MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

La importancia de los IPS y BYOD en las organizaciones: Caso de estudio CONFIDENCIAL S.A.

Propuesta de artículo presentado como requisito para la obtención del título:

Magíster en Auditoría de Tecnologías de la Información

Por la estudiante:
Nora Elena MARIDUEÑA CARRION

Bajo la dirección de:
Francisco Joseph BOLAÑOS BURGOS.

Universidad Espíritu Santo
Maestría en Auditoría de Tecnología de la Información
Samborondón - Ecuador
Junio del 2016

La importancia de los IPS y BYOD en las organizaciones: Caso de estudio CONFIDENCIAL S.A.

The importance of IPS and BYOD in organizations: Case study CONFIDENCIAL S.A.

Nora Elena MARIDUEÑA CARRION[1]
Francisco Joseph BOLAÑOS BURGOS[2]

Resumen

El objetivo del presente trabajo es evidenciar la importancia que tiene en la actualidad la correcta implementación de un Sistema de Prevención de Intrusos (IPS), así como las políticas de BYOD. Para lograr este objetivo se plantea la realización de un análisis exploratorio de la empresa CONFIDENCIA S.A. con la finalidad de comprobar la existencia de inconvenientes tanto físicos como lógicos en la infraestructura existente y a través de dicha evidencia exponer las recomendaciones de remediación necesarias. Se considera como motivación para la realización del presente trabajo, la necesidad de presentar a través de un caso práctico, una demostración de cómo múltiples inconvenientes de red se originan por una incorrecta configuración de las herramientas relacionadas con la infraestructura física. Con la finalidad de alcanzar el objetivo planteado se ejecutó una serie de análisis, además de varias entrevistas con personal clave del área de Sistemas y proveedores relacionados. Con base a los resultados obtenidos, tanto de los instrumentos de revisión y las entrevistas realizadas, fue posible determinar las principales debilidades del departamento de Sistemas, tanto a nivel de políticas existentes como en la infraestructura implementada. Gracias a este hallazgo se logró realizar una serie de recomendaciones que, de ser implementadas por el departamento de Sistemas, le permitirán mejorar su infraestructura de red y la seguridad interna de la misma.

Palabras clave: IDS, IPS, BYOD, MDM, NGFW.

Abstract

The objective of this study is to show the importance, nowadays, of the correct implementation of an Intrusion Prevention System (IPS), and also the BYOD policies. To achieve this objective, we plan to make an exploratory analysis of CONFIDENCIA S.A., with the purpose of verifying the existence of both physical and logical inconveniences in the existing infrastructure and, through this evidence, to expose the necessary remediation recommendations. It is considered as motivation for the current analysis, the necessity to present through a practical case, a demonstration of how multiple reported network drawbacks are caused by an incorrect configuration of the tools related to the physical infrastructure. In order to achieve the stated objective, a series of analyzes was carried out, in addition to several interviews with key personnel in the Information Technology area and related suppliers. Based on the results obtained, both from the instruments of analysis and from the interviews conducted; it was possible to determine the main weaknesses of the Information Technology Department, both related to the existing policies and in the implemented infrastructure. Due to this finding, it was possible to make a series of recommendations that, if implemented by the Information Technology Department, will enable it to improve its network infrastructure and its internal security..

Key words IDS, IPS, BYOD, MDM, NGFW.

[1] Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador. E-mail nmaridue@uees.edu.ec
[2] Magíster en Seguridad Informática Aplicada. Director de la Maestría en Auditoría en Tecnologías de la Información Universidad Espíritu Santo-Ecuador.

INTRODUCCIÓN

El alarmante incremento de los delitos informáticos, ha puesto en alerta a las empresas que diariamente ven como esta amenaza toma fuerza ya que se vuelve más común y a la vez sofisticada. La ventaja de la conectividad ha logrado mejorar e integrar casi todos los procesos, pero ha convertido a la infraestructura y sistemas de las empresas en un blanco fácil y atractivo para la ciberdelincuencia. La Organización de Estados Americanos (OEA) a través de su informe anual (Trend Micro Incorporated, 2015) menciona al fraude con motivaciones económicas y a los ataques contra la confidencialidad, integridad y disponibilidad como las principales tendencias relacionadas con los crímenes informáticos. El mismo estudio evidencia la existencia de 1.5 millones de intentos de conexión realizados a través de computadoras infectadas y controladas por C&Cs; alrededor 7.000 IPs semanales que son infectadas con malware, correspondiendo estos números a la actividad de alrededor de cincuenta botnets diferentes.

Este panorama genera la necesidad de mejorar los métodos de control a nivel empresarial para evitar ser víctimas de este tipo de delitos. Por tal motivo, la empresa CONFIDENCIAL S.A. participa del presente estudio con la finalidad de que un análisis general a su infraestructura informática le ayude a fortalecer los controles de seguridad para sus activos de información.

Es importante resaltar que por tema de confidencialidad, para la elaboración del presente documento se utilizará el nombre CONFIDENCIAL S.A. para referirse a la empresa objeto del estudio y no se incluye información interna de la misma. La empresa CONFIDENCIAL S.A. es una industria que elabora productos terminados que son comercializados por su fuerza de venta. En la actualidad cuenta con 650 empleados, de los cuales 250 son del área de Producción y 400 pertenecen a la plana administrativa y de negocio. En el aspecto tecnológico cuenta con varios sistemas especializados, cuya compra fue gestionada a través de proveedores del exterior. El ERP fue adquirido localmente y en la negociación se incluyó las fuentes del mismo. Cabe indicar que la empresa cuenta con tres áreas dentro del departamento de Sistemas, las áreas de Aplicaciones, Infraestructura y Desarrollo.

La empresa CONFIDENCIAL S.A. presenta inconvenientes internos con los servicios de red e internet. Lo cual se ha evidenciado a través de llamados recurrentes de usuarios de diversas áreas, según indica uno de los desarrolladores “se reporta lentitud en sus conexiones con el ERP, llegando a veces a la imposibilidad de ejecución del mismo” (Desarrollador 1, comunicación personal, 28 de noviembre del 2016). Normalmente, el trabajo se realiza sin inconvenientes, pero en determinados momentos se comienzan a presentar problemas, tales como usuarios de varios departamentos que no logran acceder a los sistemas.

Un punto adicional que se debe considerar es que a pesar de la existencia de una política sobre el uso de internet y correo electrónico, en la cual se indica la prohibición del uso de dispositivos personales para acceder a los servicios de red, existen muchos casos de usuarios que obtienen autorización de la Gerencia de cada área para obtener acceso a las redes Wi-Fi. A pesar de esto, no existe una política de gestión y uso de dispositivos personales o también llamado Bring Our Your Device (BYOD).

En la empresa CONFIDENCIAL S.A., todos los usuarios que poseen un computador tienen acceso a internet. Este acceso es controlado a través de reglas de firewall que limitan el uso de redes sociales, acceso a páginas de contenido restringido, descarga de archivos, entre otros. CONFIDENCIAL S.A. posee un enlace de internet de 10 MB que cubre 2 edificios de la matriz, pero existen situaciones que ocasionan que esta capacidad sea insuficiente para los requerimientos a cubrir. Es necesario considerar que la empresa no cuenta con una política de seguridad establecida. Se está desarrollando un

proceso de concientización de los usuarios, que se encuentra en sus fases iniciales.

Esta deficiencia origina que se haya detectado casos de usuarios que hacen mal uso de los servicios, lo cual se ha puesto en evidencia al descubrir situaciones en las que utilizan la conexión a internet para visitar páginas indebidas como por ejemplo de radios online. Este comportamiento, incrementa la posibilidad de que al navegar en sitios inseguros se realice algún tipo de infección por malware, sin contar con la falta de políticas o normas para el uso de dispositivos móviles propios.

