UNIVERSIDAD POLITÉCNICA DE PUEBLA
Ingeniería en Informática

Proyecto de Estadía Profesional

"Implementación de Filtrado Web para equipos móviles en Corporativo y Sucursales de ATM"

Área temática del CONACYT: VII
Ingenierías y tecnologías

Presenta:
Jan Carlos Robles Ortega

Asesor técnico
Ing. Javier Ruano Martínez

Asesor académico
MC Rebeca Rodríguez Huesca

Juan C. Bonilla, Puebla, México. 18 de Diciembre de 2019

Resumen

El presente proyecto consiste en la implementación de Filtrado Web para equipos móviles en corporativo y sucursales ATM, el cual considera la problemática y los requerimientos de la empresa AutoTodo Mexicana.

Se pretende implementar un filtrado web bajo la norma ISO 27001 emitida por la Organización Internacional de Normalización (ISO) que describe cómo gestionar la seguridad de la información en una empresa, asegurando la confidencialidad, disponibilidad e integridad de los datos. Así mismo, se pone en práctica los conocimientos adquiridos en la carrera de Ingeniería en Informática en la Universidad Politécnica de Puebla.

La finalidad de este proyecto es administrar los accesos a los usuarios de las sucursales de acuerdo al perfil de trabajo de cada uno de ellos y así mismo restringir las páginas de streaming, maliciosas o no permitidas, limitando el ancho de banda de internet y evitando pérdida de información confidencial.

Índice

1. Introducción 7
1.1. Descripción del problema o necesidad 7
1.2 Justificación 7
1.3 Objetivo General y Específicos 8
2. Metodología y herramientas 9
2.1 Metodología PVHA para la Gestión de la Seguridad Informática 9
2.2 Sistema de Gestión de la Seguridad de la Información 10
2.3 Redes Alámbricas 14
2.4 Redes Inalámbricas 14
2.5 Ataques 16
2.6 Software Malicioso (Malware) 20
2.7 Herramientas 23
3. Resultados 28
3.1 Planificar (Establecer el SGSI) 28
3.2 Hacer (Implementar y operar el SGSI) 36
3.3 Verificar (Revisar y dar seguimiento al SGSI) 55
3.4 Actuar (Mantener y mejorar el SGSI) 58
4.Conclusiones y recomendaciones 64
5. Referencias bibliográficas 66

Índice de figuras

Figura 1. Modelo de PVHA 9
Figura 2. Tríada CID 11
Figura 3. Estructura de ISO 27001 12
Figura 4. Ataque Pasivo 17
Figura 5. Ataque Activo 18
Figura 6. Amenazas internas y externas 20
Figura 7. Distribución de Malware por categorías 22
Figura 8. Organigrama 29
Figura 9. Virus 34
Figura 10. Descripción de Virus 34
Figura 11. Saturación de Red 35
Figura 12. Porcentaje de Riesgo 35
Figura 13. Costo de Proyecto 35
Figura 14. Instalación de WSS 36
Figura 15. Política Predeterminada 36
Figura 16. Configuración de privacidad 37
Figura 17. Ubicación Estática 37
Figura 18. Informes de usuarios y grupos 38
Figura 19. Conector de Autenticación 38
Figura 20. Configuración de cuenta de servicio 39
Figura 21. Configuración de Conector de Autenticación 39
Figura 22. Instalación Completa 40
Figura 23. Arquitectura de WSS 40
Figura 24. Panel de Control 41
Figura 25. Integración WSS a SEP 41
Figura 26. Integración de SEP a WSS 42
Figura 27. Integración Finalizada 42
Figura 28. Directorio Activo 43
Figura 29. Usuarios y grupos 43
Figura 30. Políticas 43
Figura 31. Categorías de Páginas 44
Figura 32. Agregar Política 44
Figura 33. Agregar grupo de usuarios 45
Figura 34. Categorías bloqueadas 45
Figura 35. Veredicto 46
Figura 36. Comportamiento del usuario 46
Figura 37. Uso de ancho de banda 47
Figura 38. Ancho de banda por usuario 47
Figura 39. Costo de ancho de banda 47

Figura 40. Información general de ancho de banda 48
Figura 41. Término de búsqueda..... 48
Figura 42. Solicitudes bloqueadas por sitio 48
Figura 43. Usuarios bloqueados..... 49
Figura 44. Página error..... 49
Figura 45. Cuentas de WSS..... 50
Figura 46. Wireless LAN Controller 50
Figura 47. Resumen de la red 51
Figura 48. Distribución de Access Point..... 51
Figura 49. Access Pont 52
Figura 50. Descripción de Access Point..... 52
Figura 51. WLANs 53
Figura 52. Clientes Conectados 53
Figura 53. Descripción de Clientes Conectados..... 53
Figura 54. Estado de la red 54
Figura 55. Acceso Restringido a Clientes..... 54
Figura 56. Acceso Remoto a Sucursales con LogMein 55
Figura 57. Cuenta de usuario no protegida 55
Figura 58. Página permitida bloqueada..... 56
Figura 59. Aplicaciones visitadas por el usuario..... 56
Figura 60. Resumen de Saturación..... 57
Figura 61. Monitoreo de la Red 57
Figura 62. Servidores y Enlaces..... 57
Figura 63. Creación de grupos en SEP 58
Figura 64. Asignación de equipos a grupos con integración WSS 58
Figura 65. Cuenta de Usuario Protegida 59
Figura 66. Acceso Denegado 59
Figura 67. Solicitudes bloqueadas por sitio 60
Figura 68. Bloquear el acceso a usuarios 60
Figura 69. Reporte de Virus..... 61
Figura 70. Reporte de Spyware..... 61
Figura 71. Costo de ancho de banda por día (solicitudes) 62
Figura 72. Costo de ancho por día (bytes) 62
Figura 73. Proyecto Finalizado..... 63

Índice de Tablas

Tabla 1. Director de Sistemas 30
Tabla 2. Coordinador de Infraestructura y Seguridad Informática 30
Tabla 3. Especialista en Infraestructura, Telefonía y Seguridad Informática ... 30
Tabla 4. Especialista en Infraestructura y Seguridad Informática 31
Tabla 5. Practicante 31
Tabla 6. Usuario y Computadora 33

1. Introducción

En esta sección se dará a conocer las necesidades de la empresa AutoTodo Mexicana, y las propuestas para darle solución.

