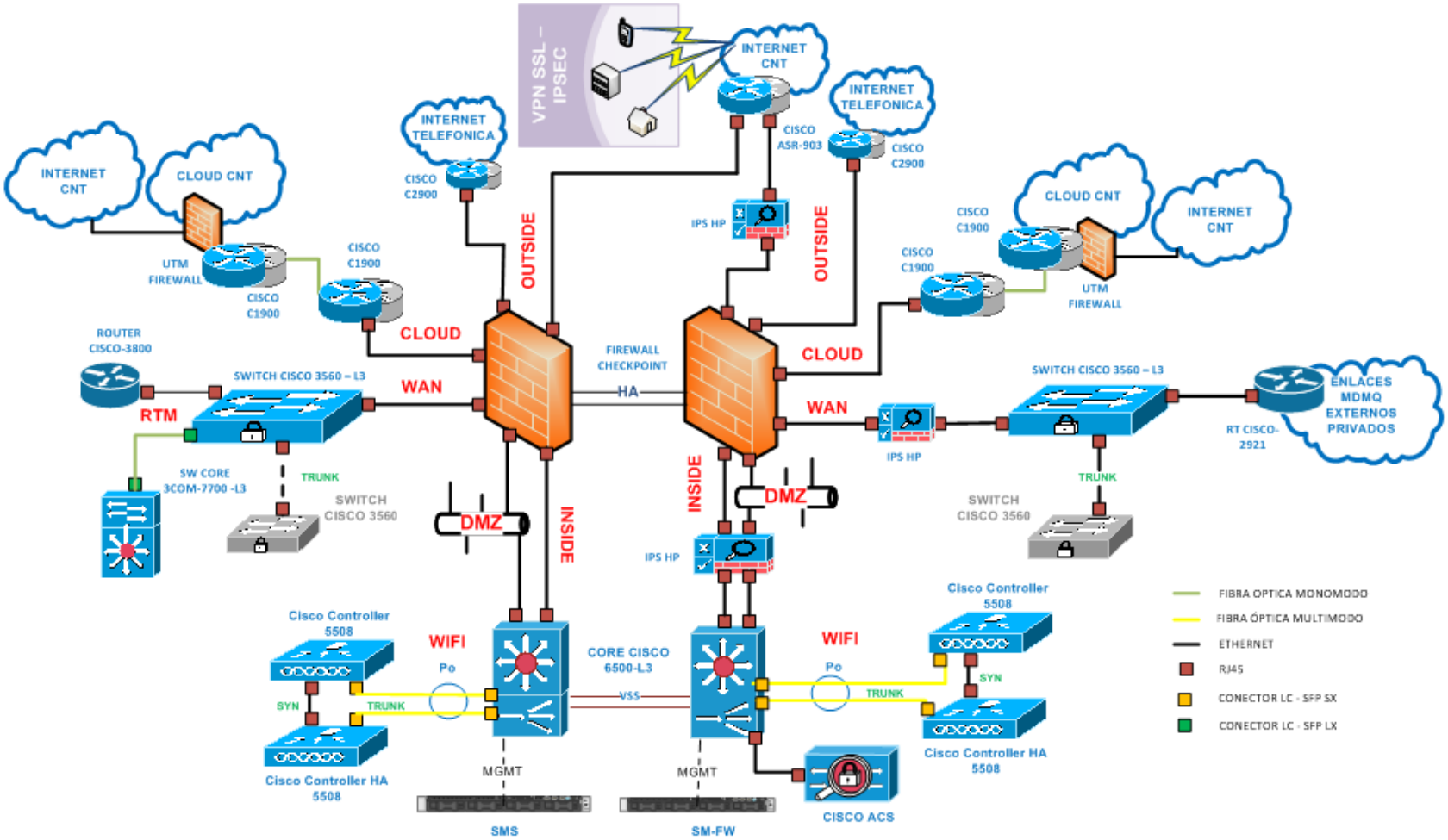

Ilustración 25. (López J. F., 2016) Arquitectura de nuevo Esquema de Seguridad

4.2 Equipamiento

Actualmente el mercado tecnológico ofrece muchas soluciones de seguridad (firewall e IPS), las cuales cuentan con varias características y funcionalidades, sin embargo, para elegir la mejor opción para la infraestructura tecnológica del MDMQ, es necesario conocer en profundidad el esquema de conectividad lógico y físico actual, como también las diferentes necesidades del MDMQ.

En base a lo indicado, a continuación, tenemos el cuadro comparativo de las diferentes soluciones de seguridad que encontramos en el mercado y que son los más destacados por sus funcionalidades y características:

4.2.1 FIREWALL

NECESIDADES Y REQUERIMIENTOS	FORTINET	CISCO	CHECKPOINT	SOPHOS
Solución de firewall de nueva generación.	√	√	√	√
Esquema automático de alta disponibilidad.	√	√	√	√
Open Server	X	X	√	X
Virtualización	√	√	√	√
Solución de filtrado web.	√	√	√	√
Solución de control de aplicaciones.	√	√	√	√
Herramientas para la administración y gestión	√	√	√	√
Simplificar la gestión de políticas	√	√	√	√
Manejo de usuarios y direcciones IP (firewall)	LIMITADO	LIMITADO	√	LIMITADO
Inspección del tráfico en tiempo real	√	√	√	√
Inspección HTTPS	LIMITADO	LIMITADO	√	LIMITADO
Escalabilidad	LIMITADO	LIMITADO	√	LIMITADO

NECESIDADES Y REQUERIMIENTOS	FORTINET	CISCO	CHECKPOINT	SOPHOS
QoS	√	√	√	√
Shapping	X	X	√	X
Balanceador de carga ISP	√	√	√	√
VPN SSL-IPSec	√	√	√	√
Prevención de Amenazas	X	X	√	X
Funcionalidades desarrolladas por el fabricante	√	X	√	√

Tabla 2. (López J. F., 2016) Comparación de soluciones de Firewall

4.2.2 IPS

NECESIDADES Y REQUERIMIENTOS	HP	CISCO	McAfee	PALOALTO
Solución de detección y prevención de intrusos de nueva generación.	√	√	√	√
Sistemas sofisticados que utilizan analítica y machine learning para predecir y bloquear extraños comportamientos.	√	√	√	√
Esquema automático de alta disponibilidad solución de IPS.	√	√	√	√
Equipo de propósito específico IPS	√	X	X	√
Licenciamiento de funcionalidades	√	LIMITADO	LIMITADO	LIMITADO
Latencia	<	>	>	>
Manejo de reputación de IPs	√	LIMITADO	LIMITADO	LIMITADO
Mecanismo de detección de fallas en capa 2 (Hardware)	√	X	X	X
Centro especializado de detección de vulnerabilidades y desarrollo de firmas	√	√	√	√

Tabla 3. (López J. F., 2016) Comparación de soluciones de IPS

4.2.3 Equipamiento Firewall

Con el fin de disponer de un esquema en alta disponibilidad, escalabilidad y rendimiento, la solución de firewall se basará en un modelo "open server" el cual lo conforman los siguientes elementos:

Descripción	Cantidad
SERVIDOR HP DL380p Gen8	3

Tabla 4. (López J. F., 2016) Equipamiento Firewall

Cada uno de estos elementos cuenta con las siguientes características físicas y lógicas, que cubren con el rendimiento y funcionalidad mínimo requerido.

CANTIDAD	CARACTERISTICAS
2	12 cores
	3 tarjetas (módulos) con 4 puertos Ethernet 10/100/1000 Base-T RJ45 cada una
	2 tarjetas (módulos) con 2 puertos a 10gigabit de fibra óptica cada uno, SFP (SX)
	12 GB de RAM
	Conjunto de instrucciones 64 bits
	Frecuencia de los procesadores de 2.5 GHz
	Almacenamiento de 2 TB
	Debe tener una fuente primaria y secundaria, con soporte para 100 a 240 VAC y 50/60 Hertz.

Tabla 5. (López J. F., 2016) Características de Hardware Firewall.

CANTIDAD	CARACTERISTICAS
1	4 cores
	Almacenamiento de 2 TB de disco (2 discos duros de 1TB)
	32 GB de RAM
	Conjunto de instrucciones 64 bits
	Frecuencia de los procesadores de 2.5 GHz
	Tarjeta (módulo) con 4 puertos Ethernet 10/100/1000 Base-T RJ45
	Debe tener una fuente de poder primaria y secundaria, con soporte para 100 a 240 VAC y 50/60 Hertz.

Tabla 6. (López J. F., 2016) Características de Hardware Firewall SM.

4.2.4 Equipamiento IPS

La solución de IP se basa en un modelo "Appliance" de propósito específico con el cual se asegura un esquema en alta disponibilidad (bypass físico y lógico), escalabilidad, baja latencia y alto rendimiento, la solución está compuesta por los siguientes elementos:

Descripción	Cantidad
APPLIANCE HP S2600 NX IPS	1
TARJETA HP NX IPS 4-segment Gig-T Bypass Mod (tarjeta interna instalada en el equipo IPS)	1
APPLIANCE HP SMS H3 w/25 Device LTU	1

Tabla 7. (López J. F., 2016) Equipamiento IPS

Cada uno de estos elementos cuenta con las siguientes características físicas y lógicas, que cubren con el rendimiento y funcionalidad mínimo requerido.

APPLIANCE HP IPS
El número de segmentos a ser protegidos es de al menos 4 segmentos (8 puertos) con interfaces de 1Gbps (en cobre).
Desempeño en inspección de tráfico de 3 Gbps
Desempeño en tráfico de red de 40 Gbps
Tiene una latencia (retardos) no mayor a 40 microsegundos
Soporta 300.000 conexiones por segundo.
Soportar 30.000.000 sesiones simultáneas.
Mecanismo para en caso de detectarse una falla, el equipo se maneje automáticamente en capa 2 dejando pasar el tráfico sin bloquearlo.
Incluye el hardware para pasar el tráfico (bypass mod), incluso si el elemento es desconectado e incluso removido o tenga un daño total, de tal manera que el tráfico no se interrumpe incluso si no existe energía eléctrica para estos componentes.
Interfaces de 1Gps

APPLIANCE HP IPS
Cuenta con al menos 1 fuente de poder redundante y 1 ventilador redundante.
Cuenta con la capacidad de expansión de por lo menos 1 módulo I/O físico para interfaces de red.

Tabla 8. (López J. F., 2016) Características de Hardware IPS

En cuanto al appliance HP SMS, es la herramienta de gestión y administración del IPS, es el medio por el cual se realiza el afinamiento y aplicación de políticas de seguridad sobre el tráfico que cursa por la red.

4.3 Implementación

El plan de implementación contempla la instalación y puesta en marcha del equipamiento y características mencionadas en el ítem 4.2, todas las funcionalidades de cada una de las soluciones y la configuración del equipamiento existente para formar el nuevo esquema de conectividad en la cual se complementen todos los elementos y formen una infraestructura tecnológica compatible y robusta por la cual converge toda la comunicación del MDMQ.

4.3.1 Firewall

El equipamiento La solución de Seguridad Perimetral consta de la configuración de los siguientes componentes:

- Check Point Security Gateway (2)
- Check Point Security Management

4.3.1.1 Check Point Security Gateway

Sobre los servidores HP DL380p Gen8 se instalará el sistema operativo basado en Linux desarrollado por la empresa Checkpoint Software Technologies llamado GAIA, sobre el mismo se cargará la aplicación Check Point Security Gateway en su versión R77.30.

Ambos servidores, en este caso los Security Gateways, se configurarán en Alta Disponibilidad en modo (Activo/Standby) con las siguientes interfaces en cada uno de ellos.

INTERFAZ	DESCRIPCIÓN
Eth0	Internet ISP 1
Eth1	Internet ISP 2
Eth2	CLOUD
Eth3	WAN
Eth4	DMZ
Eth5	WIRELESS
Eth12	SYN Failover
Ten1-2 (Link Aggregation)	INSIDE

Tabla 9. (López J. F., 2016) Interfaces del Firewall

Se realizarán las siguientes tareas en los Security Gateways:

- Instalación del Sistema Operativo Gaia
- Instalación de la Aplicación Checkpoint R77.30
- Configuración de Interfaces, PortChannels y Subinterfaces (VLANs)
- Configuración de Hostname y DNS
- Configuración de Enrutamiento
- Configuración de Control de Accesos
- Configuración de Usuarios de Administración y Roles

4.3.1.2 Check Point Security Management

En el servidor HP DL380p Gen8 se instalará el sistema operativo basado en Linux desarrollado por la empresa Checkpoint Software Technologies llamado GAIA y sobre el mismo se cargará la aplicación Check Point Security Gateway en su versión R77.30.

El equipo tendrá una única interfaz la misma que debe estar conectada al segmento de servidores internos y debe tener conectividad con los Security Gateways.