El objetivo del presente estudio es concientizar sobre la importancia de una correcta implementación de herramientas de seguridad y políticas internas, a través de la realización de un análisis de la situación de la infraestructura de la empresa, con base en las necesidades y falencias existentes, de manera que las recomendaciones expuestas mejoren la seguridad y administración de la misma, con la finalidad de que la empresa CONFIDENCIAL S.A. se encuentre mejor preparada ante futuras auditorias del ente regulador y que evite la existencia de no conformidades de carácter crítico.

MARCO TEÓRICO

Intrusion Detection System (IDS)

Se define la detección de intrusos como el proceso de monitoreo a los eventos de un sistema, con la finalidad de detectar anomalías que evidencien la existencia de posibles violaciones o amenazas de violación a las políticas de seguridad informática (Scarfone & Mell, 2007).

Las amenazas informáticas tienen como finalidad vulnerar los principios de confidencialidad, integridad y disponibilidad de la información (Singh, Goyal, & Agarwal, s/a). El constante crecimiento y avance tecnológico ha permitido que las amenazas informáticas se incrementen y adquieran mayor sofisticación.

Además, el considerable incremento en la disponibilidad de ancho de banda de la red, que años atrás se medía en megabits y que en la actualidad está en el rango de gigabits por segundo ha complicado aún más la tarea de monitorear y analizar el tráfico de red en busca de intentos de intrusión (Bruneau, 2001).

Años atrás los administradores informáticos, contaban con herramientas limitadas para la protección de los sistemas, se podían basar principalmente en la información que contenían los archivos log, pero este tipo de análisis únicamente era útil para intentar determinar que sucedió, ya que se actuaba una vez ocurrido el evento. Gracias a la evolución de la tecnología, a inicios de los años 90, aparecieron los primeros sistemas de detección de intrusos que trabajaban de forma autónoma basándose en reglas previamente determinadas, logrando obtener análisis en tiempo real. (Kemmerer & Vigna, 2002).

Los IDS monitorean todo el tráfico de la red en tiempo real, analizando y comparando los paquetes con patrones que permitan determinar si el tráfico es un intento de ataque o tráfico malicioso, lo cual de ser detectado, alerta al administrador del sistema para que realice alguna acción que impida que el ataque sé efectivice (SecurityMetrics Inc., 2003).

Existen 2 métodos de detección que se emplean principalmente en los IDS, estos son: basado en Firmas (Signature-based - SBS) y basado en Anomalías (Anomaly-based - ABS) (Jyothsna & Rama Prasad, 2011). El método SBS usa el reconocimiento de patrones que han sido previamente definidos y los usa para compararlos con los datos que está analizando. En cambio, el ABS utiliza un modelo estadístico que determina el tráfico normal de la red y cualquier anomalía es considerada maliciosa.

Adicionalmente los IDS considerando su implementación se dividen en 2 tipos, los basados en Red y los basados en Host.

Los IDS basados en Red, se ubican atrás del firewall de manera que el tráfico que logra pasar

las reglas del firewall es comparado con patrones establecidos, se analiza la frecuencia de ocurrencia y busca en los paquetes anomalías sospechosas.

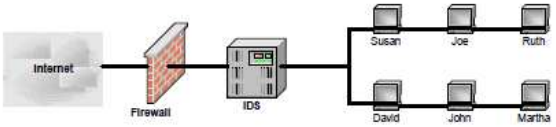


Figura 1. IDS basado en Red
Fuente: (SecurityMetrics Inc., 2003)

Los IDS basados en Host requieren de la instalación de un software en cada equipo que se desea monitorear. Esto origina que su mantenimiento sea más complejo ya que es indispensable que el software de cada equipo se mantenga actualizado para garantizar su efectividad.

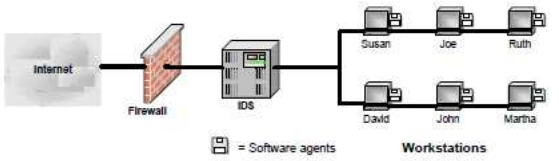


Figura 2. IDS basado en Host
Fuente: (SecurityMetrics Inc., 2003).

Un tema importante a considerar son los falsos positivos y falsos negativos. Ranum (2003) define los falsos positivos como una alerta por un evento que no es maligno, en otras palabras, un comportamiento normal que es detectado como una anomalía. Por otra parte, los falsos negativos son actividades anómalas o malignas que no generan una alarma y que pueden propiciar un ataque a los sistemas.

Cuando un IDS emplea una técnica basada en el conocimiento, la tasa de falsos positivos disminuye, pero esto implica la necesidad de que la base de conocimientos se actualice constantemente (Raut & Singh, 2014) y que haya existido una fase de aprendizaje que le permita reconocer el tráfico que existe en la red. Es importante señalar que los falsos positivos se incrementan cuando un IDS intenta detectar ataques desconocidos.

Una incorrecta configuración del IDS originará una alta tasa de falsos positivos, generando un incremento de las labores de los administradores que deberán analizar estas alertas, existiendo además la posibilidad de que tráfico malicioso no sea bloqueado, tal como lo refiere Firstov (2005).

Intrusion Prevention System (IPS)

Como se ha expuesto, los IDS permiten el análisis del tráfico de la red, pero no impiden que una amenaza se cristalice, ya que su finalidad es emitir alertas ante algún comportamiento anómalo, sin llegar a tomar acciones automáticas. Para suplir esta desventaja aparece la siguiente generación de tecnologías de seguridad: los Intrusion Prevention System (IPS). Un IPS se define como un dispositivo que tiene la capacidad de detectar y prevenir ataques, basándose en el análisis de anomalías o filtrado basado en firmas de ataques conocidos (Secure Computing Corporation, 2003).

Sequeira (2003) explica que los IPS implementan métodos de prevención cuyo objetivo es detener cualquier comportamiento malicioso antes de que cause algún daño. Al igual que los IDS, existen 2 tipos de IPS, los basados en Red y los basados en Host.

Los IPS han ido evolucionando constantemente, en sus inicios utilizaban como método de detección principalmente el reconocimiento de firmas, pero gracias a los avances tecnológicos hoy en día emplean un sinnúmero de métodos de detección que les permiten impedir intentos de ataque basados en aplicaciones o ataques a cualquier otra capa de red (Scarfone, Techtarget, 2015).

Los IPS pueden emplear varios métodos de detección, ya que cada método tiene una funcionalidad específica. Los primeros IPS usaban la técnica basada en firmas, pero en la actualidad, aunque se sigue utilizando este método, se combina con otros métodos que permitan mejorar la eficiencia del IPS. El método de detección basado en firmas consiste en la búsqueda dentro del tráfico de red de series de bytes o segmentos de paquetes que

anteriormente hayan sido catalogados como maliciosos. Este método permite el uso de firmas determinadas sobre todo cuando el alcance de protección está bien establecido, por ejemplo cuando el entorno a proteger puede ser accedido por algún protocolo en particular es posible incluir las firmas de los principales ataques que podrían intentar los criminales (Foster, 2005). Claro está que esto también genera un inconveniente ya que una firma solo se podrá crear una vez que un tipo de ataque ha sido identificado y catalogado como tal, motivo por el cual los nuevos tipos de ataques podrían pasar sin ser detectados.

Otro método de detección es el basado en anomalías, este método requiere determinar el comportamiento normal de la red, el cual debe ser aprendido o determinado por los administradores de la red. El motor de detección de anomalías, busca todo aquel comportamiento que se aleja del comportamiento normal previamente definido. El principal inconveniente es la definición de las reglas que determinan cuando un comportamiento es normal y cuando no. Este modelo también falla cuando el ataque genera un comportamiento aceptado como normal, porque involucra acciones, que en primera instancia se pueden considerar cotidianas, pero que son ejecutadas con fines delictivos (Foster, 2005).