1.1. Descripción del problema o necesidad

La empresa “AutoTodo Mexicana” ubicada en la Autopista México - Puebla 7532, Plan de Ayala, 72110 Puebla, es una de las principales distribuidoras de refacciones y partes automotrices del estado de Puebla. La cual tiene un departamento de Seguridad informática que se encarga de administrar y monitorear la red en las sucursales que conforman dicha empresa como son: Culiacán, Guadalajara, México Norte, México Sur, Mérida, Monterrey, Villahermosa, Tampico, Toluca, León, Puebla y Corporativo.
La problemática que se encuentra en las sucursales antes mencionadas, es el acceso libre y sin restricciones a usuarios internos y externos de la empresa AutoTodo Mexicana a páginas web de streaming, por lo tanto, se presentan situaciones en las que, sin el consentimiento de los usuarios, se descargan virus maliciosos como malware, spyware y rasomware, afectando el desempeño en los equipos móviles y de escritorio, no obstante, solicitan información confidencial personal y de la empresa. Esto es crítico, ya que el virus puede replicarse en toda la red de las sucursales y puede ocasionar pérdida de información, dañar sistemas de archivos, bloqueos de equipos, alterando el funcionamiento correcto de la empresa y flujo de información.
Por otro lado, al no restringir las páginas web de streaming y maliciosas a los empleados, saturan el ancho de banda, y así mismo obstruyen el envío de información, provocando inestabilidades en la red.

1.2 Justificación

Los ciberataques hoy en día se caracterizan cada vez más por su velocidad, variedad, sofisticación y representan un verdadero desafío para las organizaciones de todos los tamaños. Las ciberamenazas ya no pueden ser simplemente bloqueadas; muchos atacantes persisten en las redes durante semanas o meses antes de actuar.

De acuerdo a las problemáticas antes planteadas se implementará un filtrado web en la empresa AutoTodo Mexicana, esto incluye configuración de consola de Filtrado Web, añadir direcciones IP de los equipos de los usuarios permitiendo o restringiendo el acceso de páginas web de acuerdo a sus actividades a elaborar, limitar el ancho de banda de internet, monitorear el comportamiento de la red en las sucursales de AutoTodo Mexicana como son: Culiacán,

Guadalajara, México Norte, México Sur, Mérida, Monterrey, Villahermosa, Tampico, Toluca, León, Puebla y Corporativo. Se considera que la solución es viable debido a que se cuenta con los recursos humanos, materiales y económicos necesarios para llevar a cabo el proyecto. El departamento de Seguridad Informática cuenta con la infraestructura completa de red LAN (red de área local) y WAN (red de área amplia), Router ASA (dispositivo de seguridad adaptable), convenio con Symantec Web Security Service (WSS), empresa líder en ciberseguridad que proporciona dicho servicio.

Con la solución propuesta se podrá administrar los accesos a los usuarios de las sucursales de acuerdo al perfil de trabajo de cada uno de ellos y así mismo restringir las páginas de streaming, maliciosas o no permitidas, limitando el ancho de banda de internet y evitando pérdida de información confidencial.

1.3 Objetivo General y Específicos

Implementar un Filtrado Web para equipos móviles en Corporativo y Sucursales ATM para gestionar y monitorear el acceso a páginas no permitidas y maliciosas, logrando una mejor calidad de servicio de internet.

Objetivos Específicos:

- Crear perfiles de filtrado en los equipos móviles
- Configurar consola de Filtrado Web
- Permitir o restringir direcciones IP y direcciones MAC de acuerdo al perfil de trabajo
- Limitar el ancho de banda de internet
- Gestionar y monitorear el acceso a internet de los usuarios
- Probar y verificar que el Filtrado Web permita o restringa el acceso a internet.

2. Metodología y herramientas

En esta sección se dará a conocer la metodología y herramientas a utilizar para la implementación de proyecto.

2.1 Metodología PVHA para la Gestión de la Seguridad Informática

La metodología ciclo Deming o PVHA, en un sistema de gestión de seguridad de la información (SGSI), permite establecer, implementar, operar, dar seguimiento, mantener y mejorar el SGSI, garantizando la integridad, disponibilidad y confidencialidad de los datos de una organización.
La metodología que se va a llevar a cabo está basada en las normas ISO/IEC 27001, de acuerdo a las necesidades antes planteadas de la empresa AutoTodo Mexicana. La norma ISO 27001 adopta el ciclo de Deming como metodología, la cual se puede aplicar a todos los procesos que abarca el SGSI. Esta metodología es conocida por sus siglas en inglés PVHA: “Planificar-Hacer-Verificar-Actuar [1].

A continuación, se presentarán la descripción de las etapas que conforman la metodología

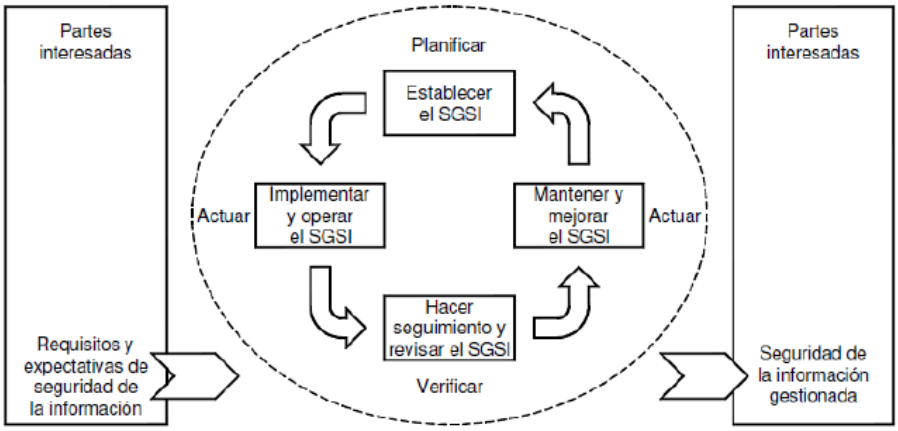


Figura 1. Modelo de PVHA

La figura 1 muestra las etapas que conforman la metodología PVHA para la implementación del proyecto.