Se realizarán las siguientes tareas en el Security Management:

- Instalación del Sistema Operativo Gaia
- Instalación de la Aplicación Checkpoint R77.30
- Configuración de Interfaces de administración
- Configuración de Hostname y DNS
- Configuración de Enrutamiento
- Configuración de Control de Accesos
- Configuración de Usuarios de Administración y Roles
- Configuración de Políticas de Seguridad
- Configuración de Smart Event

Las políticas de seguridad a configurarse son las siguientes:

CARACTERÍSTICA	DESPLIEGUE
Firewall	Se hará la transferencia de las reglas del ASA hacia el Sistema Checkpoint de forma manual, depurando las reglas no necesarias

CARACTERÍSTICA	DESPLIEGUE
	Se crearán objetos en el Firewall Check Point de manera ordenada utilizando nemónicos adecuados.
	Se hará la transferencia de los Nateos del ASA y del Fortinet (Internet) hacia Checkpoint.
Identity Awareness	Se realizará una integración transparente con el directorio activo (sin uso de agentes) utilizando una cuenta con privilegios de administrador.
	Se capturará de forma automáticas las credenciales de Windows de las máquinas unidas al Domain Controller para aplicarlas en las reglas de navegación.
	Se configurará un portal cautivo para las máquinas y dispositivos móviles que no se encuentren en el dominio.
Application Control y URL Filtering	Se creará una política base en la que se bloqueen aplicaciones de alto riesgo tales como: Pornografía, Virus, Botnets, Violencia, P2P, Hacking, etc.
	Se aplicarán bloqueos/permisos de navegación para usuarios/grupos de usuarios específicos de acuerdo a las políticas de seguridad establecidas
VPN IPsec Site to Site	Se hará la transferencia de las VPN Site to Site configuradas en el equipo Fortinet hacia los equipos Check Point, se debe mantener la dirección IP pública que se tenía en Fortinet para no realizar cambios en los sitios remotos.
VPN IPsec Remote Access	Se configurarán las VPNs de acceso remoto (a través del cliente) de acuerdo a los usuarios, passwords y políticas actuales, previamente depuradas.
Mobile Access	Se configurarán las VPNs SSL de acceso remoto (a través de browser o a través del cliente en un dispositivo móvil) de acuerdo a los usuarios, passwords y políticas actuales, previamente depuradas.

CARACTERÍSTICA	DESPLIEGUE
Advance Networking and Clustering	Se configurarán los Security Gateways en alta disponibilidad (IPs virtual, CP1 y CP2) utlizando el protocolo ClusterXL de Checkpoint que es similiar al protocolo estándar VRRP.
ISP Redundancy	Se realizará el Balanceo Automático de los proveedores de Internet, por pesos, en base a los anchos de banda de cada uno de los ISP

Tabla 10. (López J. F., 2016) Funcionalidades Solución de Firewall

La configuración de Smart Event contempla lo siguiente:

CARACTERÍSTICA	DESPLIEGUE
Servicios	Se levantarán lo servicios de Management: Logging and Status, Smart Event, Smart Reporter y Smart Log
Smart Event	Se configurarán reportes programados de Application Control y URL Filtering para que estos sean enviados por correo electrónico al correo interno. Estos reportes entregan un resumen: Sitios más visitados, Usuarios con mayor consumo de AB, etc.

Tabla 11. (López J. F., 2016) Funcionalidades Reportería

Configuración Application Control y URL Filtering:

Grupos de Acceso (DA)	Descripción
ACCESOTOTAL	GRUPO DE ACCESO ILIMITADO
INTERMEDIO	GRUPO DE ACCESO INTERMEDIO
BASICO	GRUPO DE ACCESO LIMITADO
NO-ACCESO-INTERNET	GRUPO SIN INTERNET

Tabla 12. (López J. F., 2016) Perfiles de navegación de Internet

Donde cada grupo de acceso tiene permitido o bloqueado el acceso a Internet en base a categorías definidas por la solución, las cuales pueden ser modificadas según las políticas de seguridad establecidas, ANEXO #2 documento “Categorías de Navegación”.

Es importante tomar en cuenta a dominios como *.gob.ec, *.fin.ec, *.edu.ec, etc., y crear listas blancas, donde se puedan incluir sitios y dominios de libre acceso.

4.3.1.3 Políticas de Seguridad

Una parte importante dentro de la implementación de la nueva solución de seguridad fue la migración, depuración y creación de las políticas o reglas de seguridad. Una de las ventajas de la nueva solución es el manejo eficiente y sencillo de las políticas de seguridad, de igual manera el rendimiento al momento de procesar una regla.

Las políticas que hacen referencia a los servicios más importantes del MDMQ se las coloco en las primeras posiciones, para aligerar y mejorar el rendimiento al momento de procesar las reglas. Como una buena práctica, se crearon reglas recomendadas por el fabricante, para reforzar la seguridad en la solución.

El proceso de depuración de las políticas que se migraron, ha sido un proceso paulatino, el cual consiste en deshabilitar la regla que no presenta ningún hit, sin embargo, como medida preventiva la regla permanece deshabilitada durante un periodo de tiempo específico (1 mes) antes de ser eliminada.

En base a los resultados desprendidos en el análisis de las vulnerabilidades y amenazas, se crearon nuevas políticas de seguridad para fortalecer la seguridad y mitigar las amenazas y vulnerabilidades, a continuación, se presenta una pequeña reseña del esquema de políticas del firewall:

Ilustración 26. (López J. F., 2016) Políticas de Seguridad

Para la navegación, se ha creado un conjunto de políticas, las cuales se encuentran aplicadas en base a los perfiles de usuario a través del directorio activo y por IP, de la misma forma se han creado algunas excepciones las cuales se aplican a un conjunto

de equipos que forman parte de la granja de servidores, listas negras, listas blancas, etc. así como también equipos con funcionalidades especiales.

Debido a que este control se está implementando con esta solución de seguridad, no se ha migrado ninguna regla de otra solución similar. De la misma forma se ha aplicado buenas practicas recomendadas por el fabricante en cuanto al posicionamiento de las reglas, procurando mejorar el rendimiento y procesamiento de la solución, quedando de esta forma el esquema de políticas:

Policy

Type to Search | Hit Count

No.	Hits	Name	Source	Destination	Applications/Sites	Action	Track
2	2G	Permisos Internos	Any	Redes_Privadas	Any Recognized	Allow	None
3	19M	Sitios Publicos	Any	Internet	White-List Aplicaciones-Pe...	Allow	Log
4	403I	Secretaria de Comunicacion	GRP-COMUNIC...	Internet	Aplicaciones-Se...	Allow Lim-2MB Down: 2 Mbps |...	Log
5	162I	Permisos Generales por IP	Any	PublicasPermiti...	Any Recognized	Allow	Log
6	3M	Permitido Acceso Office 365	Any	Internet	AplicacionesMic...	Allow	Log
7	32M	Bloqueos Generales	Any	Internet	Bloqueos-Basicos	Block Blocked Message	Log
8	32M	Permisos Generales	Any	Internet	Permisos-Basicos	Allow	Log
9	58	Contenido multimedia del ICAM	Host_[redacted]	Internet	Mega	Allow Lim-1M Down: 1 Mbps |...	Log
10	2K	Streaming Sala del Consejo	Srv_[redacted]	Internet	Any Recognized	Allow Lim-2MB Down: 2 Mbps |...	Log
42	6M	Rate Limit Youtube y FB	ACCESO-TOTAL	Internet	Media Streams YouTube	Allow Lim-50M Down: 50 Mbps...	Log
43	113I	Permitido Acceso Total	ACCESO-TOTAL	Internet	Any Recognized	Allow Identity Captive ...	Log
44	2K	Permitido Redes Sociales	REDES-SOCIALES	Internet	HTTP Video	Allow Lim-2MB Down: 2 Mbps |...	Log
45	2M	Bloqueo Redes Sociales	REDES-SOCIALES	Internet	Redes-Sociales	Block Blocked Message	Log
46	7M	Permitido Redes Sociales	REDES-SOCIALES	Internet	Any Recognized	Allow Identity Captive ...	Log
47	2M	Bloqueos Intermedios	INTERMEDIO	Internet	Intermedio	Block Blocked Message	Log
48	16M	Permitido Intermedio	INTERMEDIO	Internet	Any Recognized	Allow Identity Captive ...	Log
49	36M	Bloqueo Basico	BASICO	Internet	Basico	Block Blocked Message	Log
50	139I	Permitido Basico	BASICO	Internet	Any Recognized	Allow Identity Captive ...	Log

Ilustración 27. (López J. F., 2016) Políticas de Navegación

4.3.2 IPS

La solución de seguridad IPS será colocada de forma inline, para protección de los segmentos de red correspondientes a la: INSIDE, RTM (WAN), OUTSIDE y DMZ.

4.3.2.1 HP TippingPoint 2600NX

El IPS 2600NX cuenta con un rendimiento máximo de throughput de 3Gbps; sumando el tráfico que circula a través de todas sus interfaces de monitoreo.

El equipo 2600NX cuenta con 4 slots modulares, de los cuales actualmente se encuentra utilizado un slot con un módulo de 4 segmentos en cobre (RJ45) con bypass, quedando aun libres tres slots para crecimiento futuro.

La solución, realizará la protección en línea (IPS) de cuatro (04) segmentos de red tipo RJ45 a una velocidad de 1GB

Los puertos de monitoreo serán configurados en modalidad In-Line con bypass habilitado en los puertos de monitoreo. Esta configuración permite, que al fallar el IPS, el tráfico fluya sin ninguna interrupción.

La versión de software a instalarse es la más reciente y estable disponible TippingPoint Operating System (TOS) 3.8.1.4382.

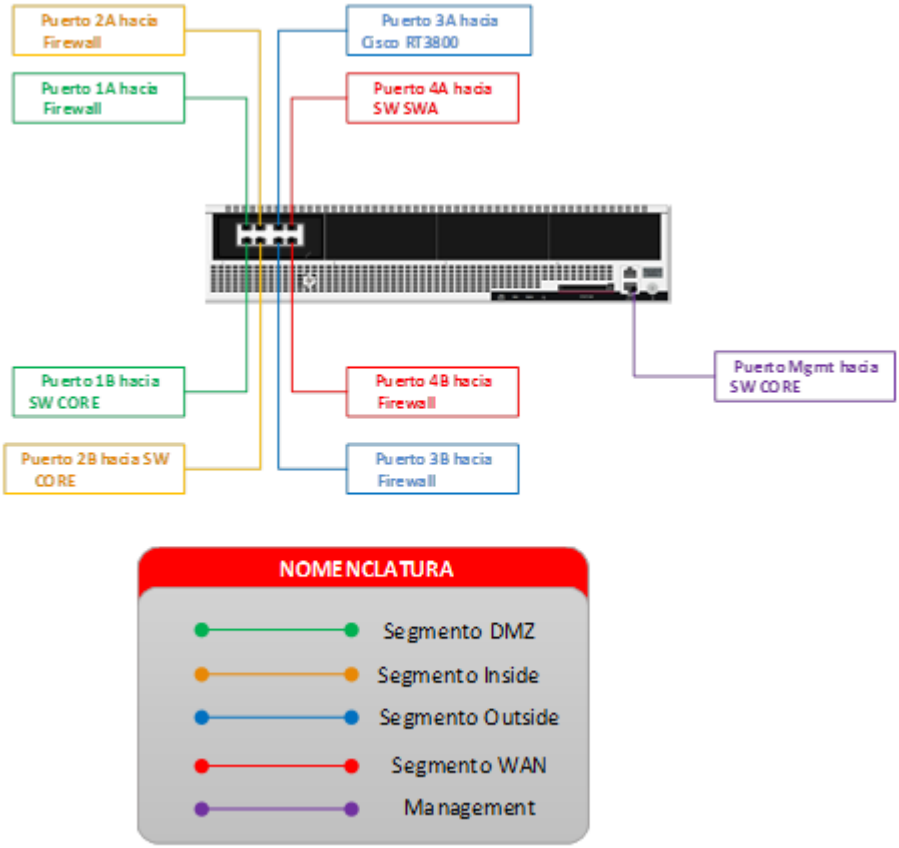

Ilustración 28. (López J. F., 2016) Diagrama de Conexión IPS

4.3.2.2 HP SMS

La administración del equipo IPS estará bajo el hardware SMS HP TippingPoint H3 Appliance y el software SMS 4.3.0.50865 más reciente y estable.

Cuenta con una capacidad de gestión de 25 IPS por parte de la consola de gestión centralizada (SMS).

La consola de gestión centralizada permitirá la configuración y monitoreo de varios dispositivos, siempre y cuando el dispositivo sea compatible con el fabricante.

Se aplicarán configuraciones de firmas de seguridad según la categoría de la firma, filtro de seguridad y al conjunto de acciones.

En base al tipo de tráfico detectado en las diferentes interfaces (INSIDE, WAN, OUTSIDE y DMZ) se crearán nuevos perfiles de seguridad, las cuales se aplicarán a su respectiva interface para la inspección, las mismas que pueden ser distribuidos a diferentes IPS o grupos de segmentos, en este caso a los 4 definidos.