El método de inspección profunda de paquetes o Deep Packet Inspection (DPI) por su nombre en inglés, es definido por Rouse (2007) como “un método avanzado de filtrado de paquetes que funciona en la capa de aplicación del modelo de referencia OSI” (p. 1). Esto implica que la búsqueda de código malicioso se realiza dentro el paquete y no sólo a nivel de cabecera como lo analiza el método de filtrado convencional. El DPI a pesar de que permite proteger de cierto tipo de ataques como los de denegación de servicios o desbordamiento de buffer, también puede ser explotado para ejecutar los ataques antes mencionados.

El análisis de flujo de red es otro método que se está utilizando en los IPS, ya que permite una mejor visualización de la seguridad de la red. Consiste en el análisis de IP, TCP, UDP y otra información de cabecera examinada junto con la fuente, los puertos de destino y las direcciones IP (Gregg, 2013).

Además de los métodos de detección antes citados es importante conocer las clases de IPS que existen en la actualidad. Los IPS pueden ser implementados en 3 modalidades: hardware o software dedicado, integrados a otros controles de seguridad y como servicio en la nube. Los IPS por hardware o software corresponden a dispositivos físicos o virtuales que realizan el proceso de monitoreo. Los IPS integrados a otros controles de seguridad son aquellos que incluyen las principales características de un IPS dentro de un dispositivo para mejorar sus capacidades; un ejemplo de estos son los firewalls de siguiente generación. Y el servicio en la nube corresponde a un nuevo tipo de servicio que es ofrecido por diversos proveedores en los cuales no se requiere tener un equipo físico o virtual dentro de las instalaciones de la organización sino únicamente contratar el servicio, el mismo que se aloja en la nube (Scarfone, Techtarget, 2015).

Next-Generation Firewalls (NGFWs)

Con el avance de la tecnología y el incremento de ataques a las redes de datos, los firewall fueron evolucionando a los hoy llamados Next Generation Firewall (NGFW), los mismos que integran las capacidades de un IPS al firewall, permitiéndole detectar y bloquear ataques sofisticados aplicando políticas de seguridad a nivel de aplicación, puertos y protocolos (Rouse, 2014). Son dispositivos que cuentan con funciones avanzadas que le permiten detectar y prevenir intrusiones, realizar un control de aplicaciones, prevenir pérdidas de datos, filtrado web y algunos tipos además incluyen funciones de antivirus.

Aunque es un tipo de tecnología relativamente nueva, Gartner en su informe referente a los Sistemas de Prevención de Intrusos del 2015 (Lawson, Hils, & Neiva, 2015), hace referencia al incremento de las implementaciones de NGFW y como estas han ido desplazando a los IPS. Pero en la actualidad la mayoría de proveedores de

Firewalls han ido incluyendo las nuevas características a sus productos lo que está generando que se conviertan en funciones básicas de un Firewall (Hils, 2015). Evidentemente existe una gran diversidad y tipo de características, por lo que cada proveedor combina las funciones de diversas maneras, y esto produce que el proceso de selección de esta clase de dispositivos sea más complejo y requiera de un mayor análisis.

Bring Your Own Device (BYOD)

Traducido al español es "trae tu propio dispositivo", una tendencia que cada día se incrementa en la mayoría de empresas e industrias, y que implica el uso de dispositivos móviles propios, sean estos laptops, tablets o smartphones, para la realización de actividades laborales. Esta práctica se ha popularizado gracias a las ventajas que implica, las mismas que incluyen la posibilidad de estar siempre conectado así como la facilidad de uso de un dispositivo propio y de la marca preferida del empleado. Pero a pesar de estas ventajas, las áreas de Tecnología tienen serias complicaciones con los controles de seguridad, políticas de soporte, así como las medidas que se debe implementar para evitar fugas de información (Reyes Vásquez, 2012). Para que las empresas que implementan BYOD puedan estar protegidas, es necesario que realicen un análisis que permita implementar políticas de uso y control de los dispositivos externos, además de una actualización de su plataforma de manera que logren distribuir correctamente los recursos.

La principal ventaja que muchas empresas encuentran al implementar políticas de BYOD es incrementar el nivel de satisfacción de los empleados, ya que según las encuestas, los empleados que tienen la libertad de usar sus propios dispositivos móviles incrementan su productividad. Otro factor que se podría considerar erróneamente como ventaja es la disminución de costos para las empresas, ya que no incurrirían en la adquisición de dispositivos móviles, pero la realidad es que este tipo de política no produce reducción de costos, ya que a pesar que disminuye la inversión en la adquisición de dispositivos móviles, se debe mejorar constantemente la infraestructura de manera que pueda estar asegurada correctamente (Alleau & Desemery, 2013).

Una implementación no planificada de BYOD puede exponer en la empresa a riesgos de seguridad y complicar la operación de la misma, debido a la existencia de un sinnúmero de dispositivos conectados a la red empresarial sin el debido monitoreo ni la certeza que el empleado haga un uso correcto de su dispositivo o el punto más básico, que cuente al menos con un buen software antivirus constantemente actualizado y una política de respaldos.

Mobile Device Management (MDM)

Justamente considerando las consecuencias que puede traer consigo la implementación de BYOD, aparece Mobile Device Management (MDM) ó Gestión de Dispositivos Móviles. Tal como indica Giusto Bilić (2016) las soluciones MDM "surgieron como un método para controlar el acceso de equipos móviles a los recursos de la empresa".

Existen un sinnúmero de proveedores de tecnología MDM, algunos tenían sus productos para computadores personales e incluyeron las funcionalidades necesarias para abarcar dispositivos móviles, otros únicamente ofrecen productos para la administración de dispositivos móviles. Aquellos sistemas especializados en dispositivos móviles generalmente ofrecen una solución más avanzada.

El servicio de MDM se puede contratar de 3 diferentes maneras: 1) como implementación dentro de la empresa, en la cual el proveedor instala el producto en las instalaciones del cliente, y es este quien administra la aplicación; 2) servicio en la nube, en la cual la solución se provee desde una nube del proveedor, sin que el cliente requiera invertir en tecnología para la implementación; y por último 3) como servicio gestionado, en el cual el proveedor ofrece el servicio pero además se encarga de gestionarlo (Durán-Sindreu Terol, 2012).

Hoy en día las aplicaciones MDM han ido mejorando la funcionalidad hasta el punto de permitir la administración de los sistemas operativos y aplicaciones existentes, borrado remoto de información en caso de pérdida o robo, así como el monitoreo de los paquetes que viajan por las redes corporativas. Permiten llegar a limitar las aplicaciones que se puede instalar gracias al uso de tiendas personalizadas.

Otra ventaja es que permiten separar la información corporativa de la información personal del empleado, lo que impide que la información propia de la empresa se divulgue con terceros no autorizados. Pero es necesario tener claro que este tipo de tecnología no representa una seguridad absoluta, ya que siempre existirá la amenaza de virus, malware o cualquier otro tipo de incidente que afecte al dispositivo móvil, por lo que es importante que se implementen políticas de seguridad que cubran múltiples capas.

METODOLOGÍA.

Para la elaboración del presente trabajo se realizó un análisis exploratorio de la situación interna actual de la empresa, que incluyo una serie de revisiones de la Infraestructura existente, se entrevistó a funcionarios y proveedores, así como también se ejecutó varios aplicativos relacionados al análisis de redes, entre los cuales se incluyó Acrylic WiFi, Wireshark y SolarWind (versión demo) para la realización de un mapeo de la red. Es importante señalar que debido a la existencia de acuerdos de confidencialidad, este estudio sólo incluye evidencias de los documentos autorizados a publicar.