Planificar (Establecer el SGSI)
En esta etapa se identifica el problema o actividades susceptibles de mejora, asignación de personas responsables, se definen las políticas de la empresa y los métodos o herramientas para conseguir los objetivos establecidos.

Hacer (Implementar y operar el SGSI)
Esta etapa tiene como objetivo fundamental garantizar una adecuada implementación de los requerimientos recolectados y la correcta aplicación de los mismos.

Verificar (Revisar y dar seguimiento al SGSI)
En esta etapa implica evaluar y, en donde sea aplicable, verificar el desempeño de los procesos contra los objetivos de seguridad, y reportar los resultados a la dirección para su revisión.

Actuar (Mantener y Mejorar el SGSI)
Esta es la etapa final, la cual consiste en revisar, optimizar, o explotar las acciones de mejora. En esta etapa se realizarán acciones correctivas y preventivas basadas en los resultados de la etapa anterior para lograr la mejora continua de SGSI.

2.2 Sistema de Gestión de la Seguridad de la Información

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.
La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información [2]

Confidencialidad

La confidencialidad garantiza la privacidad de los datos mediante la restricción del acceso con el cifrado de la autenticación. La confidencialidad hace referencia a la protección de la información frente a su divulgación a entidades o individuos no autorizados (organizaciones, personas, máquinas, procesos). Nadie debe poder leer los datos a excepción de las entidades específicas previstas.

La confidencialidad es un requisito:

- Cuando se almacenan los datos en un medio (tal como un disco duro de ordenador) al que puede acceder una persona no autorizada.
- Cuando los datos se copian en un dispositivo que puede acabar en manos de una persona no autorizada.
- Cuando los datos se transmiten a través de redes desprotegidas

Integridad de los datos

La integridad garantiza que la información sea precisa y confiable. La integridad de datos es la protección de los datos frente a la modificación, supresión, duplicación o reordenación realizada por entidades no autorizadas (organizaciones, personas, máquinas, procesos). Más concretamente, la integridad se refiere a la fiabilidad de los recursos de información. Una violación de la integridad se debe siempre a un ataque activo.

La integridad de datos es la garantía de la no alteración: se garantiza la detección de cualquier alteración de los datos (ya sea en tránsito por la red o en almacenamiento en un disco duro, por accidente o deliberadamente). La integridad de un sistema de información implica garantizar que no ha habido ninguna corrupción en los datos que han sido transmitidos o almacenados en el sistema, detectando cualquier posible manipulación.

Disponibilidad

La disponibilidad garantiza que la información esté disponible a las personas autorizadas. Mantener los equipos, realizar reparaciones de hardware, mantener los sistemas operativos y el software actualizados, así como crear respaldos, garantiza la disponibilidad de la red y los datos a los usuarios autorizados. Deben existir planes para recuperarse rápidamente ante desastres naturales o provocados por el hombre. Los equipos o software de seguridad, como los firewalls, lo protegen contra el tiempo de inactividad debido a los ataques, como la denegación de servicio (DoS). La denegación de servicio se produce cuando un atacante intenta agotar los recursos de manera tal que los servicios no estén disponibles para los usuarios [3].

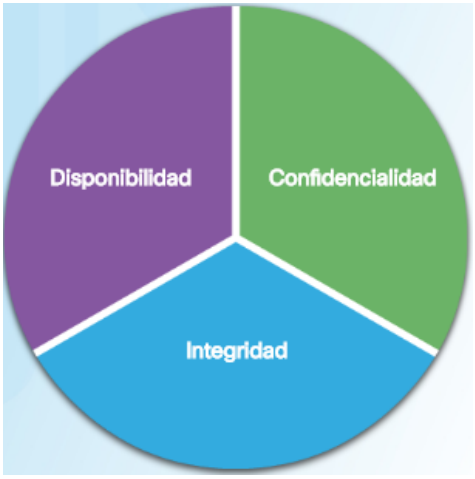


Figura 2. Tríada CID

La figura 2 muestra la confidencialidad, integridad y disponibilidad, conocidas como la tríada CID, es una guía para la seguridad informática de una organización

ISO 270001

ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.
ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013 [4].

Permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

El estándar ISO 27001:2013 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

La aplicación de ISO-27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización.

Figura 3. Estructura de ISO 27001

La evaluación y tratamiento de riesgos da origen a la implementación de medidas de seguridad como muestra la figura 3.

Seguridad

El concepto de seguridad de la información significa proteger la información y los sistemas de información de un acceso, uso, divulgación, alteración, modificación, lectura, inspección, registro o destrucción no autorizados.

La seguridad informática es el nombre genérico para el conjunto de herramientas diseñadas con el fin de proteger los datos almacenados en un equipo y evitar ataques de piratas informáticos [5].

Ciberseguridad

La ciberseguridad es el esfuerzo constante por proteger estos sistemas de red y todos los datos contra el uso no autorizado o los daños. A nivel personal, debe proteger su identidad, sus datos y sus dispositivos informáticos. A nivel corporativo, es responsabilidad de todos proteger la reputación, los datos y los clientes de la organización. A nivel del estado, la seguridad nacional, y la seguridad y el bienestar de los ciudadanos están en juego [6].