Group Name	Profile
Default	Default
SG_INSIDE	IP_INSIDE
SG_OUTSIDE	IP_OUTSIDE
SG_DMZ	IP_DMZ
SG_WAN	IP_WAN

Ilustración 29. (López J. F., 2016) Segmentos de Red

Group	Category	State	Locked	Action Set
Application Protection	Exploits	✓	○	Block + Notify
Application Protection	Identity Theft	✓	○	Recommended
Application Protection	Reconnaissance	✓	○	Recommended
Application Protection	Security Policy	✓	○	Recommended
Application Protection	Spyware	✓	○	Block + Notify
Application Protection	Virus	✓	○	Recommended
Application Protection	Vulnerabilities	✓	○	Block + Notify
Infrastructure Protection	Network Equipment	✓	○	Recommended
Infrastructure Protection	Traffic Normalization	✓	○	Recommended
Performance Protection	IM	✓	○	Recommended
Performance Protection	P2P	✓	○	Recommended
Performance Protection	Streaming Media	✓	○	Recommended

Ilustración 30. (López J. F., 2016) Perfil Segmento INSIDE

Group	Category	State	Locked	Action Set
Application Protection	Exploits	✓	○	Block + Notify
Application Protection	Identity Theft	✓	○	Recommended
Application Protection	Reconnaissance	✓	○	Recommended
Application Protection	Security Policy	✓	○	Recommended
Application Protection	Spyware	✓	○	Block + Notify
Application Protection	Virus	✓	○	Recommended
Application Protection	Vulnerabilities	✓	○	Block + Notify
Infrastructure Protection	Network Equipment	✓	○	Recommended
Infrastructure Protection	Traffic Normalization	✓	○	Recommended
Performance Protection	IM	✓	○	Recommended
Performance Protection	P2P	✓	○	Recommended
Performance Protection	Streaming Media	✓	○	Recommended

Ilustración 31. (López J. F., 2016) Perfil Segmento WAN

Group	Category	State	Locked	Action Set
Application Protection	Exploits	✓	○	Block + Notify
Application Protection	Identity Theft	✓	○	Recommended
Application Protection	Reconnaissance	✓	○	Recommended
Application Protection	Security Policy	✓	○	Recommended
Application Protection	Spyware	✓	○	Block + Notify
Application Protection	Virus	✓	○	Block + Notify
Application Protection	Vulnerabilities	✓	○	Block + Notify
Infrastructure Protection	Network Equipment	✓	○	Recommended
Infrastructure Protection	Traffic Normalization	✓	○	Recommended
Performance Protection	IM	✓	○	Recommended
Performance Protection	P2P	✓	○	Recommended
Performance Protection	Streaming Media	✓	○	Recommended

Ilustración 32. (López J. F., 2016) Perfil Segmento OUTSIDE

Group	Category	State	Locked	Action Set
Application Protection	Exploits	✓	○	Block + Notify
Application Protection	Identity Theft	✓	○	Recommended
Application Protection	Reconnaissance	✓	○	Recommended
Application Protection	Security Policy	✓	○	Recommended
Application Protection	Spyware	✓	○	Block + Notify
Application Protection	Virus	✓	○	Recommended
Application Protection	Vulnerabilities	✓	○	Block + Notify
Infrastructure Protection	Network Equipment	✓	○	Recommended
Infrastructure Protection	Traffic Normalization	✓	○	Recommended
Performance Protection	IM	✓	○	Recommended
Performance Protection	P2P	✓	○	Recommended
Performance Protection	Streaming Media	✓	○	Recommended

Ilustración 33. (López J. F., 2016) Perfil Segmento DMZ

Desde la consola de gestión centralizada se tienen los diferentes sistemas operativos de IPS, desde la cual se pueden hacer despliegues los mismos a los diferentes IPS de forma centralizada.

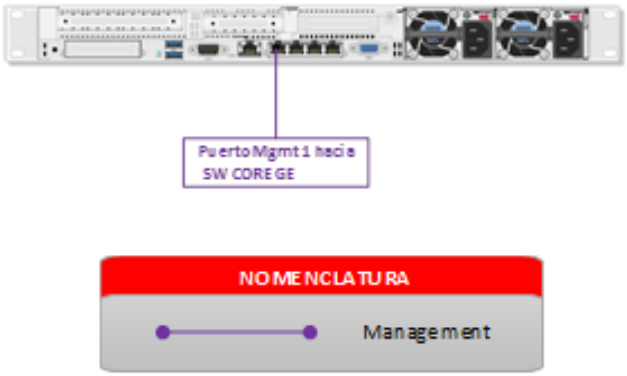

Ilustración 34. (López J. F., 2016) Diagrama de Conexión SMS

4.4 Mejoras y Beneficios

Una vez realizada la implementación de los nuevos elementos de seguridad junto con el nuevo esquema de conectividad, se crea una base fundamental que inicia la cultura de seguridad dentro del MDMQ, con una base más robusta y tecnologías de última generación.

Los nuevos controles de seguridad han permitido cerrar brechas de seguridad, identificadas sobre la antigua infraestructura del MDMQ a través de la herramienta Kali Lunix sobre algunos servicios internos y externos, tales como:

4.4.1 Servicios Públicos

Servicio de VPN

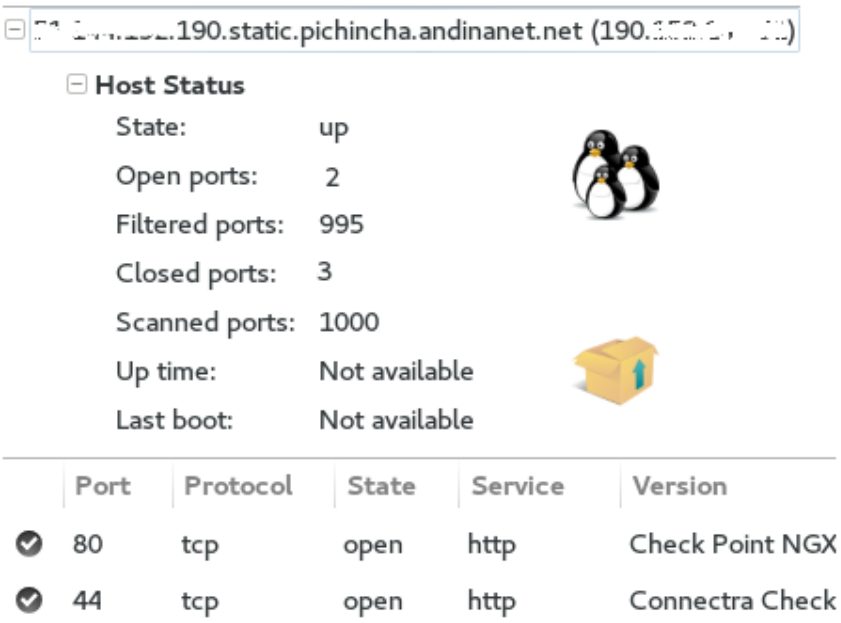

Ilustración 35. (López J. F., 2016) IP Publica servicio de VPN

Sitio web

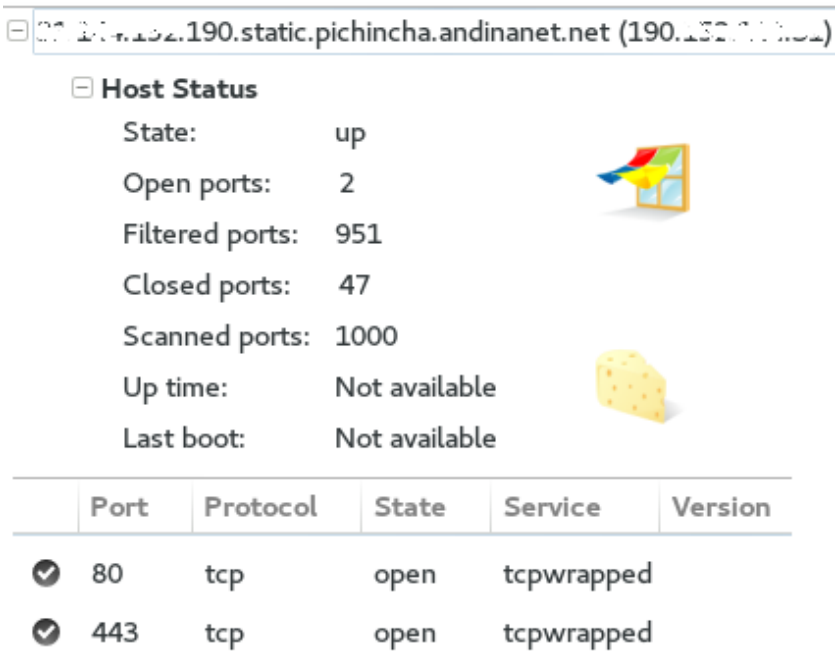

Ilustración 36. (López J. F., 2016) IP pública sitio web

4.4.2 Servicios Privados

Directorio Activo

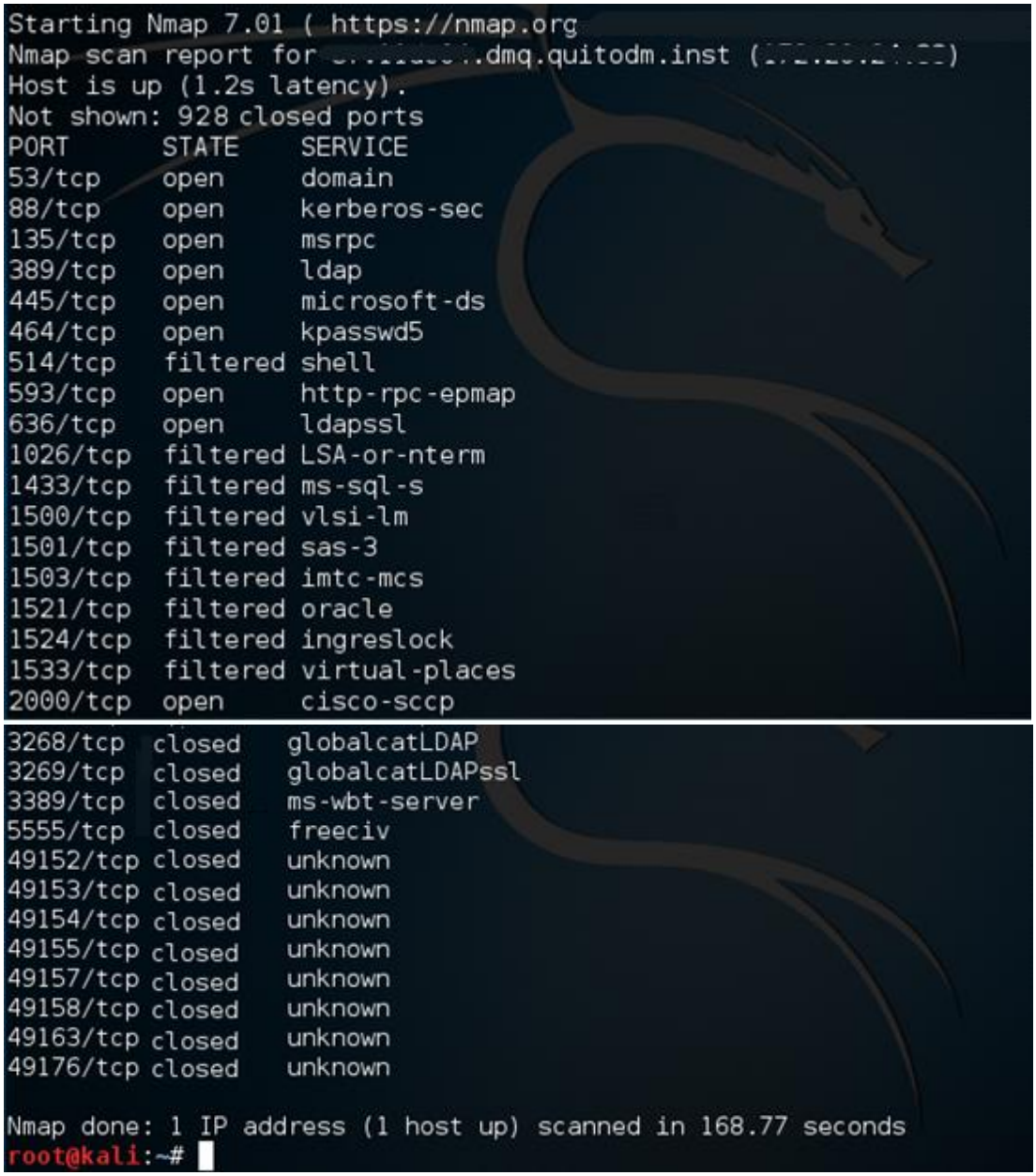

Ilustración 37. (López J. F., 2016) IP Servicio del DA

Sitio Web

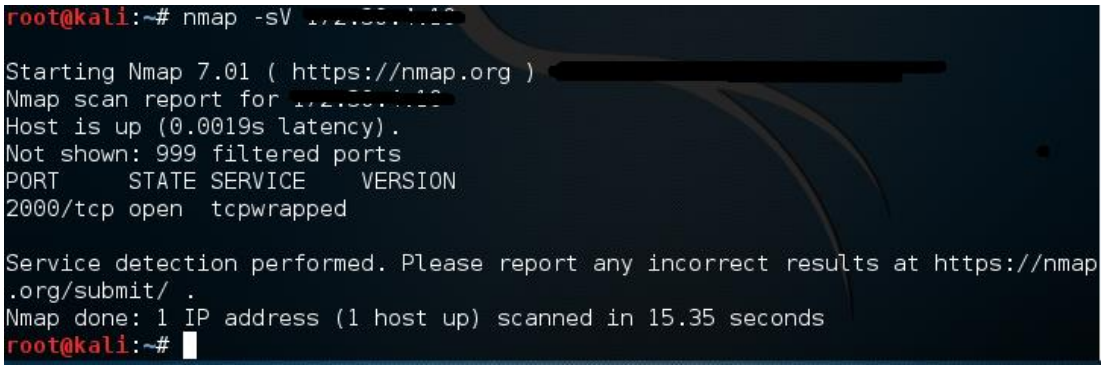

Ilustración 38. (López J. F., 2016) IP Sitio web interno

El servicio de navegación sufrió un considerable cambio, debido a la implementación de nuevas políticas de seguridad y la implementación de un servicio más granular y avanzado en la detección del tráfico de navegación a Internet. Se realiza un mayor control en la navegación y los sitios web de contenido prohibido están siendo bloqueados. Los resultados del escaneo se encuentran en el ANEXO #3 documento "Web Content Security Validaton Report after".