Gracias al análisis realizado se logró evidenciar las falencias existentes en las redes de datos. Las entrevistas realizadas con el personal de la empresa y con varios proveedores de la tecnología existente, permitieron afianzar los resultados de los análisis efectuados.

Para la selección de los criterios a considerar en las herramientas propuestas se realizaron reuniones que permitieron, a través de una lluvia de ideas, determinar los principales factores que debían ser considerados. Posteriormente se realizó un focus group, que permitió valorar la importancia de cada uno de los factores determinantes para el producto a través de una matriz de priorización.

El alcance del presente trabajo incluye la demostración de las falencias y las recomendaciones tanto en procesos como en herramientas a implementar que permitirán mejorar los niveles de desempeño y seguridad de la red corporativa.

ANÁLISIS DE RESULTADOS

DIAGNOSTICO DE SITUACION ACTUAL

El presente estudio se basa en el análisis de la situación en la infraestructura de redes de la empresa CONFIDENCIAL S.A. Se trata de una empresa mediana que cuenta con 650 empleados. Posee sucursales en varias ciudades: Ambato, Cuenca, Manta y Riobamba, pero su matriz está ubicada en la ciudad de Guayaquil y la oficina principal en la ciudad de Quito. La empresa ha tenido un crecimiento constante desde hace 5 años, fecha en que, por temas logísticos, se cambió a las nuevas instalaciones. Este cambio implicó la adecuación de dos áreas destinadas a un datacenter principal y un datacenter secundario.

Considerando que las instalaciones están conformadas por dos edificios, se definió que la ubicación del datacenter principal sería en el edificio administrativo. El datacenter secundario se instaló en la planta baja del edificio de la planta.

Durante la remodelación del inmueble que se convertiría en la oficina matriz, la empresa contrató diversos servicios para la puesta en marcha del proyecto, entre ellos el servicio de cableado estructurado, así como la movilización de los racks existentes en el edificio antiguo. El

datacenter principal se conectó con el datacenter secundario a través de un enlace de fibra óptica (ver anexo 1).

Considerando que al momento del cambio a las nuevas instalaciones el número de equipos existentes no excedía de 300 y sólo contaban con 10 servidores, el administrador estableció 3 subredes para la estructura de la red. Se incluyó la implementación de varios switch de capa 3, marca ZYXEL que poseían la capacidad de creación de Virtual LAN (VLANS), según el estándar IEEE 802.1Q. Pero según lo indicado (Proveedor 1, comunicación personal, 28 de diciembre del 2016) no se realizó la implementación completa de las recomendaciones dadas para el proyecto, que incluía la instalación de una backbone colapsada.

En la actualidad no existe ningún tipo de segmentación ni creación VLAN o De-Militarized Zone (DMZ), lo que ha generado que la infraestructura de redes tenga muchos inconvenientes y una muestra de esto es la gran cantidad de broadcast que se genera, el mismo que se evidencia en un análisis de tráfico realizado con la herramienta Wireshark (ver anexo 2).

La empresa cuenta con un firewall por software llamado KERIO CONTROL versión 9.0, el mismo que está instalado en una PC ubicado en la matriz. También cuenta con KERIO CONNECT para la gestión de correo electrónico. Este software se actualizó recientemente a la última versión, tanto en los servidores de Guayaquil y Quito.
En el firewall se implementó una serie de políticas y reglas, pero existen varios parámetros por defecto que no han sido analizados para mejorar y utilizar todas las funcionalidades del firewall. KERIO CONTROL incluye un IPS basado en SNORT, el mismo que, según conversaciones mantenidas (Proveedor 1, comunicación personal, 29 de diciembre del 2016) no ha sido configurado apropiadamente, y cuyas reglas no han sido personalizadas.

Un tema adicional a considerar es que a pesar de la existencia de una política de uso de internet y correo electrónico en la que se incluye una sección relacionada a la prohibición del uso de dispositivos móviles personales, existen muchos funcionarios que han sido autorizados por la Gerencia General para el uso de sus dispositivos dentro de la red corporativa. En estos momentos según lo indicado por Funcionario 1 (comunicación personal, 7 de diciembre del 2016), los gerentes, directores y varios funcionarios de los departamentos Financiero, Comercial y de negocios hacen uso de sus dispositivos personales y tienen acceso a las redes inalámbricas de la empresa. Esto sin que exista una política de control BYOD, ni las medidas básicas para mitigar efectos indeseables, como violaciones de seguridad, fuga de información, pérdida de datos, entre otros.

Con base en los inconvenientes detectados se procederá a realizar una serie de recomendaciones orientadas a mejorar los niveles de desempeño y seguridad de la red corporativa de la empresa CONFIDENCIAL S.A.

RECOMENDACIONES

Uso de VLANs

Considerando que la red de la empresa CONFIDENCIAL S.A. reflejó una gran cantidad de broadcast, el cual se origina cuando una computadora lanza un mensaje para determinar la ubicación de otro dispositivo, pero que usa el medio común para transmitir el mensaje, se recomienda la creación de VLANs dentro de los switches existentes, de manera que los mensajes de broadcast solo se limiten a ciertos puertos y de esta forma se afecte la menor cantidad de estaciones. Además de la definición de un bloque de direcciones IP por cada VLAN.

La implementación de esta recomendación permitirá una menor congestión al separar los dominios de broadcast, con la ventaja adicional de tener la capacidad de establecer un ancho de banda específico a cada puerto del switch, lo que

permitirá incrementar los niveles de seguridad de la red.

Es importante resaltar que segmentar la red a través de VLANs permite además reducir y limitar el alcance en el cumplimiento de la norma PCI DSS, la misma que es requerida a las empresas que procesan, almacenan o transmiten datos de tarjetas de crédito (Segarra López, 2012).

La configuración VLAN por defecto del switch ZYXEL se muestra en la figura 3 y el procedimiento recomendado por Soporte Técnico ZYXEL se puede revisar en la página oficial del producto. Adicionalmente el personal de la empresa CONFIDENCIAL S.A. posee al momento un contrato de soporte con el proveedor que le permitirá contar con ayuda especializada.

Figura 3. Configuración por defecto de VLAN en switch ZYXEL
Fuente: (ZYXEL, S/A)

Implementación DMZ

Una De-Militarized Zone (DMZ) o zona desmilitarizada implica la ubicación de los servidores de acceso público en un segmento independiente y aislado de la red, esto con la finalidad de impedir que estos servidores estén en contacto con segmentos internos de la red.

Al momento la empresa CONFIDENCIAL S.A. no cuenta con una DMZ por lo que los servidores con acceso a internet se encuentran dentro de la red principal sin ningún tipo de protección adicional. La implementación de una DMZ permitirá tener aislados los servidores que tienen acceso a internet, como por ejemplo el servidor de correo, lo cual generará que el tráfico interno de la red no sea visible en la DMZ, dando un mayor nivel de seguridad a la información sensible de la empresa.

Para la implementación de una DMZ es vital el firewall, ya que es ahí donde se establecen las políticas de protección de la red local de la DMZ.

El firewall existente en la empresa, KERIO CONTROL, permite la creación de la DMZ a través de ciertas reglas que se debe establecer. En la figura 4 se muestra una serie de reglas de tráfico que maneja KERIO CONTROL.

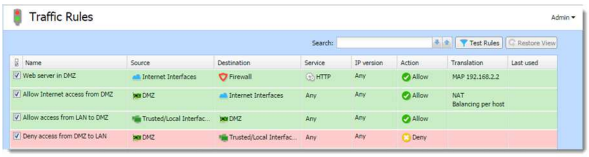


Figura 4. Reglas de Tráfico Kerio Control
Fuente: (Ferschmannová , 2016)

Aplicando las reglas de tráfico, KERIO CONTROL permite una infraestructura como la indicada en la figura 5. Es importante conocer que el portal oficial de KERIO CONTROL cuenta con el procedimiento completo de creación de una DMZ.