Filtrado Web

Se refiere a un programa diseñado para controlar qué contenido se permite mostrar, especialmente para restringir el acceso a ciertos materiales de la Web. Es una solución de software y/o hardware que tiene como finalidad actuar como un intermediario entre los accesos de los colaboradores a internet, posibilitando la aplicación de políticas definidas por la empresa. El filtro de contenido determina qué contenido estará disponible en una máquina o red particular. El motivo suele ser para prevenir a las personas ver contenido que el dueño de la computadora u otras autoridades consideran objetable [7].

Cifrado

Tratamiento de un conjunto de datos, contenidos o no en un paquete, a fin de impedir que nadie excepto el destinatario de los mismos pueda leerlos. Suele emplearse para ello un algoritmo de cifrado y una clave de cifrado [8].

VPN

VPN (Virtual Private Network) Red privada que permite conectar de forma segura a las empresas con otras oficinas de su organización, empleados a distancia, personas con móviles, proveedores [8].

Firewall

Un firewall o cortafuegos es un dispositivo que se utiliza para proteger la red interna de una organización. Esta protección se lleva a cabo mediante la separación de la red interna del mundo exterior, o Internet. Todos los mensajes que entran o salen de la red interna a través del firewall son examinados para verificar si cumplen las normas de seguridad especificadas en las reglas del firewall [16].

Un firewall puede hacer dos cosas. Puede bloquear o permitir una comunicación. Por lo general, se permiten todas las comunicaciones de la red interna a la red externa (Internet), pero si la política de seguridad establece una regla impidiendo el paso de un tipo de mensajes, el firewall lo bloqueará. Por ejemplo, a veces se impiden conexiones a sitios que no sean de confianza ni a otros lugares

considerados una amenaza para la seguridad o inapropiados para la organización.

2.3 Redes Alámbricas

Las redes alámbricas son utilizadas principalmente cuando se necesita mover grandes cantidades de datos a altas velocidades, como medios multimedia de calidad profesional. Se comunica a través de cables de datos (generalmente basada en Ethernet. Los cables de datos, conocidos como cables de red de Ethernet o cables con hilos conductores (CAT5), conectan computadoras y otros dispositivos que forman las redes. [9]

2.4 Redes Inalámbricas

Las redes inalámbricas (Wireless networks, WLAN) gozan actualmente de gran popularidad ya que permiten la movilidad de los usuarios y de los equipos dentro del área de cobertura de la red. Estas redes permiten la conexión a Internet en casi todas partes y ofrecen servicios de comunicación de voz y datos. Las comunicaciones inalámbricas presentan grandes posibilidades, pero también suponen un alto riesgo de seguridad derivados de la facilidad de acceso a la señal radio en el rango de cobertura de red inalámbrica. Por eso, la seguridad en las conexiones inalámbricas son un tema de gran actualidad [10].

La seguridad en WLAN implica las siguientes tareas:

- Garantizar la confidencialidad o cifrado del contenido de la comunicación,
- Autenticación de usuario o control de acceso a la red.

Access Point

Los puntos de acceso, también llamados APs o wireless access point, son equipos hardware configurados en redes Wifi y que hacen de intermediario entre el ordenador y la red externa (local o Internet). El access point o punto de acceso, hace de transmisor central y receptor de las señales de radio en una red Wireless.

Los Access Point son dispositivos que permiten la conexión de un dispositivo móvil de cómputo (computadora, tableta, smartphone) con una red. Los APs tienen asignadas direcciones IP, para poder ser configurados.

Ancho de Banda

Es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado. El ancho de banda se indica generalmente en bites por segundo (BPS), kilobytes por segundo (kbps), o megabytes por segundo (mps). El ancho de banda denota la capacidad de transmisión de una conexión y es un factor importante al determinar la calidad y la velocidad de una red.

Seguridad en Redes Inalámbricas

La seguridad en redes inalámbricas exige estos servicios:

- Autenticación,
- Confidencialidad,

Autenticación

Proceso mediante el cual se comprueba la identidad de un usuario o un equipo en la red. La autenticación es el proceso mediante el cual los usuarios se asocian a la red inalámbrica (Wireless LAN, WLAN). Así pues, sólo tras una correcta autenticación se permite la asociación de usuarios a la red [11].

Confidencialidad en redes WLAN

La confidencialidad en las redes WLAN se realiza mediante el uso de algoritmos criptográficos. Los algoritmos más utilizados son RC4 (WEP) y AES (WPA2) [12].

WEP

WEP (Wired Equivalent Privacy) Primer mecanismo de seguridad que se implementó bajo el estándar de redes inalámbricas IEEE 802.11x para codificar los datos que se transfieren a través de una red inalámbrica.

WPA

WPA Estándar desarrollado por la Wi-Fi Alliance, basado en un borrador del estándar IEEE 802.11i, para mejorar el nivel de codificación existente en WEP, así como para incorporar un método de autenticación.

IEEE 802.11i

IEEE 802.11i Estándar del IEEE que define la encriptación y la autenticación para complementar, completar y mejorar la seguridad en redes WLAN proporcionada por WEP.

WPA2

WPA2 Implementación aprobada por Wi-Fi Alliance interoperable con IEEE 802.11i. El grupo WPA2 de la Wi-Fi Alliance es el grupo de certificación del estándar IEEE 802.11, para lo cual se basa en las condiciones obligatorias del estándar.

IEEE 802.1x

IEEE 802.1x Estándar de nivel 2 para el control de acceso a red. Mediante el empleo de puertos ofrece un marco para una autenticación superior (basada en una pareja identificador de usuario y contraseña o certificados digitales) y distribución de claves de cifrado.

EAP

EAP (Extensible Authentication Protocol) Protocolo de autenticación para llevar a cabo tareas de AAA que define las credenciales necesarias para la autenticación de usuarios. En redes WLAN es utilizado junto con el protocolo IEEE 802.1x en la negociación de la conexión entre el punto de acceso y el usuario de la red WLAN.