Adicionalmente, la nueva infraestructura tecnológica implementada brinda los siguientes beneficios y mejoras:

- Esquema de conectividad simplificado y convergente.
- Esquema de conectividad que alcanzan velocidades de hasta 10G.
- Alto nivel de seguridad.
- Soluciones avanzadas e integradas.
- Gestión y administración centralizada.
- Soluciones escalables y en alta disponibilidad (software y hardware).
- Flexibilidad, manejabilidad, seguridad total y rendimiento garantizado.
- Gestión y monitoreo de múltiples gateways que cubren la seguridad perimetral.

- Correlacionador de eventos para analizar la seguridad y prevenir futuros ataques.
- Prestaciones avanzadas de red, enrutamiento, inspección, detección y prevención.
- Mecanismo de control de aplicaciones y filtrado web que optimizará el servicio de Internet que dispone el MDMQ para sus usuarios internos y externos.
- Mecanismos automáticos contra caídas o fallas.
- Políticas de seguridad y controles de navegación que evitan el mal uso del servicio y saturación del canal de Internet.
- Acelerada detección, identificación y mitigación de amenazas a la seguridad de la red interna y externa.
- Garantizan la continuidad del negocio.
- Acceso a fuentes de investigación (DVLabs) para la identificación, mitigación o bloqueo de las últimas vulnerabilidades de seguridad.
- Gestión, administración y personalización sencillas y amigables.
- Depuración y simplificación de reglas o políticas de seguridad.
- Completa integración con el directorio activo del MDMQ.
- Manejo de políticas de seguridad a través del directorio activo.
- Infraestructura tecnológica más robusta.
- Servicios de seguridad de última generación, alto rendimiento y tecnología de punta.
- Balanceo de carga de dos o más ISPs.

- Comunicación vía VPN SSL o IPSec más seguros y amigables para el usuario final.
- Total integración de sistemas, elementos o dispositivos de la infraestructura tecnológica.

4.5 Costos

4.5.1 Solución de Firewall

4.5.1.1 Equipamiento, garantías e implementación

Se ha solicitado a cuatro empresas reconocidas a nivel nacional, que emitan sus propuestas de productos y servicio, relacionado a la Adquisición de una Solución Firewall y Filtrado WEB.

A continuación se muestra un comparativo de las ofertas presentadas por las empresas, basado en la información recibida de cada una de ellas.

Empresa	Oferta
Andean Trade	$ 259.319,00
EBTeL	$ 261.179,54
MEGASUPPLY	$ 264.972,00
Comunicaciones Gold Partner	$ 259.260,00
Valor promedio	$ 260.432,64

Tabla 13. (López J. F., 2016) Valores Referenciales Solución Firewall

Para la adquisición de equipamiento, garantías e implementación se ha obtenido el valor promedio de las ofertas presentadas dando como resultado $ 260.432,64 (Doscientos sesenta mil cuatrocientos treinta y dos dólares de los Estados Unidos de América con sesenta y cuatro centavos, valor que no incluye IVA.

4.5.1.2 Mantenimiento

A continuación se muestra un comparativo de las ofertas presentadas por las empresas, basado en la información recibida de cada una de ellas.

Empresa	Año 2016	Año 2017	Año 2018	Total Oferta
Andean Trade	$1 .200,00	$1 .200,00	$1 .200,00	$ 3.600,00
MEGASUPPLY	$1 .300,00	$1 .300,00	$1 .300,00	$ 3.900,00
Comunicaciones Gold Partner	$1 .000,00	$1 .000,00	$1 .000,00	$ 3.000,00
Valor Promedio	$ 1.166,67	$ 1.166,67	$ 1.166,67	**$ 3.500,00**

Tabla 14. (López J. F., 2016) Valores de Mantenimiento de la Solución de Firewall

Para el Mantenimiento Anual (tres años en total) se ha obtenido el valor promedio de las ofertas presentadas dando como resultado $ 3.500,00 (Tres mil quinientos dólares de los Estados Unidos de América con cero centavos, valor que no incluye IVA.

4.5.1.3 Resumen Económico

Ítem	Total
Equipamiento, garantías e implementación	$ 260.432,64
Mantenimiento	$ 3.500,00
Total	**$ 263.932,64**

Tabla 15. (López J. F., 2016) Resumen Económico Solución de Firewall

4.5.2 Solución de IPS

4.5.2.1 Equipamiento, garantías e implementación

Se ha solicitado a tres empresas reconocidas a nivel nacional, que emitan sus propuestas de productos y servicio, relacionado a la Adquisición de una Solución de IPS.

A continuación se muestra un comparativo de las ofertas presentadas por las empresas, basado en la información recibida de cada una de ellas.

EMPRESA	OFERTA
Binaria Sistemas S.A	$ 138.930,00
Point Technical Soluciones Cía. Ltda.	$ 140.480,00
Comercio y Asesoría COMASE Cía. Ltda.	$ 132.390,00

Tabla 16. (López J. F., 2016) Valores referenciales Solución IPS

Para la adquisición de equipamiento, garantías e implementación se ha obtenido el valor más bajo de las ofertas presentadas dando como resultado $ 132.390,00 (Ciento treinta y dos mil trescientos noventa dólares de los Estados Unidos de América con cero centavos, valor que no incluye IVA.

4.5.2.2 Mantenimiento

A continuación se muestra un comparativo de las ofertas presentadas por las empresas, basado en la información recibida de cada una de ellas.

Empresa	Año 2016	Año 2017	Año 2018	Total Oferta
Binaria Sistemas S.A	$ 240,00	$ 240,00	$ 240,00	$ 720,00
Point Technical Soluciones Cía. Ltda.	$ 260,00	$ 260,00	$ 260,00	$ 780,00
Comercio y Asesoría COMASE Cía. Ltda.	$ 200,00	$ 200,00	$ 200,00	$ 600,00
Valor Promedio	$ 233,33	$ 233,33	$ 233,33	**$ 700,00**

Tabla 17. (López J. F., 2016) Valores referenciales mantenimiento Solución IPS

Para el Mantenimiento Anual (tres años en total) se ha obtenido el valor promedio de las ofertas presentadas dando como resultado $ 700,00 (Setecientos dólares de los Estados Unidos de América con cero centavos.

4.5.2.3 Resumen Económico

Ítem	Total
Equipamiento, garantías e implementación	$ 132.390,00
Mantenimiento	$ 700,00
Total	**$ 133.090,00**

Tabla 18. (López J. F., 2016) Resumen Económico Solución IPS

4.5.3 Presupuesto Referencial

Basado en el estudio económico realizado, el presupuesto referencial para la implementación de las nuevas soluciones de seguridad es de trescientos noventa y siete mil veinte y dos con 64/100 dólares de los Estados Unidos de América (US$397.022,64) más IVA.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Durante el análisis de la Infraestructura Tecnológica del MDMQ, se constató y evidenció que el Municipio de Quito carece de equipamiento de seguridad con la cual pueda asegurar la integridad, confidencialidad y la disponibilidad de la información, así como también de los diferentes servicios que el Municipio brinda a la ciudadanía. Todo esto sumado a la falta de una cultura de seguridad de la información, hacen que la infraestructura sea un punto vulnerable y fácil de atacar, y el usuario ya sea interno o externo pueda ser víctima de algún delito asociado al robo de la información.

Adicional a esto, la infraestructura tecnológica del MDMQ, no cuenta con mecanismos o sistemas de seguridad de última generación con métodos de aseguramiento o resguardo de la información capaces de soportar, mitigar, bloquear y detectar cualquier tipo de ataque avanzado y complejo. En cuanto al esquema de conectividad del MDMQ, luego del análisis, se evidenció que posee puntos vulnerables, brechas de seguridad, equipamiento innecesario, puntos de acceso no controlados y carece de esquemas redundantes (físicas y lógicas) y contingentes, que de igual forma, pasan a formar parte al grupo de falencias que lo vuelven vulnerable.

La carencia de un área especializada y dedicada a generar, aplicar, mantener y promover el cumplimiento de políticas y normas de seguridad, y gestión de riegos

que ayuden a proteger y asegurar los recursos y servicios del MDMQ, así como también garantizar que la información esté protegida, y así la integridad, la confidencialidad y la disponibilidad de esta, minimizando los riesgos y las amenazas a la privacidad de los datos o amenazas a la seguridad, las cuales pueden traer efectos negativos para el MDMQ, y hacen al MDMQ un blanco aún más fácil de atacar y vulnerar.

En base al análisis realizado, y en conjunto con las diferentes áreas de tecnología del MDMQ directamente relacionados con la IT, se definió las necesidades y requerimientos fundamentales para iniciar un proceso de cambio y renovación completa de la IT en temas de seguridad. El MDMQ requiere la implementación de soluciones de seguridad IT con características avanzadas que supervise de manera continua la IT, con la capacidad de controlar y proteger de manera centralizada la infraestructura de TI, como también la facultad de responder de forma inmediata a cambios que pudieran quebrantar la seguridad IT.

Características avanzadas como:

- Alta disponibilidad (físico y lógico)
- Balanceo de Carga y calidad de servicio.
- Tecnología y equipamiento de última generación.
- Sistemas de detección, mitigación y bloqueo de cualquier tipo de ataque informático.
- Sistemas de control de acceso, filtrado web y control de aplicaciones.
- Convergencia, escalabilidad y estabilidad.
- Soluciones robustas y de alto rendimiento.

- Servicios de VPN seguras.
- Soporte especializado de fábrica.
- Cuenten con el respaldo de laboratorios internacionales de investigación, pruebas y desarrollo de vacunas, parches y actualización de la base de datos para minimizar, neutralizar o bloquear las amenazas y vulnerabilidades.

La implementación de las soluciones de seguridad parte inicialmente en la selección de la solución adecuada para cubrir con todas las necesidades y requerimientos que el MDMQ tiene y que nacen en base a los diferentes servicios que brinda a la ciudadanía y a sus usuarios internos, los diferentes elementos físicos y lógicos con las que cuenta la IT, la carga transaccional e información que genera, así como también del presupuesto con el que cuenta para este fin, siendo este una gran limitante.

La implementación de la nueva infraestructura de seguridad propuesta en este estudio, da como resultado, el inicio del proceso de cambio en temas de seguridad y protección de la información, y el inicio de una cultura de seguridad en el MDMQ. Todo bajo una nueva base o core de seguridad de última generación acompañado de servicios de alto rendimiento que servirán como un justificativo para mantener un ciclo de renovación de otras tecnologías y mantenerse a la par del desarrollo tecnológico.

Los resultados obtenidos se los puede evidenciar tanto en el diseño como en la arquitectura implementada, así como también en los nuevos servicios implementados. Todo esto ha permitido cerrar y minimizar brechas de seguridad evidenciados y encontrados en los diferentes servicios del MDMQ, fortaleciendo y

asegurando la integridad, confidencialidad y la disponibilidad de la información, así como también de los diferentes servicios que brinda a la ciudadanía, cumpliendo con el objetivo general y específicos planteados.

5.2 Recomendaciones

El tiempo de vigencia (3años) de los servicios de garantías y mantenimientos presentados en este estudio, se establecieron en base a los lineamientos del Servicio Nacional de Compras Públicas SERCOP, sin embargo, y debido al limitante en el presupuesto, no se incluyó dentro de la propuesta de los diferentes proveedores el servicio de soporte especializado de fábrica, únicamente se consideró el soporte especializado brindado por el canal, que en términos generales cumplen un SLA de 8X5XNBD. Tema que se debe considerar dentro del plan anual de contratación para su adquisición.

Así mismo, y por la misma razón, la propuesta no incluye ningún tipo de capacitación formal de fábrica para el personal técnico que administra la IT, lo cual genera un gasto adicional para el MDMQ ya que requiere de soporte especializado a través del canal, tema que igualmente debe ser considerado en el PAC. Contar con personal especializado dentro de la institución garantizan el correcto funcionamiento y administración de la infraestructura tecnológica implementada y sobre todo que las funciones del personal sean de ingeniería.

Es fundamental que, dentro de este nuevo proceso de cambio, se cree un área dentro de la Dirección de Tecnología del MDMQ, cuyo objetivo sea la Seguridad de las Tecnologías de la Información, y que sus competencias estén enfocadas en:

- Procedimientos de Ethical hacking o hardening.
- Administración de Riesgos.
- Regulador y generador de políticas y normas de seguridad.
- Campañas de seguridad
- Capacitación en temas de seguridad
- Determinar la infraestructura crítica y los riesgos del negocio
- Analizar las vulnerabilidades sobre la infraestructura tecnológica.