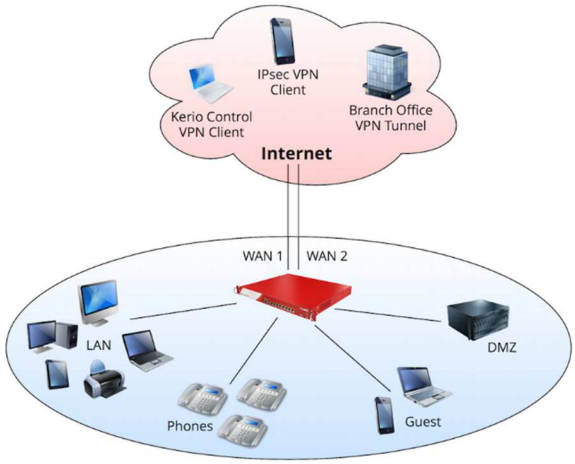


Figura 5. Infraestructura de red usando Kerio Control
Fuente: (Redicom - Centro de Ayuda, 2016)

Revisión de la configuración de KERIO CONTROL

Es necesario realizar una revisión completa de las configuraciones existentes en el software de KERIO CONTROL de preferencia en conjunto con personal especializado y con certificaciones en el manejo de los dispositivos KERIO.

Considerando el crecimiento de la empresa y con la finalidad de actualizar tecnología se recomienda la implementación de KERIO CONTROL NG 500 el cual está recomendado para medianas empresas y se puede montar en un rack.

En la actualidad la empresa mantiene el software de KERIO CONTROL en un computador personal básico, que por su naturaleza no fue diseñado para un funcionamiento continuo 24x7. Se recomienda mejorar esta implementación sin incurrir en el costo de un servidor como tal, sino en un dispositivo físico especialmente diseñado para este propósito. Esto permitirá un ahorro equivalente al costo de un servidor como tal, más el costo de las licencias de usuario que se adquiere cuando ingresa nuevo personal a la empresa.

El dispositivo KERIO CONTROL NG 500 posee un procesador de 4 núcleos y memoria de 4 GB. Tienen embebido el software KERIO CONTROL, Existe un modelo que incluye el uso para usuarios ilimitados. El precio de lista es de $3.950,00 para el primer año, pero si se considera los gastos de nacionalización adicionales, la solución puede llegar a costar $8.000,00. La lista completa de características de este dispositivo se detalla en el anexo 3.

Implementación de políticas BYOD

Debido a que se evidenció el uso de dispositivos móviles personales por parte de un número considerable de funcionarios, se recomienda la definición e implementación de políticas de BYOD.

Para esto, es necesario que el área de Tecnología establezca políticas de seguridad relacionadas a los datos, redes y accesos, definir un catálogo de dispositivos permitidos, así como el alcance de la cobertura que brindará la empresa. Se deberán definir normas, así como las medidas necesarias para el cumplimiento de las mismas.

En la figura 6 se incluye un resumen de los puntos importantes a considerar previo a la implementación de una política BYOD, el mismo que está basado en una investigación realizada por Deloitte Research (2013).

POLITICAS CLAVE	DEFINICION
Elegibilidad del empleado	Definir que empleados pueden ser incluidos en el programa de BYOD
Acuerdo de financiación BYOD	Definir si la empresa cubrirá costos de adquisición de dispositivos
Modelo de soporte para dispositivos propiedad de los empleados	El alcance del soporte que brindará la empresa
Educación de los empleados y gestión del cambio	Talleres de capacitación para el correcto uso de BYOD por parte de los funcionarios
Legal y privacidad	Analizar las implicaciones legales así como de privacidad

Figura 6. Resumen de Políticas clave para BYOD
Fuente: (Deloitte Research , 2013)

Como se indicó previamente, una correcta implementación de las políticas necesarias para BYOD permitirá mantener un nivel aceptable de seguridad para la organización.

Implementación de un Mobile Device Management (MDM)

Una vez definidas las políticas BYOD se recomienda implementar un software de gestión de dispositivos móviles. Se realiza esta recomendación para que la empresa CONFIDENCIAL S.A. posea un mejor control de la información que se maneja a través de dispositivos móviles, evitará pérdidas de información confidencial en caso de robo de dispositivos, así como también se logrará prevenir fugas de información.

Previo a la definición de la herramienta a recomendar se realizó una estimación del número de dispositivos que se deberá proteger. Se consideró que en la actualidad emplean dispositivos móviles propios el siguiente personal: gerentes de departamento (8), directores (10), personal de los Dptos. Financiero (5), Comercial (5), Negocio (3). El total actual de usuarios que emplean dispositivos propios es de 31. Considerando el crecimiento se estima que la política de BYOD incluirá un mínimo de 40 funcionarios.

Para realizar la selección del software que mejor se ajuste a los requerimientos de la empresa CONFIDENCIAL S.A., se tomó en consideración el análisis comparativo realizado por Solutions Review (2017), el mismo que permitirá analizar las caracteristicas de los principales productos existentes en el mercado.

Se considerará las funcionalidades básicas descritas en la figura 7. La ponderación de cada funcionalidad se definió en base a un focus group realizado con el personal de Sistemas, en el cual participaron los niveles altos y medios, quienes apoyándose en la situación actual y experiencias previas, valoraron la importancia relativa de cada criterio respecto el resto de criterios, considerando una escala predefinida (Anexo 4).

CARACTERISTICAS NECESARIAS	PONDERACION
Soporte Android, iOS	12%
Integración con el directorio activo	15%
Facilidad para creación de perfiles	4%
Manejo de inventario de hardware y software	8%
Actualización remota	7%
Políticas de seguridad remotas (borrado, bloqueo, cifrado)	15%
Configuración centralizada de parámetros básicos	8%
Blacklist y whitelist de aplicaciones	12%
Inventario de dispositivos	7%
Copia de seguridad remota	12%
	100%

Figura 7. Ponderación de Funcionalidades básicas MDM
Fuente: Elaboración propia

Basándose en las caracteristicas definidas y en el análisis comparativo de Solutions Review (2017), se determina los 4 principales productos que cumplen las especificaciones (Figura 8).

CARACTERISTICAS NECESARIAS	VMWARE AIRWATCH	CITRIX XENMOBILE	SOTI MOBICONTROL	IBM MAAS360
Soporte Android, iOS	✓	✓	✓	✓
Integración con el directorio activo	✓	✓	✓	✓
Facilidad para creación de perfiles	✓	✓	✓	✓
Manejo de inventario de hardware y software	✓	✓	✓	✓
Actualización remota	✓	✓	✓	✓
Políticas de seguridad remotas (borrado, bloqueo, cifrado)	✓	✓	✓	✓
Configuración centralizada de parámetros básicos	✓	✓	✓	✓
Blacklist y whitelist de aplicaciones	✓	✓	✓	✓
Inventario de dispositivos	✓	✓	✓	✓
Copia de seguridad remota	✓	✓	✓	✓

Figura 8. Productos que cumplen características básicas
Fuente: Elaboración propia

La Gerencia de Sistemas estableció que para la selección del producto coordinará, con los diversos proveedores, la implementación de versiones demo para de esta manera determinar cuál es el producto que mejor se ajusta a las necesidades de la empresa y realizará el análisis incluyendo el costo de la solución.

CONCLUSIONES

Con los resultados de los análisis realizados en el presente trabajo fue posible evidenciar falencias existentes en las redes de datos, así como la falta de políticas para normar actividades como la del uso de dispositivos móviles propios, algo que no había sido considerado una amenaza para la organización.