Protocolos

Un protocolo es un método establecido de intercambiar datos en Internet. Un protocolo es un método por el cual dos ordenadores acuerdan comunicarse, una especificación que describe cómo los ordenadores hablan el uno al otro en una red. El protocolo determina lo siguiente [13]:

- El tipo de comprobación de errores que se utilizará.
- Cómo indicará el dispositivo que envía que ha acabado el enviar un mensaje.
- Cómo indicará el dispositivo que recibe que ha recibido un mensaje.

Protocolo HTTP

HTTP o Hypertext Transfer Protocol es un protocolo usado en la world wide web sin estado ya que cada uno de sus comandos se ejecutan de forma independiente no guarda información sobre sesiones o comandos ejecutados anteriormente por tanto el uso de cookies que permite almacenar en el servidor la información del cliente [14].

Protocolo HTTPS

HTTPS (Hypertext Transfer Protocol Secure), como su nombre lo dice es un protocolo de aplicación en el cual se implementa el protocolo HTTP (Hypertext Transfer Protocol) con seguridad. A nivel mundial está comenzando una migración desde el protocolo HTTP a HTTPS, esto tiene que ver con la seguridad con la que los usuarios de las distintas páginas web puedan tener confianza en el lugar donde dejan sus datos.

2.5 Ataques

Un ataque es el término que se utiliza para describir un programa escrito para aprovecharse de una vulnerabilidad conocida. El acto de aprovecharse de una vulnerabilidad se conoce como ataque. El objetivo del ataque es acceder a un sistema, los datos que aloja o recursos específicos.

Ataques Pasivos

Un ataque pasivo es aquél en que el atacante monitoriza el canal de comunicación sin modificar ni añadir datos. Un atacante pasivo sólo pone en

peligro la confidencialidad de los datos. El objetivo del atacante es obtener la información que se está transmitiendo [15].

Los ataques pasivos están relacionados con el contenido del mensaje y con el análisis de tráfico:

- **Espionaje:** En general, la mayoría de la información que se transmite utilizando una red de comunicaciones se envía de forma no segura (sin cifrar) permitiendo a un atacante "escuchar" o interpretar (leer) los datos intercambiados. Uno de los mayores problemas a los que se enfrenta un administrador de una red deriva de la capacidad de un atacante para monitorizarla. Sin servicios de cifrado (basados en el uso de técnicas criptográficas), los datos pueden ser leídos por otras personas a medida que circulan por la red.

- **Análisis de tráfico:** Se refiere al proceso de interceptar y examinar los mensajes con el fin de deducir información de patrones en la comunicación. Se puede realizar incluso cuando los mensajes están cifrados. En general, cuanto mayor es el número de mensajes observados, interceptados y almacenados, más se puede inferir del tráfico. El análisis de tráfico, entre otras cosas, permite a un atacante verificar que dos entidades están manteniendo una comunicación en un determinado momento.

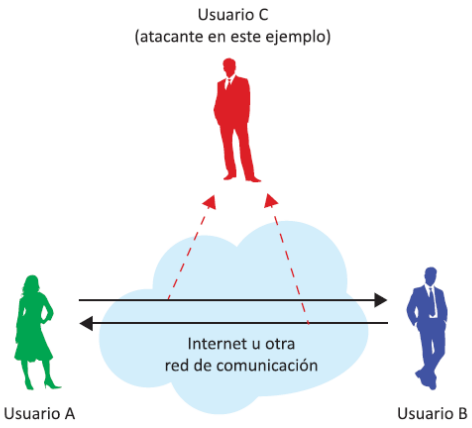


Figura 4. Ataque Pasivo

La figura 4 representa un modelo de ataque pasivo, en donde el atacante analiza la comunicación de los usuarios.

Ataques Activos

Un ataque activo intenta alterar los recursos del sistema o afectar a su funcionamiento. En este tipo de ataque el adversario intenta borrar, añadir, o modificar los datos transmitidos. Un atacante activo amenaza la integridad de datos y autenticación, así como la confidencialidad [15].

Los ataques activos engloban alguna modificación del flujo de datos o la creación de datos falsos. Puede dividirse en seis categorías:

- Suplantación de identidad. Es un tipo de ataque en el que el atacante suplanta la identidad de otro usuario.
- Repetición. En este tipo de ataque, una transmisión de datos válida es repetida o retardada de forma maliciosa. Este ataque lo puede provocar el mismo emisor de datos originales o bien un atacante que los intercepta y posteriormente los retransmite, posiblemente como parte de un ataque de suplantación de identidad.
- Modificación de mensajes. El atacante elimina un mensaje que atraviesa la red, lo altera, y lo reinserta.
- Hombre en el medio (Man in the Middle, MitM). En este tipo de ataques, un atacante intercepta las comunicaciones entre dos entidades, por ejemplo, entre un usuario y un sitio web. El atacante puede utilizar la información que consigue para luego suplantar la identidad del usuario o realizar cualquier otro tipo de fraude.
- Denegación de Servicio (Denial of Service DoS) y Denegación de Servicio Distribuida (Distributed Denial of Service, DDoS). Una denegación de servicio (DoS) es una situación en la que un usuario u organización se ve privado de los servicios o recursos que normalmente debería tener. En denegación de servicio distribuida, un gran número de sistemas comprometidos (a veces llamado botnet) atacan a un solo objetivo.
- Amenazas Avanzadas Persistentes (Advanced Persistent Threat, APT). Es un ataque a la red en el que un atacante consigue un acceso no autorizado a la red y permanece allí sin ser detectado durante un largo período de tiempo. La principal intención de un ataque APT es robar datos más que causar daños a la red u organización. Algunas organizaciones que pueden ser objetivo de ataques APT son sectores con alto valor informativo, como la defensa nacional, la industria financiera [15].