Las soluciones de seguridad presentadas en este caso de estudio, cuentan con mayores prestaciones y funcionalidades, las cuales no han sido tomadas en cuenta debido a que actualmente no son necesarias, se recomienda realizar un análisis de las ventajas y costos de activar estos servicios en una segunda fase, como parte de un fortalecimiento de las prestaciones de las soluciones de seguridad.

BIBLIOGRAFÍA

- Ayala G., G., & Gómez, J. (2011). *GUÍA DE BUENAS PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN EN CONTEXTOS DE MICRO, PEQUE,A Y MEDIANAS EMPRESAS DE LA REGIÓN.* Pereira.
- Barrera, D. A. (2011). *PLAN DE DESARROLLO 2012 – 2022.* Quito.
- Checkpoint. (2016). *Url Categories*. Obtenido de https://www.checkpoint.com/urlcat/categories.htm
- Computerworld. (2015). Seguridad de la Información. *Computerworld*.
- DTe. (2015). *Universidad de Sevilla.* Obtenido de https://www.dte.us.es/docencia/etsii/gii-ti/tecnologias-avanzadas-de-la-informacion
- Flórez R., W., Arboleda S., C., & Cadavid A., J. (2012). *SOLUCIÓN INTEGRAL DE SEGURIDAD PARA LAS PYMES MEDIANTE UN UTM.* Obtenido de http://web.usbmed.edu.co/usbmed/fing/v3n1/v3n1a4.pdf
- Fortinet. (2015). *Fortinet High Perfonance Network Security*. Obtenido de https://www.fortinet.com/
- FUOC. (2007). *Universitat Oberta de Catalunya.* Obtenido de Mecanismos para la detección de ataques e intrusiones: http://ocw.uoc.edu/computer-science-technology-and-multimedia/advanced-aspects-of-network-security/advanced-aspects-of-network-security/P06_M2107_01773.pdf
- Giménez, M. I. (2008). Utilización de Sistemas de Detección de Intrusos como Elemento de Seguridad Perimetral. Almeria.
- Gómez, Á. (s.f.). TIPOS DE ATAQUES E INTRUSOS EN LAS REDES INFORMÁTICAS.
- Kali. (2015). *Kali Linux*. Obtenido de http://www.kali.org

- Kaspersky Lab. (2016). *Amenazas de seguridad en Internet*. Obtenido de http://www.kaspersky.es/internet-security-center/threats/all-articles
- Kaspersky Lab. (2016). *Types of Malware*. Obtenido de http://latam.kaspersky.com/mx/internet-security-center/threats/malware-classifications
- Laudon, K., & Laudon, J. (2012). *SISTEMAS DE INFORMACIÓN GERENCIAL*. PEARSON.
- López, I. J. (2015). *Infraestructura Tecnológica del Municipio del Distrito Metropolitano de Quito.* Quito.
- López, J. F. (2016). *Infraestructura Tecnológica del Municipio del Distrito Metropolitano de Quito.* Quito.
- Mieres, J. (2009). Buenas prácticas en seguridad informática. *ESET*, 3.
- Miller, R. (2012). *CA Technologies.* Obtenido de http://www.ca.com/~/media/Files/whitepapers/latam/CS2548_advanced_persistent_threats_wp_0712_las.pdf
- Netmedia. (2016). *b: Secure Conference*. Obtenido de http://www.netmedia.mx
- Northcutt, S., Zeltser, L., Winters, S., Kent, K., & W. Ritchey, R. (2005). *Inside Network Perimeter Security.* Sams Publishing.
- Oficina Nacional de Tecnologías de Información. (2005). Modelo de Política de Seguridad de la Información para Organismos de la Administración Pública Nacional. Argentina.
- Piraquive, F. N. (2008). Principales estándares para la seguridad de la información IT. *EOS*.
- Quezada, A. E. (2015). *Hacking con Kali Linux.* Obtenido de http://www.reydes.com/archivos/Kali_Linux_v2_ReYDeS.pdf

- Rodas, M. (2014). *Propuestas Alcaldía de Quito.* Obtenido de http://www.quito.gob.ec
- Symantec. (2016). *Glosario de Seguridad*. Obtenido de https://www.symantec.com
- TIC. (2015). *Evaluación de Riesgos en Tecnologías de Información.* Obtenido de http://docplayer.es/4514471-Anexo-ntp3-evaluacion-de-riesgos-en-tecnologias-de-informacion.html

ANEXOS

ANEXO #1

Amenazas y Vulnerabilidades del MDMQ

AMENAZA / VULNERABILIDAD	IMPLICANCIA DE SEGURIDAD
Actividades de hackers o crackers	• Afectación en la disponibilidad, integridad y confidencialidad de la información. • Delitos cibernéticos. • Afectación en la disponibilidad de los servicios. • Daños en la infraestructura tecnológica. • Funcionalidades deshabilitadas de sistemas o servicios.
Ejecución de malwares	• Infección y propagación de virus dentro la infraestructura tecnológica. • Explotación de vulnerabilidades. • Ataques internos. • Phishing. • Comportamientos anómalos dentro de la IT. • Afectación de sistemas, equipos o redes. • Bajo rendimiento y lentitud. • Perdida de información.

AMENAZA / VULNERABILIDAD	IMPLICANCIA DE SEGURIDAD
Fuga de información	• Filtración de información. • Envió de información confidencial a fuentes externas (Internet). • Perdida de información. • Sustracción de información sin autorización. • Robo y secuestro de información.
Suplantación de Identidad	• Filtración de datos de usuarios. • Control de Accesos a recursos no autorizados. • Espiar la actividad de los usuarios. • Modificación de información.
Hardware y Software redundantes	• Falla de componentes de hardware, que afecte la disponibilidad de los servicios. • Falla de software, que afecte la disponibilidad de los servicios.
Esquema en alta disponibilidad	• Afectación en la disponibilidad de los servicios. • Procedimientos y cambios manuales de la infraestructura tecnológica.

AMENAZA / VULNERABILIDAD	IMPLICANCIA DE SEGURIDAD
Filtrado web y control de aplicaciones	• Accesos no autorizados hacia Internet. • Fuga de Información. • Actividades ilegales a través de Internet. • Uso de aplicativos no autorizados. • Navegación a sitios de maliciosa reputación. • La falta de herramientas de inspección de contenido.
Tecnologías obsoletas	• Equipamiento que no cuenta con tecnologías actuales, que permitan identificar, detectar y mitigar nuevas formas de vulnerar la seguridad. • Equipamiento con escasas características de software y hardware. • Sobrecarga de procesamiento.

AMENAZA / VULNERABILIDAD	IMPLICANCIA DE SEGURIDAD
Políticas de seguridad	• Falta de normas o procedimientos de seguridad establecidos. • Falta de políticas de seguridad, administración de seguridad, así como implementación de controles o configuraciones de seguridad. • Falta de una adecuada capacitación y orientación en seguridad de la información. • Tareas, actividades o procedimientos sin controles de seguridad.
Sistema de prevención de intrusos	• Perfiles con firmas obsoletas, no inspeccionan, nuevas tecnologías de penetración. • Falta de detección de tráfico malicioso, mediante mecanismos de identificación de reputación y geo posicionamiento.
Redes inalámbricas	• Esquemas de red sin medidas de seguridad. • Segmentos de red con accesos hacia la red interna, externa o Internet. • Falta de controles para el acceso de dispositivos inteligentes.

AMENAZA / VULNERABILIDAD	IMPLICANCIA DE SEGURIDAD
Arquitectura de Red	• Acceso a la red interna a través de redes externas sin la debida protección, y viceversa. • Huecos de seguridad en los servicios expuestos al Internet para el acceso público.

Tabla 19. (López I. J., 2015) Análisis de Vulnerabilidades

Análisis de Riesgos

DESCRIPCION DEL RIEGO	IMPACTO	CATEGORIA
Ausencia de esquemas en alta disponibilidad	MAYOR	INFRAESTRUCTURA
Redes inalámbricas inseguras	SIGNIFICATIVO	OPERACION
Danos de hardware en la IT	IMPORTANTE	INFRAESTRUCTURA
Danos de software en la IT	IMPORTANTE	OPERACION
Equipamiento de la IT obsoleto	MAYOR	GESTION
Sistemas obsoletos o desactualizados	SIGNIFICATIVO	OPERACION
Ausencia de equipamiento de seguridad con tecnologías actuales de detección y prevención.	MAYOR	GESTION
Ausencia de herramientas para filtrado web	SIGNIFICATIVO	SEGURIDAD
Ausencia de herramientas para control de aplicaciones	SIGNIFICATIVO	SEGURIDAD
Ausencia de herramientas de control de identidad	SIGNIFICATIVO	SEGURIDAD

DESCRIPCION DEL RIEGO	IMPACTO	CATEGORIA
Los recursos de la IT no soportan la carga que demandan los servicios	IMPORTANTE	GESTION
Ausencia de equipamiento para la detección y prevención de intrusos.	MAYOR	GESTION
Suspensión de los servicios	MAYOR	INFRAESTRUCTURA
Caída de servicios web	IMPORTANTE	INFRAESTRUCTURA
Fallas de equipamiento de comunicaciones dentro de la IT	IMPORTANTE	INFRAESTRUCTURA
Fallas de equipamiento computacional del datacenter.	MAYOR	INFRAESTRUCTURA
Ausencia de políticas de seguridad	SIGNIFICATIVO	OPERACION
Ausencia de controles de seguridad	SIGNIFICATIVO	OPERACION
Falta de herramientas de detección de incidentes	SIGNIFICATIVO	OPERACION
Accesos no autorizados a la información	SIGNIFICATIVO	SEGURIDAD
Accesos no autorizados a la red interna municipal	SIGNIFICATIVO	SEGURIDAD
Arquitectura de seguridad desactualizada	IMPORTANTE	INFRAESTRUCTURA
Falta de herramientas de administración y gestión de la IT	IMPORTANTE	INFRAESTRUCTURA
Accesos a la red municipal de dispositivos inteligentes (IoT)	SIGNIFICATIVO	INFRAESTRUCTURA
El personal técnico no está capacitado para manejar una incidencia.	IMPORTANTE	RECURSOS HUMANOS

DESCRIPCION DEL RIEGO	IMPACTO	CATEGORIA
Falta de capacitación a los usuarios en temas de seguridad	REGULAR	RECURSOS HUMANOS
Falta de un plan de acción y contingencia, durante y al final de una incidencia	MAYOR	RECURSOS HUMANOS

Tabla 20. (López I. J., 2015) Análisis de Riesgos

ANEXO #2

Categorías de Navegación

GRUPO DE ACCESO	
Categoría	**Permitido / Bloqueado**
Alcohol	
Anonymizer	
Art / Culture	
Blogs / Personal Pages	
Botnets	
Business / Economy	
Child Abuse	
Computers / Internet	
Critical Risk	
Education	
Email	
Entertainment	
Fashion	
File Storage and Sharing	
Financial Services	
Gambling	
Games	
General	

GRUPO DE ACCESO	
Categoría	**Permitido / Bloqueado**
Government / Military	
Greeting Cards	
Hacking	
Hate / Racism	
Health	
High Risk	
Illegal / Questionable	
Illegal Drugs	
Inactive Sites	
Instant Chat	
Instant Messaging	
Job Search / Careers	
Lifestyle	
Lingerie and Swimsuit / Suggestive	
Low Risk	
Media Sharing	
Media Streams	
Medium Risk	
Nature / Conservation	
News / Media	
Newsgroups / Forums	
Non-profits & NGOs	
Nudity	
P2P File Sharing	
Personals / Dating	
Phishing	
Political / Legal	
Pornography	

GRUPO DE ACCESO	
Categoría	**Permitido / Bloqueado**
Real Estate	
Recreation	
Religion	
Restaurants / Dining / Food	
Search Engines / Portals	
Sex	
Sex Education	
Shopping	
Social Networking	
Software Downloads	
Spam	
Sports	
Spyware / Malicious Sites	
Suspicious Content	
Tasteless	
Translation	
Travel	
Uncategorized	
Vehicles	
Very Low Risk	
Violence	
Weapons	
Web Advertisements	

Tabla 21. (Checkpoint, 2016) Categorías de Navegación Internet

ANEXO #3

Web Content Security Validaton Report before

WARNING: URLs listed are assumed to contain malicious content.

Do not attempt to visit any of these websites. The user assumes all responsibility from the misuse of any of the content of this report.