El departamento de Sistemas, ahora cuenta con los resultados de un análisis externo, que le permitirán justificar la necesidad de mejorar su infraestructura de redes, proceder con la definición de una política BYOD y en base a las revisión de herramientas MDM seleccionadas, realizar un proceso de evaluación de cada una de ellas.

La actualización del Firewall y su correcta configuración permitirá a la empresa contar con las funcionalidades de un IPS, que ayudará a mitigar posibles intrusiones a los sistemas, así como evitar que los equipos informáticos lleguen a ser atacados para convertirlos en parte de botnets, lo que originaría consumo de recursos para fines delictivos.

Entre las limitaciones que se encontró están la imposibilidad de incluir los documentos evidencia de los procesos realizados, los mismos que se encuentran amparados por una cláusula de confidencialidad, que impide demostrar gráficamente los resultados obtenidos. Por otro lado, es necesario considerar que la omisión de

información por parte de los mandos altos o medios en el departamento de Sistemas puede generar un sesgo en la investigación.

Queda pendiente para la empresa CONFIDENCIAL S.A. la gestión y acercamiento con los diversos proveedores de soluciones MDM quienes, además de demostrar las bondades de cada producto, podrían contribuir en la creación de políticas BYOD.

Además, luego de la aplicación de las recomendaciones realizadas para las redes de datos, podrían analizar las mejoras obtenidas comparando los nuevos resultados con los generados durante la realización del análisis relacionado a este estudio es decir, realizar una auditoría longitudinal.

REFERENCIAS BIBLIOGRÁFICAS

Alleau, B., & Desemery, J. (2013). *Bring Your Own Device It's all about Employee Satisfaction and Productivity, not Costs!* Capgemini Consulting.

Bruneau, G. (2001). The History and Evolution of Intrusion Detection.

Deloitte Research . (2013). *Understanding the Bring-Your-Own-Device landscape.*

Durán-Sindreu Terol, S. (2012). *Mobile Device Management.* Barcelona.

Ferschmannová , V. (21 de 07 de 2016). *KERIO Knowledge Base*. Obtenido de KERIO: http://kb.kerio.com/product/kerio-control/traffic-rules/configuring-demilitarized-zone-dmz-347.html

Firstov, S. (2005). *Case Study on a Successful Implementation of Juniper/Netscreen IDP.*

Foster, J. (05 de 2005). *TechTarget*. Obtenido de IDS: Signature versus anomaly detection: http://searchsecurity.techtarget.com/tip/IDS-Signature-versus-anomaly-detection

Giusto Bilić, D. (07 de 01 de 2016). *Welivesecurity (en español)*. Obtenido de ¿Qué son las soluciones MDM y por qué debes tenerlas en mente?: http://www.welivesecurity.com/la-es/2016/01/07/que-son-las-soluciones-mdm/

Gregg, M. (05 de 2013). *TechTarget*. Obtenido de Using network flow analysis to improve network security visibility: http://searchsecurity.techtarget.com/tip/Using-network-flow-analysis-to-improve-network-security-visibility

Hils, A. (29 de 12 de 2015). *Gartner Blog Network*. Obtenido de For 2016, Should We Retire the "Next Generation Firewall"?: http://blogs.gartner.com/adam-hils/for-2016-should-we-retire-the-term-next-generation-firewall/

Jyothsna, V., & Rama Prasad, V. V. (2011). A Review of Anomaly based IntrusionDetection Systems. *International Journal of Computer Applications (*, 26-35.

Kemmerer, R. A., & Vigna, G. (2002). Intrusion Detection: A Brief History and Overview. *Security & Privacy*, 27-30.

Lawson, C., Hils, A., & Neiva, C. (16 de 11 de 2015). *Gartner, Inc*. Obtenido de Magic Quadrant for Intrusion Prevention Systems: https://www.gartner.com/doc/reprints?id=1-2SGN5HM&ct=151118&st=sb

Ranum, M. J. (2003). *False Positives: A User's Guide to Making Sense of IDS Alarms.* ICSA Labs IDSC. Obtenido de IDFAQ: What is a false positive and why are false positives a problem?: https://www.sans.org/security-resources/idfaq/what-is-a-false-positive-and-why-are-false-positives-a-problem/2/8

Raut, A. S., & Singh, K. R. (2014). Anomaly Based Intrusion Detection-A Review. *Int. J. on Network Security, 5*, 7-12.

Redicom - Centro de Ayuda. (09 de 05 de 2016). *REDICOM*. Obtenido de Inicio rápido con Kerio Control: https://redicom.freshdesk.com/support/solutions/articles/8000034929-inicio-r%C3%A1pido-con-kerio-control

Reyes Vásquez, V. E. (2012). BYOD y la movilidad corporativa. *ING-NOVACIÓN*, 117-121.

Rouse, M. (11 de 2007). *TechTarget*. Obtenido de Deep packet inspection (DPI): http://searchnetworking.techtarget.com/definition/deep-packet-inspection-DPI

Rouse, M. (01 de 2014). *TechTarget Network.* Recuperado el 11 de 12 de 2016, de Next-Generation Firewall (NGFW): http://searchsecurity.techtarget.com/definition/next-generation-firewall-NGFW

Scarfone, K. (10 de 2015). *Techtarget.* Obtenido de The basics of network intrusion prevention systems: http://searchsecurity.techtarget.com/feature/The-basics-of-network-intrusion-prevention-systems

Scarfone, K., & Mell, P. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS).* Gaithersburg.

Secure Computing Corporation. (2003). *Intrusion Prevention Systems (IPS).*

SecurityMetrics Inc. (2003). *Integrated, Vulnerability Asessment, Intrusion Detection and Prevention.*

Segarra López, M. (2012). Usando la segmentación de red para reducir el alcance de PCI DSS. *S I C*, 82-95.

Sequeira, D. (2003). Intrusion Prevention Systems: Security's Silver Bullet? *BUSINESS COMMUNICATIONS REVIEW*, 36-41.

Singh, G., Goyal, S., & Agarwal, R. (s/a). Intrusion Detection Using Network Monitoring Tools. India.