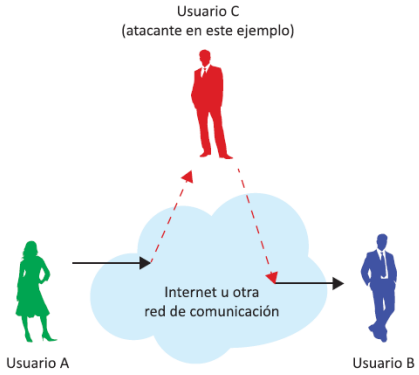


Figura 5. Ataque Activo

La figura 5 muestra un ejemplo de un ataque activo (en concreto, de un ataque de modificación).

Vulnerabilidad

Las vulnerabilidades de seguridad son cualquier tipo de defecto en software o hardware. Después de obtener conocimientos sobre una vulnerabilidad, los usuarios malintencionados intentan explotarla.

Atacantes

Un atacante o intruso es un individuo que obtiene, o trata de obtener, permisos o acceso no autorizado al sistema de información [8].

Desde el punto de vista de la ubicación del atacante, existen dos tipos diferentes

de atacantes:

- Atacante interno
- Atacante externo o intruso

Atacante Interno

Un atacante interno es, en general, una persona que tiene acceso a la red informática interna, y por lo tanto es un usuario legítimo, pero intenta obtener acceso a datos, recursos y servicios del sistema a los que él no debería acceder o bien hacer mal uso de cualquier dato al que esté autorizado.

Atacante Externo

Un intruso o atacante externo es generalmente una persona que no está autorizada a acceder a la red informática interna y desea entrar aprovechando vulnerabilidades del sistema.

Tipos de Atacantes

En la actualidad existen diferentes tipos de atacantes que se mostrarán a continuación.

Aficionados

Se denominan Script Kiddies. Generalmente, son atacantes con poca o ninguna habilidad que, a menudo, utilizan las herramientas existentes o las instrucciones que se encuentran en Internet para llevar a cabo ataques. Algunos de ellos solo son curiosos, mientras que otros intentan demostrar sus habilidades y causar daños. Pueden utilizar herramientas básicas, pero los resultados aún pueden ser devastadores [15].

Hacker

Un Hacker es una persona con excelentes habilidades en informática o telecomunicaciones, muchas veces con experiencia en proyectos importantes de software y cuyo conocimiento es muy útil para encontrar posibles

vulnerabilidades y agujeros de seguridad en los sistemas. La actividad del hacker es útil y provechosa. Incluso hay códigos éticos del comportamiento que debe tener un hacker [16].

Estos atacantes se clasifican como de Sombrero Blanco, Gris o Negro.

- **Sombrero Blanco:** Los atacantes de Sombrero Blanco ingresan a las redes o los sistemas informáticos para descubrir las debilidades para poder mejorar la seguridad de estos sistemas. Estas intrusiones se realizan con el permiso previo y los resultados se informan al propietario.
- **Sombrero Negro:** Los atacantes de Sombrero Negro aprovechan las vulnerabilidades para obtener una ganancia ilegal personal, financiera o política. Los atacantes de Sombrero Gris están en algún lugar entre los atacantes de sombrero blanco y negro.
- **Sombrero Gris:** Los atacantes de Sombrero Gris pueden encontrar una vulnerabilidad en un sistema. Es posible que los hackers de Sombrero Gris informen la vulnerabilidad a los propietarios del sistema si esa acción coincide con su agenda. Algunos hackers de Sombrero Gris publican los hechos sobre la vulnerabilidad en Internet para que otros atacantes puedan sacarles provecho [16].

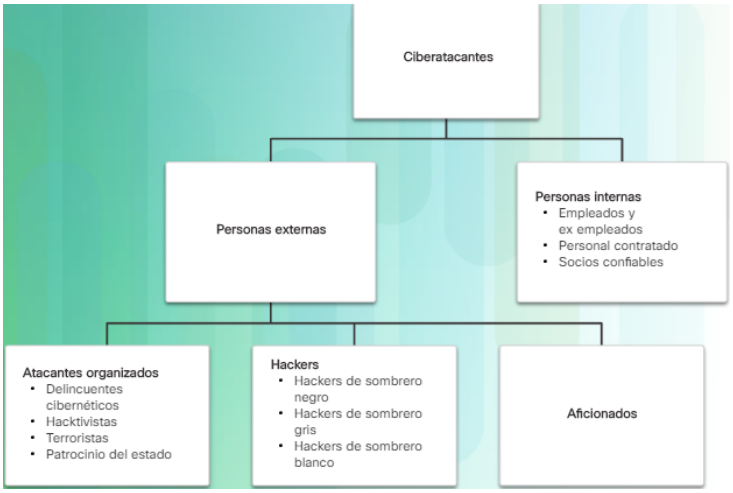


Figura 6. Amenazas internas y externas

La figura 6 muestra los diferentes tipos de ciberatatacantes en una organización.

2.6 Software Malicioso (Malware)

Malware, acrónimo para el inglés “Malicious Software” (Software malicioso), es cualquier código que pueda utilizarse para robar datos, evitar los controles de acceso, ocasionar daños o comprometer un sistema. Hace referencia a cualquier software dañino instalado en un sistema, diseñado para ejecutar instrucciones no deseadas en un ordenador, sin el consentimiento del usuario [17].

La ejecución de malware puede degradar la velocidad de las tareas que un usuario desea realizar en su ordenador y también puede obtener información

crítica u obtener acceso no autorizado a un sistema informático. Malware no es lo mismo que software defectuoso, este último es software que tiene un propósito legítimo, pero contiene errores que no fueron detectados antes de su despliegue.

De hecho, los virus informáticos son en realidad un subconjunto de la familia de malware, donde también se incluyen los gusanos, troyanos, adware, spyware, rasomware, etc.

Una primera clasificación de programas maliciosos se basa en la necesidad de un archivo de host para propagarse. Los siguientes cuatro tipos de software malicioso se corresponden a malware que requieren dicho archivo [18]:

- Puertas trampa (Trap doors)
- Bombas lógicas (Logic bombs)
- Caballos de Troya o troyanos
- Virus.