ID	Category Name	URL	Result	Block Reason
13186	Malware Files	http://molionia.ru/get/52570	Error	Error
13187	Malware Files	http://molionia.ru/get/55774	Error	Error
13188	Malware Files	http://molionia.ru/get/52602	Error	Error
13193	Malware Files	http://molionia.ru/get/52496	Error	Error
13196	Malware Files	http://hackgame.org/download/HackBauVatCF_1120.exe	Retrieved	Retrieved
13197	Malware Files	http://gunzupdates.universe-gamers.com/patchpublic/License.dll	Retrieved	Retrieved
13198	Malware Files	http://downloadsave.info/?e=ssale&publisher=2017&dd=2&p=http://ca.isohunt.com/download/451204351/argo.torrent?src=saven	Retrieved	Retrieved
13199	Malware Files	http://downloadsave.info/?e=ssale&publisher=2017&dd=2&p=http://ca.isohunt.com/download/448776886/here+comes+the+boom.torrent?src=saven	Retrieved	Retrieved
13200	Malware Files	http://downloadsave.info/?e=ssale&publisher=2017&dd=2&p=http://ca.isohunt.com/download/203603385/counter+strike.torrent?src=saven	Retrieved	Retrieved
13201	Malware Files	http://www.aqualogs.com/download/free/start.exe	Error	Error
13202	Malware Files	http://downloadsave.info/?e=ssale&publisher=2017&dd=2&p=http://ca.isohunt.com/download/442932725/Microsoft+Office+2013+Professional+Plus.torrent?src=saven	Retrieved	Retrieved
63969	Hacking	http://fengzhiguxiaoyouxi.blogspot.com/2010_01_03_archive.html	Error	Error
63970	Hacking	http://www.zargoosh.blogfa.com/	Retrieved	Retrieved
63971	Hacking	http://aresrd.blogspot.com/2009_04_01_archive.html	Error	Error
63975	Hacking	http://alfokzafrzaq.livejournal.com/	Retrieved	Retrieved
63976	Hacking	http://reynaleyour.livejournal.com/33406.html?	Retrieved	Retrieved
63979	Hacking	http://www.phimsop.com/feeds/posts/default/-/Phim%20c%E1%BA%A5p%203?	Retrieved	Retrieved
63983	Hacking	http://fdl4u.blogspot.com/	Retrieved	Retrieved
63984	Hacking	http://budokanclub.ru/index.php?name=Info&url=www.insecuro.pl/rss.php	Error	Error
63985	Hacking	http://hakceretruquesdeorkut.blogspot.com/	Error	Error
63987	Hacking	http://www.eivissasostenible.org/foro/viewtopic.php?f=2&t=24499	Retrieved	Retrieved
63988	Hacking	http://networkedblogs.com/dzvao?	Retrieved	Retrieved
63990	Hacking	http://textart4u.blogspot.com/2012/04/meme-face-text-art.html	Retrieved	Retrieved
63991	Hacking	http://degolqetf.livejournal.com/	Retrieved	Retrieved
63992	Hacking	http://www.facebook.com/plugins/like.php?href=http%3A%2F%2Fwww.rlslog.net%2Fdallas-complete-dvdrip-xvid-mixed%2F&layout=standard&show_faces=false&width=450&action=like&colorscheme=light&height=35	Retrieved	Retrieved
63993	Hacking	http://thelittleforum.com/forumsmf/index.php?action=profile;u=8760	Retrieved	Retrieved
63994	Hacking	http://www.tnctr.com/topic/82655-autocad-2008-keygen/?	Retrieved	Retrieved

65086	Malicious iFrame Redirection	http://smol-jurist.ru/	Error	Error
65088	Malicious iFrame Redirection	http://dghlsb.com/index.html	Retrieved	Retrieved
65093	Malicious iFrame Redirection	http://www.ullerslev-gaf.dk/admin/my_documents/my_files/2BZ_index.htm	Error	Error
65316	Malicious iFrame Redirection	http://www.travelworldonline.in/topstory-longnews.php	Retrieved	Retrieved
65317	Malicious iFrame Redirection	http://www.travelworldonline.in/topstory-longnews.php?	Retrieved	Retrieved
65318	Malicious iFrame Redirection	http://www.travelworldonline.in/airlines-longnews.php	Retrieved	Retrieved
65319	Malicious iFrame Redirection	http://www.travelworldonline.in/airlines-longnews.php?	Retrieved	Retrieved
65356	Malicious iFrame Redirection	http://sacredheartschool.co.in/	Retrieved	Retrieved
65359	Malicious iFrame Redirection	http://www.hy12345.gov.cn/	Retrieved	Retrieved
65364	Malicious iFrame Redirection	http://file.upi.edu/Direktori/FPTK/JUR._PEND._TEKNIK_MESIN/197611162005011-RIDWAN_ADAM_MUHAMAD_NOOR/Teknologi_Sepeda_Motor/suspension_bible.html	Retrieved	Retrieved
65371	Malicious iFrame Redirection	http://file.upi.edu/Direktori/FPTK/JUR._PEND._TEKNIK_MESIN/197611162005011-RIDWAN_ADAM_MUHAMAD_NOOR/Teknologi_Sepeda_Motor/suspension_bible_files/ads.htm	Retrieved	Retrieved
65462	Malicious iFrame Redirection	http://www.sonisamaj.co.in/people_hm.php?	Retrieved	Retrieved
65463	Malicious iFrame Redirection	http://teste1.xlsistemas.com/help.php?module=glossary&file=allowduplicatedentries.html	Retrieved	Retrieved
65465	Malicious iFrame Redirection	http://teste1.xlsistemas.com/help.php?file=coursecategory.html	Retrieved	Retrieved

69123	Malicious Web Redirection	http://sanlav.110mb.com/rife36.html?ahuida=dbfb075c	Retrieved	Retrieved
69146	Malicious Web Redirection	http://sanlav.110mb.com/rife36.html?akuuow=ae0ec5	Retrieved	Retrieved
69165	Malicious Web Redirection	http://sanlav.110mb.com/rife36.html?aex=aa44280b3b15fdda37c1	Retrieved	Retrieved
69187	Malicious Web Redirection	http://sanlav.110mb.com/rife36.html?adyxycy=be6f42820adbe7a6	Retrieved	Retrieved
69188	Malicious Web Redirection	http://sanlav.110mb.com/rife36.html?adariqeyuqy=ed5a3252e5ad341863081	Retrieved	Retrieved
69218	Malicious Web Redirection	http://sanlav.110mb.com/rife36.html?alezacuv=59cf7f19ebe339888e3e0088f	Retrieved	Retrieved
69221	Malicious Web Redirection	http://sanlav.110mb.com/rife36.html?abaceasy=275f0f5fe09	Retrieved	Retrieved
69222	Malicious Web Redirection	http://sanlav.110mb.com/rife36.html?ajotebo=fdc8f5e6c25b	Retrieved	Retrieved
69230	Malicious Web Redirection	http://www.scoutsdepanne.be/5k6386y.html	Retrieved	Retrieved
69231	Malicious Web Redirection	http://www.aecyt.com/20clqod.html	Retrieved	Retrieved
69233	Malicious Web Redirection	http://dance-ballet.com/media/chapter/city-of-vacaville.html	Retrieved	Retrieved
69234	Malicious Web Redirection	http://dance-ballet.com/media/2008/dodge-rams-seat-covers.html	Retrieved	Retrieved
69235	Malicious Web Redirection	http://dance-ballet.com/media/2008/silly-nickname-generators.html	Retrieved	Retrieved
69237	Malicious Web Redirection	http://dance-ballet.com/media/records/replacing-dodge-caravan-evaporator.html	Retrieved	Retrieved
69238	Malicious Web Redirection	http://dance-ballet.com/media/dirs/timber-framing-clamps.html	Retrieved	Retrieved
69239	Malicious Web Redirection	http://dance-ballet.com/media/chapter/american-furniture-warehouse-colorado.html	Retrieved	Retrieved
69240	Malicious Web Redirection	http://dance-ballet.com/media/2009/olive-garden-salad-dressing-recipe.html	Retrieved	Retrieved

70657	Malicious Web Exploits	http://www.alfaproject.org.uk/	Retrieved	Retrieved
70658	Malicious Web Exploits	http://www.alfaproject.org.uk/index.html	Retrieved	Retrieved
70659	Malicious Web Exploits	http://gaczi.com/	Retrieved	Retrieved
70660	Malicious Web Exploits	http://gabysuniqueboutique.com/	Retrieved	Retrieved
70661	Malicious Web Exploits	http://www.itunesgroove.com/?feed=rss2&p=2	Retrieved	Retrieved
70662	Malicious Web Exploits	http://www.itunesgroove.com/	Retrieved	Retrieved
70663	Malicious Web Exploits	http://www.ur-in-business.com/	Retrieved	Retrieved
70664	Malicious Web Exploits	http://www.twmins.com/index.htm	Retrieved	Retrieved
70665	Malicious Web Exploits	http://www.ur-in-business.com/index.htm	Error	Error
70666	Malicious Web Exploits	http://www.twmins.com/	Retrieved	Retrieved
70674	Malicious Web Exploits	http://gabysboutique.com/	Retrieved	Retrieved
70675	Malicious Web Exploits	http://miniaturenetdns.com/cgi-sys/suspendedpage.cgi	Error	Error
70676	Malicious Web Exploits	http://webcocktail.co.nz/	Retrieved	Retrieved
70677	Malicious Web Exploits	http://webcocktail.co.nz/index.html	Retrieved	Retrieved
70678	Malicious Web Exploits	http://www.iqtech.gr/	Retrieved	Retrieved
70679	Malicious Web Exploits	http://truevisioncs.com/index.php?	Retrieved	Retrieved
70680	Malicious Web Exploits	http://truevisioncs.com/index.php?nav1=About	Retrieved	Retrieved
70681	Malicious Web Exploits	http://truevisioncs.com/index.php?nav1=WebServices&nav2=WebHosting	Retrieved	Retrieved
70682	Malicious Web Exploits	http://truevisioncs.com/index.php?nav1=ComputerServices&nav2=CustomSolutions	Retrieved	Retrieved
70683	Malicious Web Exploits	http://truevisioncs.com/index.php?nav1=MarketingServices	Retrieved	Retrieved
70684	Malicious Web Exploits	http://truevisioncs.com/?nav1=faq	Retrieved	Retrieved
70685	Malicious Web Exploits	http://truevisioncs.com/index.php?nav1=GraphicServices&nav2=WebDesign	Retrieved	Retrieved
70686	Malicious Web Exploits	http://truevisioncs.com/index.php?nav1=Packages	Retrieved	Retrieved
70687	Malicious Web Exploits	http://www.adeptonline.net/cgi-sys/suspendedpage.cgi	Retrieved	Retrieved

79172	Malicious Web Obfuscation	http://www.drinkspotapp.com/?p=1086	Error	Error
79173	Malicious Web Obfuscation	http://www.drinkspotapp.com/?tag=blackheads	Error	Error
79174	Malicious Web Obfuscation	http://www.drinkspotapp.com/?p=776	Error	Error
79175	Malicious Web Obfuscation	http://www.drinkspotapp.com/?p=1109	Error	Error
79176	Malicious Web Obfuscation	http://www.drinkspotapp.com/?p=933	Error	Error
79177	Malicious Web Obfuscation	http://www.drinkspotapp.com/?p=281	Error	Error
79178	Malicious Web Obfuscation	http://www.drinkspotapp.com/?p=255	Error	Error
79179	Malicious Web Obfuscation	http://www.drinkspotapp.com/?page_id=229	Error	Error
79180	Malicious Web Obfuscation	http://www.drinkspotapp.com/?p=801	Error	Error
79181	Malicious Web Obfuscation	http://www.drinkspotapp.com/?p=898	Error	Error
79182	Malicious Web Obfuscation	http://www.drinkspotapp.com/?p=1213	Error	Error
79183	Malicious Web Obfuscation	http://www.drinkspotapp.com/?m=201104	Error	Error
79184	Malicious Web Obfuscation	http://www.drinkspotapp.com/?p=1195	Error	Error
79185	Malicious Web Obfuscation	http://www.drinkspotapp.com/?p=565	Error	Error
79186	Malicious Web Obfuscation	http://www.drinkspotapp.com/?p=718	Error	Error
79187	Malicious Web Obfuscation	http://www.drinkspotapp.com/?p=856	Error	Error

80678	Proxy Avoidance	http://www.guizmovpn.com/index.php?option=com_content&view=article&id=7&Itemid=18	Retrieved	Retrieved
80684	Proxy Avoidance	http://www.win-e.net/?p=140431	Retrieved	Retrieved
80690	Proxy Avoidance	http://www.vialo.net/themenreihe.p?c=R%C3%A9seau%20de%20t%C3%A9l%C3%A9communications	Error	Error
80692	Proxy Avoidance	http://prps.info/index.php?q=wyjatkowanoc.pl	Retrieved	Retrieved
80700	Proxy Avoidance	http://www.ireland24.ie/cha-cha/index30.htm?	Retrieved	Retrieved
80701	Proxy Avoidance	http://totestardoll.blogspot.nl/?	Retrieved	Retrieved
80721	Proxy Avoidance	http://adescalzers.blogtrue.com/	Error	Error
80731	Proxy Avoidance	http://01patche.blogspot.com/	Retrieved	Retrieved
80752	Proxy Avoidance	http://freedailyproxy.ru/?p=2	Retrieved	Retrieved
80759	Proxy Avoidance	http://country-directories.com/story.php?title=ideas-on-how-to-prevent-water-damage	Retrieved	Retrieved
80799	Proxy Avoidance	http://www.ciadoesmalte.com/2012/02/e-carnaval.html?	Retrieved	Retrieved
80841	Proxy Avoidance	http://www.torproject.org.in/projects/torbrowser.html.en?	Retrieved	Retrieved
80853	Proxy Avoidance	http://brand24.pl/static/js/default.js?	Retrieved	Retrieved
80862	Proxy Avoidance	http://onne.eu/www.facebook.com/plugins/likebox.php?href=http%3A%2F%2Fwww.facebook.com%2Fpages%2FOnneeu%2F460981643953452&width=208&height=320&show_faces=true&colorscheme=light&stream=false&border_color=%23f6b923&header=false	Retrieved	Retrieved
80875	Proxy Avoidance	http://www.rutartan.com/wordpress/?p=663	Retrieved	Retrieved