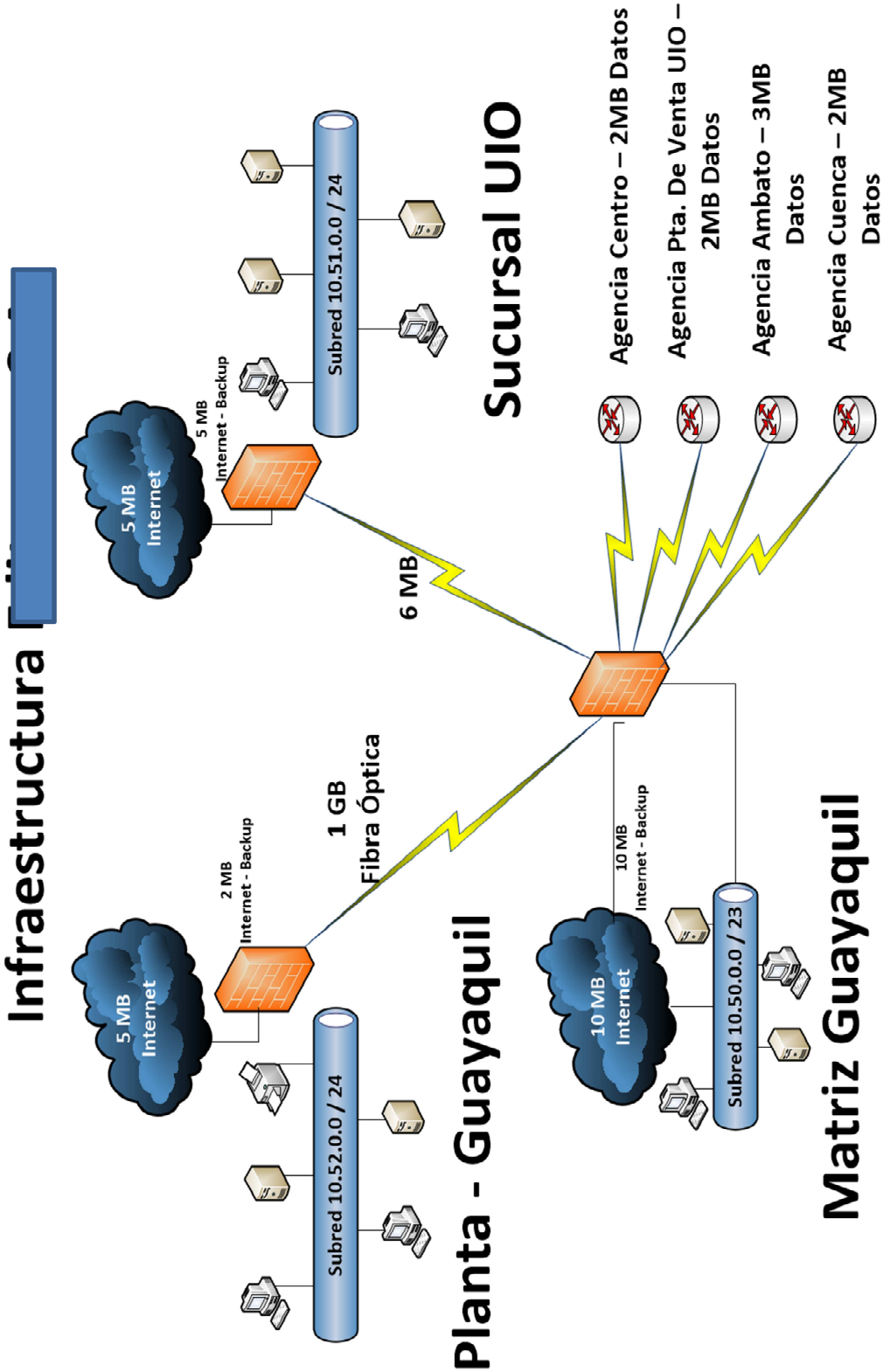
Solutions Review . (2017). *Mobility Management Buyer's Guide.* Massachusetts. Obtenido de Comparison of MDM Providers: http://www.enterpriseios.com/wiki/Comparison_MDM_Providers

Trend Micro Incorporated. (2015). *REPORTE DE SEGURIDAD CIBERNÉTICA E INFRAESTRUCTURA CRÍTICA DE LAS AMÉRICAS.*

ZYXEL. (S/A). *ZYXEL*. Obtenido de ZYXEL Knowledge Base: https://kb.zyxel.com/KB/searchArticle!viewDetail.action?articleOid=014091&lang=EN