Puertas Trampa

Son como entradas ocultas en el programa que permiten conseguir el acceso al sistema, evitando los mecanismos de seguridad. Estos mecanismos son utilizados por los programadores durante la depuración de programas para evitar el uso de mecanismos de autenticación y obtener así privilegios especiales. El software malicioso busca estas trampas para evitar los mecanismos de seguridad. Las consecuencias en el sistema informático suelen ser graves.

Bombas Lógicas

Constituyen la clase de software malicioso más antigua. Es un software integrado en un programa legítimo que se activa cuando se dan algunas condiciones. Un ejemplo de estas condiciones puede ser la presencia o ausencia de un archivo específico en días preestablecidos, semana o fecha de inicio de una aplicación determinada… Una bomba lógica puede causar pérdida o daños en el sistema de información, por ejemplo, puede borrar algunos archivos, dejar de ejecutar aplicaciones y así sucesivamente.

Troyanos

Son programas o comandos, que realizan procedimientos o procesos útiles, y al mismo tiempo realizan actividades maliciosas en segundo plano como 28 borrado de datos. Un caso particular es el spyware, un software que captura las contraseñas introducidas a través del teclado, recopila la información sobre las páginas web visitadas, el tipo de software que está utilizando en el equipo, y toda esa información recopilada se envía a través de Internet.

Virus

Son programas capaces de conectarse a otro programa o archivo y pueden ejecutar acciones no autorizadas. Para su propagación es necesario que el archivo host pueda ser modificado por el virus. Los virus pueden atacar a otros archivos, propagarse y corromper sistemas de información [18].

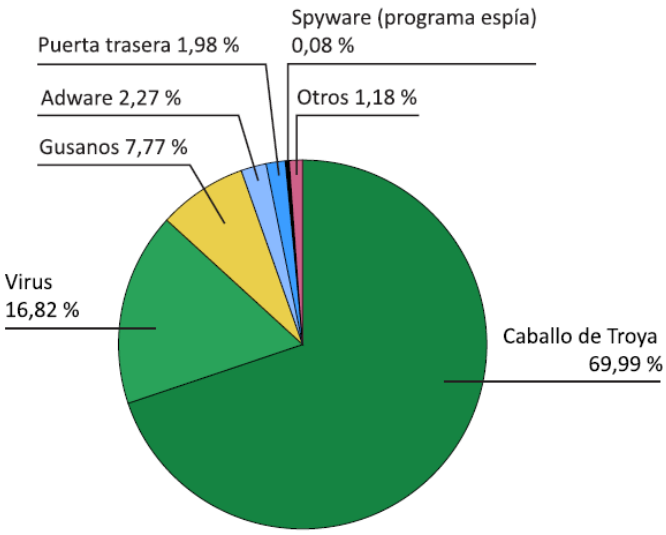


Figura 7. Distribución de Malware por categorías

Las categorías de malware se distribuyen como muestra la figura 7. Cabe mencionar que el caballo de troya es el malware más peligroso.

Hay dos tipos de software malicioso que no necesitan un archivo de host para su propagación:

- Gusanos (Worms),
- Zombies.

Gusanos

Los gusanos son códigos maliciosos que se replican mediante la explotación independiente de las vulnerabilidades en las redes. Los gusanos, por lo general, ralentizan las redes. Mientras que un virus requiere la ejecución de un programa del host, los gusanos pueden ejecutarse por sí mismos. A excepción de la infección inicial, ya no requieren la participación del usuario. Una vez infectado el host, el gusano puede propagarse rápidamente por la red.

Zombi

Un zombi es un software malicioso que se propaga a través de la red. Después de penetrar con éxito en un sistema informático, el ordenador infectado puede ser controlado y administrado remotamente. Cuando varios ordenadores están infectados por el mismo tipo de software malicioso y controlados por un ordenador remoto, se denomina botnet. Este ordenador remoto puede forzar a

los ordenadores infectados a ejecutar las mismas órdenes, dando lugar a los ataques de denegación de servicio distribuido DDoS (Distributed Denial of Service).

2.7 Herramientas

Para realizar el cableado estructurado se utilizaron diferentes tipos de herramientas, las cuales fueron fundamentales y necesarias para llevar a cabo el proyecto. Cabe destacar que el material fue proporcionado por el departamento de Seguridad Informática.

2.7.1 Symantec Endpoint Protection (SEP)

Symantec Endpoint Protection es una solución del servidor de cliente que protege equipos portátiles, equipos de escritorio y servidores en su red contra el software malicioso, los riesgos y las vulnerabilidades. Symantec Endpoint Protection combina protección contra virus con protección contra amenazas avanzada para proteger proactivamente sus equipos contra amenazas conocidas y desconocidas, como virus, gusanos, troyanos y publicidad no deseada. Symantec Endpoint Protection proporciona protección contra los ataques más sofisticados que evaden las medidas de seguridad tradicionales, como rootkits, ataques de día cero y spyware que se transforma [19].

Al permitir bajo mantenimiento y alto desempeño, Symantec Endpoint Protection se comunica por medio de la red para proteger automáticamente los equipos contra ataques de sistemas virtuales y físicos. Symantec Endpoint Protection proporciona soluciones de administración que son eficientes y fáciles de implementar y usar.

Ventajas

- Protege el equipo de los virus.
- Permite instalar el antivirus y conectarse al servidor sin el consentimiento del usuario.
- Proporciona información del equipo

Desventajas

- Debe ser monitoreado para ver el estado del equipo
- Instalar actualizaciones constantemente

2.7.2 Symantec Web Security Service (WSS)

Este servicio de seguridad de la red a través de la nube aplica protección integral para Internet y políticas de cumplimiento de datos, independientemente de la ubicación o del dispositivo que se utilice. Symantec Web Security Service (WSS) es una línea de defensa indispensable contra las ciberamenazas modernas.

Ofrece servicios web seguros y permite a las empresas controlar el acceso y proteger a los usuarios y los datos confidenciales contra las amenazas [20].