83753	Botnets	http://franmo.ovh.org/update/sygn_serw.dat	Retrieved	Retrieved
83755	Botnets	http://cu003.www.duba.net/duba/tools/dubatools/usb/fakeqvodconfig.txt	Retrieved	Retrieved
83756	Botnets	http://api.eduvideo.com.cn/MainAppDistribution/update.inf	Retrieved	Retrieved
83758	Botnets	http://mirror.math.ku.edu/tex-archive/systems/win32/latexpix/lpxsetup.updateinfo	Retrieved	Retrieved
83759	Botnets	http://mirror.utexas.edu/ctan/systems/win32/latexpix/lpxsetup.updateinfo	Retrieved	Retrieved
83761	Botnets	http://jkoenig.homedns.org/NAS/~files.lst%3Frecursive	Error	Error
83762	Botnets	http://forumswatcher.com/list.txt	Retrieved	Retrieved
83763	Botnets	http://helpers.remoteless.no/update.txt	Retrieved	Retrieved
83764	Botnets	http://cohstats.relic.com/relic/coh/retail_autopatch/english_2500.txt	Error	Error
83765	Botnets	http://powdertoy.co.uk/Download/Extra/README.txt	Retrieved	Retrieved
83766	Botnets	http://mirror.jmu.edu/pub/CTAN/systems/win32/latexpix/lpxsetup.updateinfo	Retrieved	Retrieved
83768	Botnets	http://franmo.hexsite.pl/update/sygn_serw.dat	Retrieved	Retrieved
83769	Botnets	http://uploaded.net/list/8vbw1x/plain	Retrieved	Retrieved
83770	Botnets	http://allfinder.co.kr/updateserver/AutoUpdate/Updateversion/UpdateVer.txt	Error	Error
83771	Botnets	http://carroll.aset.psu.edu/pub/CTAN/systems/win32/latexpix/lpxsetup.updateinfo	Retrieved	Retrieved
83772	Botnets	http://cu003.www.duba.net/duba/tools/dubatools/usb/mbrconfig.txt	Retrieved	Retrieved
83774	Botnets	http://81.177.169.215/human/gate.php?	Error	Error
83775	Botnets	http://81.177.169.215/human/gate.php	Error	Error
83776	Botnets	http://91.217.254.210/abc1/gate.php	Error	Error
83777	Botnets	http://91.217.254.210/139/gate.php	Error	Error

83837	Gambling	http://bestrouletteblog.tumblr.com/?	Retrieved	Retrieved
83838	Gambling	http://www2.twingly.com/3F336866A46FC1EA324E59FDB74676?	Retrieved	Retrieved
83839	Gambling	http://friendfeed.com/depage?	Retrieved	Retrieved
83840	Gambling	http://www.pom1688.com/?post=76	Error	Error
83842	Gambling	http://resultadosmelate.blogspot.mx/feeds/posts/default/-/N%C3%9AMEROS%20GANADORES?	Retrieved	Retrieved
83843	Gambling	http://api.bwbx.io/v2/stories/362c7d52-918f-11e2-8065-d8d385601e40?	Retrieved	Retrieved
83844	Gambling	http://pingdamon51.wordpress.com/	Retrieved	Retrieved
83845	Gambling	http://api.twitter.com/1/statuses/user_timeline.json?screen_name=phantomefx&count=1&callback=jsonp13651730352248&_=1365173035315	Retrieved	Retrieved
83846	Gambling	http://183123.com/viewthread.php?tid=7159&extra=page=1	Retrieved	Retrieved
83847	Gambling	http://www.oddsen.nu/langoddsen/ullensaker_kisa_-_strmsgodset_2/124254	Retrieved	Retrieved
83848	Gambling	http://mannsverk.org/drupal/fotball?	Retrieved	Retrieved
83849	Gambling	http://riku.s59.xrea.com/	Retrieved	Retrieved
83851	Gambling	http://loterias-sorte.blogspot.com.br/2012/10/lotofacil-813.html?	Retrieved	Retrieved
83854	Gambling	http://www.rr6666.com/?	Retrieved	Retrieved
83855	Gambling	http://tat4cai.blogspot.se/2011/11/hack-accounts-with-rin-logger.html	Error	Error
83856	Gambling	http://sofiagustara.blogspot.com/2011/01/blog-post_3028.html?	Retrieved	Retrieved
83857	Gambling	http://t-wire.com/?	Retrieved	Retrieved
83858	Gambling	http://hayleyghoover.blogspot.se/2012/09/twenty-one-ing.html?m=1	Retrieved	Retrieved
83859	Gambling	http://map46save.tumblr.com/post/46225925527/gclub-gambling-online-tricks-instructions-earn-money	Retrieved	Retrieved

87356	Sex	http://str8freexxxvideos.blogspot.com/	Retrieved	Retrieved
87357	Sex	http://forum.londoner25.net/viewtopic.php?f=10&t=647511	Retrieved	Retrieved
87359	Sex	http://smocking2byaquilareale62.blogspot.com/2012/09/il-fascino-della-figa-pelosa.html	Error	Error
87361	Sex	http://brawny3d.blogspot.com/	Retrieved	Retrieved
87362	Sex	http://www.secretcitygirls.co.uk/	Retrieved	Retrieved
87364	Sex	http://www.bentuw.com/urls/news.asp?	Error	Error
87365	Sex	http://porn-week.tumblr.com/?	Retrieved	Retrieved
87366	Sex	http://bigbellanova.tumblr.com/post/47118249018/could-you-imagine-being-balls-deep-or-in-my-case	Retrieved	Retrieved
87367	Sex	http://altnopifuun.livejournal.com/1864.html	Retrieved	Retrieved
87370	Sex	http://unkar.org/r/mlb/1235313977	Error	Error
87372	Sex	http://xxxprincealbertxxx.tumblr.com/?	Retrieved	Retrieved
87373	Sex	http://gatypyuk.zeblog.com/	Retrieved	Retrieved
87374	Sex	http://pornofilmesflash.blogspot.com/	Retrieved	Retrieved
87375	Sex	http://jeannieweavi.livejournal.com/	Retrieved	Retrieved
87377	Sex	http://500px.com/photo/16297131?	Retrieved	Retrieved
87379	Sex	http://damnsoonice.tumblr.com/	Retrieved	Retrieved
87380	Sex	http://macporno3.blogspot.com/	Error	Error
87381	Sex	http://ml-tube.blogspot.be/2013_02_01_archive.html	Retrieved	Retrieved
87382	Sex	http://bradstockboys.blogspot.com/2008/05/porn-again.html	Retrieved	Retrieved
87384	Sex	http://gymbooty.com/notes/16041880177/66OhwRKwX?	Retrieved	Retrieved
87385	Sex	http://doubyuru.blog.fc2.com/	Retrieved	Retrieved
87387	Sex	http://www.clip-adulte.com/uprofile.php?UID=63	Retrieved	Retrieved
87388	Sex	http://charlizetheronnudesettingout.typepad.com/?	Retrieved	Retrieved

Web Content Security Validation Report After

WARNING: URLs listed are assumed to contain malicious content.

Do not attempt to visit any of these websites. The user assumes all responsibility from the misuse of any of the content of this report.

ID	Category Name	URL	Result	Block Reason
13186	Malware Files	http://molionia.ru/get/52570	Error	Error
13187	Malware Files	http://molionia.ru/get/55774	Error	Error
13188	Malware Files	http://molionia.ru/get/52602	Error	Error
13193	Malware Files	http://molionia.ru/get/52496	Error	Error
13196	Malware Files	http://hackgame.org/download/HackBauVatCF_1120.exe	Retrieved	Retrieved
13197	Malware Files	http://gunzupdates.universe-gamers.com/patchpublic/License.dll	Error	Error
13198	Malware Files	http://downloadsave.info/?e=ssale&publisher=2017&dd=2&p=http://ca.isohunt.com/download/451204351/argo.torrent?src=saven	Error	Error
13199	Malware Files	http://downloadsave.info/?e=ssale&publisher=2017&dd=2&p=http://ca.isohunt.com/download/448776886/here+comes+the+boom.torrent?src=saven	Error	Error
13200	Malware Files	http://downloadsave.info/?e=ssale&publisher=2017&dd=2&p=http://ca.isohunt.com/download/203603385/counter+strike.torrent?src=saven	Error	Error
13201	Malware Files	http://www.aqualogs.com/download/free/start.exe	Error	Error
13202	Malware Files	http://downloadsave.info/?e=ssale&publisher=2017&dd=2&p=http://ca.isohunt.com/download/442932725/Microsoft+Office+2013+Professional+Plus.torrent?src=saven	Error	Error
63969	Hacking	http://fengzhiguxiaoyouxi.blogspot.com/2010_01_03_archive.html	Error	Error
63970	Hacking	http://www.zargoosh.blogfa.com/	Error	Error
63971	Hacking	http://aresrd.blogspot.com/2009_04_01_archive.html	Error	Error
63975	Hacking	http://alfokzafrzaq.livejournal.com/	Error	Error
63976	Hacking	http://reynaleyour.livejournal.com/33406.html?	Error	Error
63979	Hacking	http://www.phimsop.com/feeds/posts/default/-/Phim%20c%E1%BA%A5p%203?	Error	Error
63983	Hacking	http://fdl4u.blogspot.com/	Error	Error
63984	Hacking	http://budokanclub.ru/index.php?name=Info&url=www.insecuro.pl/rss.php	Error	Error
63985	Hacking	http://hakceretruquesdeorkut.blogspot.com/	Error	Error
63987	Hacking	http://www.eivissasostenible.org/foro/viewtopic.php?f=2&t=24499	Error	Error
63988	Hacking	http://networkedblogs.com/dzvao?	Error	Error
63990	Hacking	http://textart4u.blogspot.com/2012/04/meme-face-text-art.html	Error	Error
63991	Hacking	http://degolqetf.livejournal.com/	Error	Error
63992	Hacking	http://www.facebook.com/plugins/like.php?href=http%3A%2F%2Fwww.rlslog.net%2Fdallas-complete-dvdrip-xvid-mixed%2F&layout=standard&show_faces=false&width=450&action=like&colorscheme=light&height=35	Error	Error
63993	Hacking	http://thelittleforum.com/forumsmf/index.php?action=profile;u=8760	Error	Error
63994	Hacking	http://www.tnctr.com/topic/82655-autocad-2008-keygen/?	Error	Error

65086	Malicious iFrame Redirection	http://smol-jurist.ru/	Error	Error
65088	Malicious iFrame Redirection	http://dghlsb.com/index.html	Error	Error
65093	Malicious iFrame Redirection	http://www.ullerslev-gaf.dk/admin/my_documents/my_files/2BZ_index.htm	Error	Error
65316	Malicious iFrame Redirection	http://www.travelworldonline.in/topstory-longnews.php	Error	Error
65317	Malicious iFrame Redirection	http://www.travelworldonline.in/topstory-longnews.php?	Error	Error
65318	Malicious iFrame Redirection	http://www.travelworldonline.in/airlines-longnews.php	Error	Error
65319	Malicious iFrame Redirection	http://www.travelworldonline.in/airlines-longnews.php?	Error	Error
65356	Malicious iFrame Redirection	http://sacredheartschool.co.in/	Error	Error
65359	Malicious iFrame Redirection	http://www.hy12345.gov.cn/	Error	Error
65364	Malicious iFrame Redirection	http://file.upi.edu/Direktori/FPTK/JUR._PEND._TEKNIK_MESIN/197611162005011-RIDWAN_ADAM_MUHAMAD_NOOR/Teknologi_Sepeda_Motor/suspension_bible.html	Error	Error
65371	Malicious iFrame Redirection	http://file.upi.edu/Direktori/FPTK/JUR._PEND._TEKNIK_MESIN/197611162005011-RIDWAN_ADAM_MUHAMAD_NOOR/Teknologi_Sepeda_Motor/suspension_bible_files/ads.htm	Error	Error
65462	Malicious iFrame Redirection	http://www.sonisamaj.co.in/people_hm.php?	Error	Error
65463	Malicious iFrame Redirection	http://teste1.xlsistemas.com/help.php?module=glossary&file=allowduplicatedentries.html	Error	Error
65465	Malicious iFrame Redirection	http://teste1.xlsistemas.com/help.php?file=coursecategory.html	Error	Error