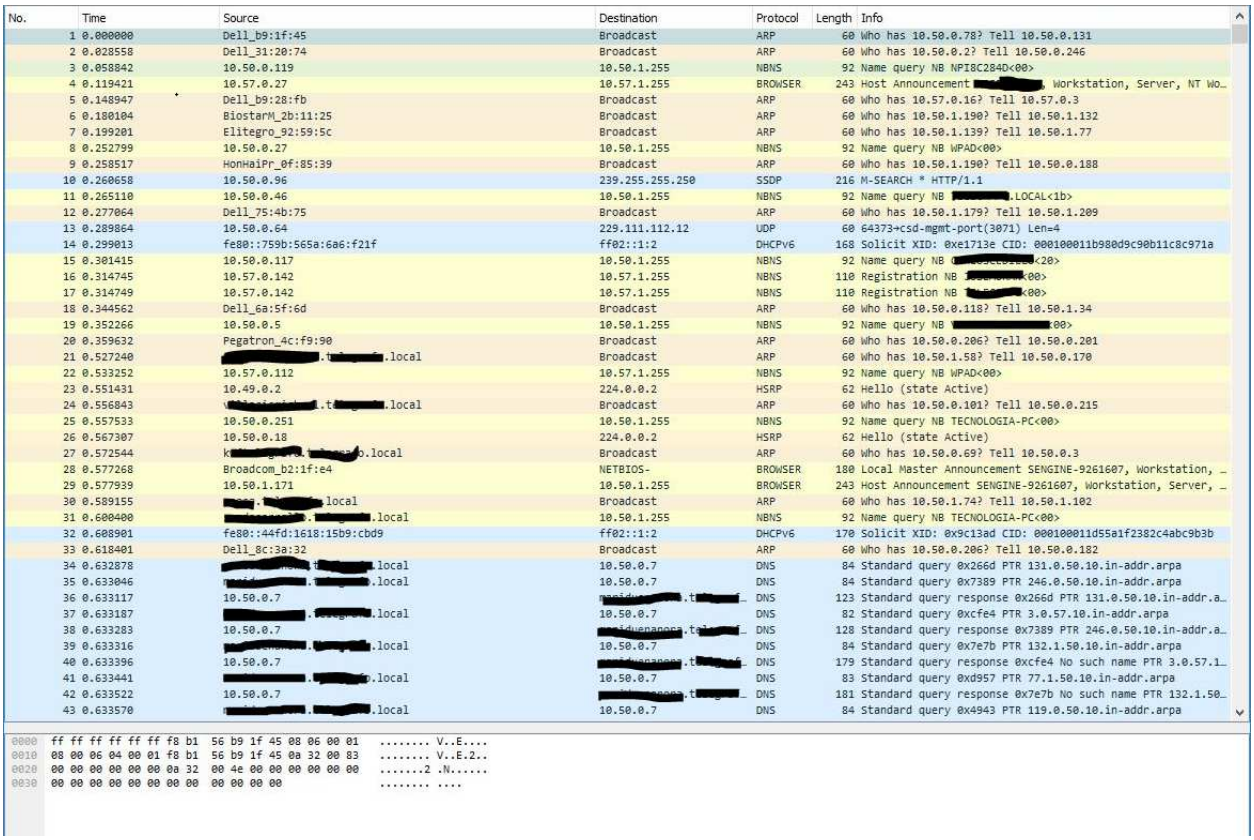
ANEXO 1

ESTRUCTURA DE RED



ANEXO 2

RESULTADOS DE ANALISIS A LA RED – HERRAMIENTA WIRESHARK



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Dell_b9:1f:45	Broadcast	ARP	60	Who has 10.50.0.78? Tell 10.50.0.131
2	0.028558	Dell_31:20:74	Broadcast	ARP	60	Who has 10.50.0.2? Tell 10.50.0.246
3	0.058842	10.50.0.119	10.50.1.255	NBNS	92	Name query NB NPI8C284D<00>
4	0.119421	10.57.0.27	10.57.1.255	BROWSER	243	Host Announcement [redacted], Workstation, Server, NT Wo…
5	0.148947	Dell_b9:28:fb	Broadcast	ARP	60	Who has 10.57.0.16? Tell 10.57.0.3
6	0.180104	BiostarM_2b:11:25	Broadcast	ARP	60	Who has 10.50.1.190? Tell 10.50.1.132
7	0.199201	Elitegro_92:59:5c	Broadcast	ARP	60	Who has 10.50.1.139? Tell 10.50.1.77
8	0.252799	10.50.0.27	10.50.1.255	NBNS	92	Name query NB WPAD<00>
9	0.258517	HonHaiPr_0f:85:39	Broadcast	ARP	60	Who has 10.50.1.190? Tell 10.50.0.188
10	0.260658	10.50.0.96	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
11	0.265110	10.50.0.46	10.50.1.255	NBNS	92	Name query NB [redacted].LOCAL<1b>
12	0.277064	Dell_75:4b:75	Broadcast	ARP	60	Who has 10.50.1.179? Tell 10.50.1.209
13	0.289864	10.50.0.64	229.111.112.12	UDP	60	64373+csd-mgmt-port(3071) Len=4
14	0.299013	fe80::759b:565a:6a6:f21f	ff02::1:2	DHCPv6	168	Solicit XID: 0xe1713e CID: 000100011b980d9c90b11c8c971a
15	0.301415	10.50.0.117	10.50.1.255	NBNS	92	Name query NB [redacted]<20>
16	0.314745	10.57.0.142	10.57.1.255	NBNS	110	Registration NB [redacted]<00>
17	0.314749	10.57.0.142	10.57.1.255	NBNS	110	Registration NB [redacted]<00>
18	0.344562	Dell_6a:5f:6d	Broadcast	ARP	60	Who has 10.50.0.118? Tell 10.50.1.34
19	0.352266	10.50.0.5	10.50.1.255	NBNS	92	Name query NB [redacted]<00>
20	0.359632	Pegatron_4c:f9:90	Broadcast	ARP	60	Who has 10.50.0.206? Tell 10.50.0.201
21	0.527240	[redacted].local	Broadcast	ARP	60	Who has 10.50.1.58? Tell 10.50.0.170
22	0.533252	10.57.0.112	10.57.1.255	NBNS	92	Name query NB WPAD<00>
23	0.551431	10.49.0.2	224.0.0.2	HSRP	62	Hello (state Active)
24	0.556843	[redacted].local	Broadcast	ARP	60	Who has 10.50.0.101? Tell 10.50.0.215
25	0.557533	10.50.0.251	10.50.1.255	NBNS	92	Name query NB TECNOLOGIA-PC<00>
26	0.567307	10.50.0.18	224.0.0.2	HSRP	62	Hello (state Active)
27	0.572544	[redacted].local	Broadcast	ARP	60	Who has 10.50.0.69? Tell 10.50.0.3
28	0.577268	Broadcom_b2:1f:e4	NETBIOS-	BROWSER	180	Local Master Announcement SENGINE-9261607, Workstation, …
29	0.577939	10.50.1.171	10.50.1.255	BROWSER	243	Host Announcement SENGINE-9261607, Workstation, Server, …
30	0.589155	[redacted].local	Broadcast	ARP	60	Who has 10.50.1.74? Tell 10.50.1.102
31	0.600400	[redacted].local	10.50.1.255	NBNS	92	Name query NB TECNOLOGIA-PC<00>
32	0.608901	fe80::44fd:1618:15b9:cbd9	ff02::1:2	DHCPv6	170	Solicit XID: 0x9c13ad CID: 000100011d55a1f2382c4abc9b3b
33	0.618401	Dell_8c:3a:32	Broadcast	ARP	60	Who has 10.50.0.206? Tell 10.50.0.182
34	0.632878	[redacted].local	10.50.0.7	DNS	84	Standard query 0x266d PTR 131.0.50.10.in-addr.arpa
35	0.633046	[redacted].local	10.50.0.7	DNS	84	Standard query 0x7389 PTR 246.0.50.10.in-addr.arpa
36	0.633117	10.50.0.7	[redacted]	DNS	123	Standard query response 0x266d PTR 131.0.50.10.in-addr.a…
37	0.633187	[redacted].local	10.50.0.7	DNS	82	Standard query 0xcfe4 PTR 3.0.57.10.in-addr.arpa
38	0.633283	10.50.0.7	[redacted]	DNS	128	Standard query response 0x7389 PTR 246.0.50.10.in-addr.a…
39	0.633316	[redacted].local	10.50.0.7	DNS	84	Standard query 0x7e7b PTR 132.1.50.10.in-addr.arpa
40	0.633396	10.50.0.7	[redacted]	DNS	179	Standard query response 0xcfe4 No such name PTR 3.0.57.1…
41	0.633441	[redacted].local	10.50.0.7	DNS	83	Standard query 0xd957 PTR 77.1.50.10.in-addr.arpa
42	0.633522	10.50.0.7	[redacted]	DNS	181	Standard query response 0x7e7b No such name PTR 132.1.50…
43	0.633570	[redacted].local	10.50.0.7	DNS	84	Standard query 0x4943 PTR 119.0.50.10.in-addr.arpa

```
0000  ff ff ff ff ff ff f8 b1  56 b9 1f 45 08 06 00 01   ........ V..E....
0010  08 00 06 04 00 01 f8 b1  56 b9 1f 45 0a 32 00 83   ........ V..E.2..
0020  00 00 00 00 00 00 0a 32  00 4e 00 00 00 00 00 00   .......2 .N......
0030  00 00 00 00 00 00 00 00  00 00 00 00              ........ ....
```

ANEXO 3

CARACTERISTICAS DE DISPOSITIVO KERIO CONTROL NG500

	KERIO CONTROL NG500
Usuarios incluidos	Ilimitados
Software	Kerio Control with Sophos Antivirus and Kerio Control Web Filter
CARACTERISTICAS	
Chasis	1 U Rack mount unit
Dimension	16.97 x 1.73 x 12 in / 431 x 44 x 305 mm
Peso	15.4 lb / 7 kg
Ethernet	6 x 10/100/1000 RJ-45
Otros puertos	2 x USB 2.0, 1x RJ45 Console
Entrada de poder	220W
Promedio de consumo	30W
Disco duro	32 GB SSD
Memoria	4 GB
Procesador	Intel Core i5-4570S 4 Cores / 4 Threads 3.6GHz
Garantia	Standard 1 año
PERFORMANCE	
Firewall	1 Gbit/s
IPS	610 Mbit/s
Antivirus	340 Mbit/s
UTM (FW + IPS + AV + WebFilter)	250 Mbit/s

ANEXO 4

TABLA DE VALORACION DE CRITERIOS A CONSIDERAR PARA LA SELECCIÓN DE UN MDM

	Soporte Android, iOS	Integracion con el directorio activo	Facilidad para creacion de perfiles	Manejo de inventario de hardware y software	Actualizacion remota	Politicas de seguridad remotas (borrado, bloqueo, cifrado)	Configuracion centralizada de parametros basicos	Blacklist y whitelist de aplicaciones	Inventario de dispositivos	Copia de seguridad remota	TOTAL FILA	% TOTAL GLOBAL
Soporte Android, iOS		1	5	1	1	0,5	1	1	1	2	13,5	12%
Integracion con el directorio activo	2		5	1	2	1	2	1	2	1	17	15%
Facilidad para creacion de perfiles	0,5	0,5		0,5	0,5	0,5	0,5	0,5	0,5	0,5	4,5	4%
Manejo de inventario de hardware y software	0,5	1	2		1	0,5	1	1	1	0,5	8,5	8%
Actualizacion remota	0,5	0,5	1	0,5		0,5	1	1	2	1	8	7%
Politicas de seguridad remotas (borrado, bloqueo, cifrado)	1	1	5	2	2		2	1	2	1	17	15%
Configuracion centralizada de parametros basicos	1	0,5	2	2	1	0,5		0,5	1	1	9,5	8%
Blacklist y whitelist de aplicaciones	1	1	2	2	1	1	2		1	2	13	12%
Inventario de dispositivos	0,5	0,5	1	1	2	0,5	1	0,5		0,5	7,5	7%
Copia de seguridad remota	0,5	0,5	5	1	1	0,5	2	1	2		13,5	12%
TOTAL COLUMNA	7,5	6,5	28	11	11,5	5,5	12,5	7,5	12,5	9,5	112	

ESCALA

1 = Igualdad en importancia o preferencia.

2 = Mas importante o preferido.

5 = Significativamente más importante o preferido.