69123	Malicious Web Redirection	http://sanlav.110mb.com/rife36.html?ahuida=dbfb075c	Error	Error
69146	Malicious Web Redirection	http://sanlav.110mb.com/rife36.html?akuuow=ae0ec5	Error	Error
69165	Malicious Web Redirection	http://sanlav.110mb.com/rife36.html?aex=aa44280b3b15fdda37c1	Error	Error
69187	Malicious Web Redirection	http://sanlav.110mb.com/rife36.html?adyxycy=be6f42820adbe7a6	Error	Error
69188	Malicious Web Redirection	http://sanlav.110mb.com/rife36.html?adariqeyuqy=ed5a3252e5ad341863081	Error	Error
69218	Malicious Web Redirection	http://sanlav.110mb.com/rife36.html?alezacuv=59cf7f19ebe339888e3e0088f	Error	Error
69221	Malicious Web Redirection	http://sanlav.110mb.com/rife36.html?abaceasy=275f0f5fe09	Error	Error
69222	Malicious Web Redirection	http://sanlav.110mb.com/rife36.html?ajotebo=fdc8f5e6c25b	Retrieved	Retrieved
69230	Malicious Web Redirection	http://www.scoutsdepanne.be/5k6386y.html	Retrieved	Retrieved
69231	Malicious Web Redirection	http://www.aecyt.com/20clqod.html	Retrieved	Retrieved
69233	Malicious Web Redirection	http://dance-ballet.com/media/chapter/city-of-vacaville.html	Error	Error
69234	Malicious Web Redirection	http://dance-ballet.com/media/2008/dodge-rams-seat-covers.html	Error	Error
69235	Malicious Web Redirection	http://dance-ballet.com/media/2008/silly-nickname-generators.html	Error	Error
69237	Malicious Web Redirection	http://dance-ballet.com/media/records/replacing-dodge-caravan-evaporator.html	Error	Error
69238	Malicious Web Redirection	http://dance-ballet.com/media/dirs/timber-framing-clamps.html	Error	Error
69239	Malicious Web Redirection	http://dance-ballet.com/media/chapter/american-furniture-warehouse-colorado.html	Error	Error

70657	Malicious Web Exploits	http://www.alfaproject.org.uk/	Error	Error
70658	Malicious Web Exploits	http://www.alfaproject.org.uk/index.html	Error	Error
70659	Malicious Web Exploits	http://gaczi.com/	Error	Error
70660	Malicious Web Exploits	http://gabysuniqueboutique.com/	Error	Error
70661	Malicious Web Exploits	http://www.itunesgroove.com/?feed=rss2&p=2	Error	Error
70662	Malicious Web Exploits	http://www.itunesgroove.com/	Error	Error
70663	Malicious Web Exploits	http://www.ur-in-business.com/	Error	Error
70664	Malicious Web Exploits	http://www.twmins.com/index.htm	Error	Error
70665	Malicious Web Exploits	http://www.ur-in-business.com/index.htm	Error	Error
70666	Malicious Web Exploits	http://www.twmins.com/	Error	Error
70674	Malicious Web Exploits	http://gabysboutique.com/	Error	Error
70675	Malicious Web Exploits	http://miniaturenetdns.com/cgi-sys/suspendedpage.cgi	Error	Error
70676	Malicious Web Exploits	http://webcocktail.co.nz/	Error	Error
70677	Malicious Web Exploits	http://webcocktail.co.nz/index.html	Error	Error
70678	Malicious Web Exploits	http://www.iqtech.gr/	Error	Error
70679	Malicious Web Exploits	http://truevisioncs.com/index.php?	Error	Error
70680	Malicious Web Exploits	http://truevisioncs.com/index.php?nav1=About	Error	Error
70681	Malicious Web Exploits	http://truevisioncs.com/index.php?nav1=WebServices&nav2=WebHosting	Error	Error
70682	Malicious Web Exploits	http://truevisioncs.com/index.php?nav1=ComputerServices&nav2=CustomSolutions	Error	Error
70683	Malicious Web Exploits	http://truevisioncs.com/index.php?nav1=MarketingServices	Error	Error
70684	Malicious Web Exploits	http://truevisioncs.com/?nav1=faq	Error	Error
70685	Malicious Web Exploits	http://truevisioncs.com/index.php?nav1=GraphicServices&nav2=WebDesign	Error	Error
70686	Malicious Web Exploits	http://truevisioncs.com/index.php?nav1=Packages	Error	Error
70687	Malicious Web Exploits	http://www.adeptonline.net/cgi-sys/suspendedpage.cgi	Error	Error

79172	Malicious Web Obfuscation	http://www.drinkspotapp.com/?p=1086	Error	Error
79173	Malicious Web Obfuscation	http://www.drinkspotapp.com/?tag=blackheads	Error	Error
79174	Malicious Web Obfuscation	http://www.drinkspotapp.com/?p=776	Error	Error
79175	Malicious Web Obfuscation	http://www.drinkspotapp.com/?p=1109	Error	Error
79176	Malicious Web Obfuscation	http://www.drinkspotapp.com/?p=933	Error	Error
79177	Malicious Web Obfuscation	http://www.drinkspotapp.com/?p=281	Error	Error
79178	Malicious Web Obfuscation	http://www.drinkspotapp.com/?p=255	Error	Error
79179	Malicious Web Obfuscation	http://www.drinkspotapp.com/?page_id=229	Error	Error
79180	Malicious Web Obfuscation	http://www.drinkspotapp.com/?p=801	Error	Error
79181	Malicious Web Obfuscation	http://www.drinkspotapp.com/?p=898	Error	Error
79182	Malicious Web Obfuscation	http://www.drinkspotapp.com/?p=1213	Error	Error
79183	Malicious Web Obfuscation	http://www.drinkspotapp.com/?m=201104	Error	Error
79184	Malicious Web Obfuscation	http://www.drinkspotapp.com/?p=1195	Error	Error
79185	Malicious Web Obfuscation	http://www.drinkspotapp.com/?p=565	Error	Error
79186	Malicious Web Obfuscation	http://www.drinkspotapp.com/?p=718	Error	Error
79187	Malicious Web Obfuscation	http://www.drinkspotapp.com/?p=856	Error	Error
79188	Malicious Web Obfuscation	http://www.drinkspotapp.com/?p=1194	Error	Error

80678	Proxy Avoidance	http://www.guizmovpn.com/index.php?option=com_content&view=article&id=7&Itemid=18	Error	Error
80684	Proxy Avoidance	http://www.win-e.net/?p=140431	Error	Error
80690	Proxy Avoidance	http://www.vialo.net/themenreihe.p?c=R%C3%A9seau%20de%20t%C3%A9l%C3%A9communications	Error	Error
80692	Proxy Avoidance	http://prps.info/index.php?q=wyjatkowanoc.pl	Error	Error
80700	Proxy Avoidance	http://www.ireland24.ie/cha-cha/index30.htm?	Error	Error
80701	Proxy Avoidance	http://totestardoll.blogspot.nl/?	Error	Error
80721	Proxy Avoidance	http://adescalzers.blogtrue.com/	Error	Error
80731	Proxy Avoidance	http://01patche.blogspot.com/	Error	Error
80752	Proxy Avoidance	http://freedailyproxy.ru/?p=2	Error	Error
80759	Proxy Avoidance	http://country-directories.com/story.php?title=ideas-on-how-to-prevent-water-damage	Error	Error
80799	Proxy Avoidance	http://www.ciadoesmalte.com/2012/02/e-carnaval.html?	Error	Error
80841	Proxy Avoidance	http://www.torproject.org.in/projects/torbrowser.html.en?	Error	Error
80853	Proxy Avoidance	http://brand24.pl/static/js/default.js?	Error	Error
80862	Proxy Avoidance	http://onne.eu/www.facebook.com/plugins/likebox.php?href=http%3A%2F%2Fwww.facebook.com%2Fpages%2FOnneeu%2F460981643953452&width=208&height=320&show_faces=true&colorscheme=light&stream=false&border_color=%23f6b923&header=false	Error	Error
80875	Proxy Avoidance	http://www.rutartan.com/wordpress/?p=663	Error	Error

83753	Botnets	http://franmo.ovh.org/update/sygn_serw.dat	Error	Error
83755	Botnets	http://cu003.www.duba.net/duba/tools/dubatools/usb/fakeqvodconfig.txt	Error	Error
83756	Botnets	http://api.eduvideo.com.cn/MainAppDistribution/update.inf	Error	Error
83758	Botnets	http://mirror.math.ku.edu/tex-archive/systems/win32/latexpix/lpxsetup.updateinfo	Error	Error
83759	Botnets	http://mirror.utexas.edu/ctan/systems/win32/latexpix/lpxsetup.updateinfo	Error	Error
83761	Botnets	http://jkoenig.homedns.org/NAS/~files.lst%3Frecursive	Error	Error
83762	Botnets	http://forumswatcher.com/list.txt	Error	Error
83763	Botnets	http://helpers.remoteless.no/update.txt	Error	Error
83764	Botnets	http://cohstats.relic.com/relic/coh/retail_autopatch/english_2500.txt	Error	Error
83765	Botnets	http://powdertoy.co.uk/Download/Extra/README.txt	Error	Error
83766	Botnets	http://mirror.jmu.edu/pub/CTAN/systems/win32/latexpix/lpxsetup.updateinfo	Error	Error
83768	Botnets	http://franmo.hexsite.pl/update/sygn_serw.dat	Error	Error
83769	Botnets	http://uploaded.net/list/8vbw1x/plain	Error	Error
83770	Botnets	http://allfinder.co.kr/updateserver/AutoUpdate/Updateversion/UpdateVer.txt	Error	Error
83771	Botnets	http://carroll.aset.psu.edu/pub/CTAN/systems/win32/latexpix/lpxsetup.updateinfo	Error	Error
83772	Botnets	http://cu003.www.duba.net/duba/tools/dubatools/usb/mbrconfig.txt	Error	Error
83774	Botnets	http://81.177.169.215/human/gate.php?	Error	Error
83775	Botnets	http://81.177.169.215/human/gate.php	Error	Error
83776	Botnets	http://91.217.254.210/abc1/gate.php	Error	Error
83777	Botnets	http://91.217.254.210/139/gate.php	Error	Error

83837	Gambling	http://bestrouletteblog.tumblr.com/?	Error	Error
83838	Gambling	http://www2.twingly.com/3F336866A46FC1EA324E59FDB74676?	Error	Error
83839	Gambling	http://friendfeed.com/depage?	Error	Error
83840	Gambling	http://www.pom1688.com/?post=76	Error	Error
83842	Gambling	http://resultadosmelate.blogspot.mx/feeds/posts/default/-/N%C3%9AMEROS%20GANADORES?	Error	Error
83843	Gambling	http://api.bwbx.io/v2/stories/362c7d52-918f-11e2-8065-d8d385601e40?	Error	Error
83844	Gambling	http://pingdamon51.wordpress.com/	Retrieved	Retrieved
83845	Gambling	http://api.twitter.com/1/statuses/user_timeline.json?screen_name=phantomefx&count=1&callback=jsonp1365173035224&_=1365173035315	Error	Error
83846	Gambling	http://183123.com/viewthread.php?tid=7159&extra=page=1	Error	Error
83847	Gambling	http://www.oddsen.nu/langoddsen/ullensaker_kisa_-_strmsgodset_2/124254	Retrieved	Retrieved
83848	Gambling	http://mannsverk.org/drupal/fotball?	Retrieved	Retrieved
83849	Gambling	http://riku.s59.xrea.com/	Error	Error
83851	Gambling	http://loterias-sorte.blogspot.com.br/2012/10/lotofacil-813.html?	Error	Error
83854	Gambling	http://www.rr6666.com/?	Error	Error
83855	Gambling	http://tat4cai.blogspot.se/2011/11/hack-accounts-with-rin-logger.html	Error	Error
83856	Gambling	http://sofiagustara.blogspot.com/2011/01/blog-post_3028.html?	Error	Error
83857	Gambling	http://t-wire.com/?	Error	Error
83858	Gambling	http://hayleyghoover.blogspot.se/2012/09/twenty-one-ing.html?m=1	Error	Error

87356	Sex	http://str8freexxxvideos.blogspot.com/	Error	Error
87357	Sex	http://forum.londoner25.net/viewtopic.php?f=10&t=647511	Error	Error
87359	Sex	http://smocking2byaquilareale62.blogspot.com/2012/09/il-fascino-della-figa-pelosa.html	Error	Error
87361	Sex	http://brawny3d.blogspot.com/	Error	Error
87362	Sex	http://www.secretcitygirls.co.uk/	Error	Error
87364	Sex	http://www.bentuw.com/urls/news.asp?	Error	Error
87365	Sex	http://porn-week.tumblr.com/?	Error	Error
87366	Sex	http://bigbellanova.tumblr.com/post/47118249018/could-you-imagine-being-balls-deep-or-in-my-case	Error	Error
87367	Sex	http://altnopifuun.livejournal.com/1864.html	Error	Error
87370	Sex	http://unkar.org/r/mlb/1235313977	Error	Error
87372	Sex	http://xxxprincealbertxxx.tumblr.com/?	Error	Error
87373	Sex	http://gatypyuk.zeblog.com/	Error	Error
87374	Sex	http://pornofilmesflash.blogspot.com/	Error	Error
87375	Sex	http://jeannieweavi.livejournal.com/	Error	Error
87377	Sex	http://500px.com/photo/16297131?	Error	Error
87379	Sex	http://damnsoonice.tumblr.com/	Error	Error
87380	Sex	http://macporno3.blogspot.com/	Error	Error
87381	Sex	http://ml-tube.blogspot.be/2013_02_01_archive.html	Error	Error
87382	Sex	http://bradstockboys.blogspot.com/2008/05/porn-again.html	Error	Error
87384	Sex	http://gymbooty.com/notes/16041880177/66OhwRKwX?	Error	Error
87385	Sex	http://doubyuru.blog.fc2.com/	Error	Error
87387	Sex	http://www.clip-adulte.com/uprofile.php?UID=63	Error	Error