Ventajas

- Filtrado de URL y categorización
- Autenticación de usuario
- Protección avanzada contra amenazas
- Conectividad universal
- Análisis de Malware

Desventajas

- Se necesita pagar licencias
- Conexión con SEP

2.7.3 WLC

WLC es un dispositivo que asume un papel central en la CUWN. El WLC realiza los roles tradicionales de los puntos de acceso, como la asociación o autenticación de clientes inalámbricos. Los puntos de acceso, llamados Lightweight Access Points (LAP) en el entorno unificado, se registran con un WLC y canalizan todos los paquetes de administración y datos a los WLC, que luego cambian los paquetes entre clientes inalámbricos y la parte cableada de la red. Todas las configuraciones se realizan en el WLC. Los LAP descargan la configuración completa de los WLC y actúan como una interfaz inalámbrica para los clientes [21].

Ventajas

- Gestiona la red de la empresa
- Control total de los dispositivos conectados a la red
- Permite visualizar las aplicaciones y páginas visitadas de los usuarios
- Muestra la información de los dispositivos conectados
- Permite añadir o restringir el acceso a los dispositivos a la red

Desventajas

- Debe ser monitoreado constantemente
- Mantenimiento cada 6 meses
- Es costoso

2.7.4 Logmein

LogMeIn Hamachi es un servicio de redes virtuales que se instala en unos minutos y permite acceder remotamente y con seguridad a la red de su empresa, desde cualquier lugar que disponga de conexión a Internet.

A diferencia de los sistemas VPN tradicionales basados en hardware y software, Hamachi es un servicio de redes virtuales bajo demanda que le permite concentrar su tiempo y energía en proporcionar a sus usuarios las conexiones remotas que necesitan, y no en la tecnología o infraestructura que utiliza para ofrecerles soporte [22].

Ventajas

- Permite conectarse remotamente sin la autorización y consentimiento del usuario
- Muestra toda la información de la máquina del usuario
- Administra los recursos de la máquina

Desventajas

- Los equipos deben de tener instalado el programa
- Se necesita pagar licencia

2.7.5 PingInfoView

PingInfoView es una herramienta que le permite hacer ping fácilmente a múltiples nombres de host y direcciones IP, y ver el resultado en una tabla. Hace ping automáticamente a todos los hosts cada número de segundos que especifique, y muestra el número de pings exitosos y fallidos, así como el tiempo promedio de ping. También puede guardar el resultado del ping en el archivo de texto / html / xml, o copiarlo al portapapeles [23].

Ventajas

- Permitir a los usuarios de redes informáticas tanto experimentados como novatos monitorear y solucionar problemas de redes.
- Descubre la configuración básica de su red
- Muestra el estado actual de la red
- Es fácil de utilizar y es gratuito

Desventajas

- Se debe añadir las direcciones a monitorear

2.7.6 KeePass

Es un gestor de contraseñas multiplataforma, open source y cifrado. Lo que hace Keepass es almacenar las contraseñas de manera segura para que no tengas que recordarlas. Lo hace en forma de pares: usuario-contraseña, para un control óptimo de este tipo de sesiones. Con una contraseña maestra puedes acceder a la aplicación, generar los ficheros cifrados con tus contraseñas, guardarlos en un directorio compartido o enviarlas por email si lo necesitas [24].

Ventajas

- **Organización.** Cada contraseña en su sitio. Tus cuentas de correo en un grupo, las de *shopping* en otro, las redes sociales en el suyo…
- **Seguridad**. Todo lo introducido en la base de datos se encripta bajo un potente algoritmo, así que es bastante más seguro que guardarlo en un fichero de texto plano, una hoja de cálculo o una hoja de papel.
- **Genera contraseñas de manera automática**. Así es, él solo se encarga de generarte una contraseña tan larga y enrevesada como tú desees.
- **Movilidad**. Puedes tener el archivo con tus contraseñas en tu dispositivo iOS o Android sin problemas, ya que existen versiones de KeePass para más sistemas operativos (también de escritorio).

Desventajas

- No se puede recuperar la contraseña de acceso en caso de olvidarla

2.7.7 Putty

Es un cliente Ssh, Telnet, rlogin, y TCP raw con licencia libre. Disponible para Microsoft Windows, Unix, y se está desarrollando la versión para Mac OS clásico y Mac OS X. Otros desarrolladores han contribuido con versiones no oficiales para otras plataformas, tales como Symbian para teléfonos móviles. Es software beta escrito y mantenido principalmente por Simon Tatham, Open Source y licenciado bajo la Licencia MIT. Se utilizó este programa debido a que la empresa PEMEX lo utiliza para conectar servidores remotamente y poder configurar mediante consola [25].

Ventajas

- Funcionalidad como la reconexión automática al volver del modo suspendido.
- Es de código abierto y se puede descargar gratuitamente.
- Respuestas de puertos
- Soporte Ipv6
- Soporte SCP y SFTP
- Soporte para conexiones de puerto serie local.

Desventajas:

- Actualización de controladores de puertos Polific COM

2.7.8 CMD

Es un programa (cmd.exe) de Microsoft Windows equivalente al programa command.com, intérprete de comandos de MS-DOS (MicroSoft Disk Operating System). Para su ejecución es necesario la inserción de comandos.

Son comandos muy útiles que nos van a permitir acceder a información básica de nuestro equipo para poder, por ejemplo, comunicarnos vía remota o con otros equipos de la red. Se utilizó porque es bastante flexible, viene instalado de manera predeterminada en los dispositivos finales (computadoras) a comparación de otros programas [26].

Ventajas:

- Permite conocer la configuración básica de la red (IP, la máscara de red, puerta de enlace).
- Permite verificar la conectividad de dispositivos que se encuentran en la red.
- Permite visualizar el camino que siguen los paquetes de red desde un equipo a otro y así determinar si existe algún problema en algún momento entre ambos.

Desventajas:

- Solo se puede ejecutar una tarea al mismo tiempo.
- Es monousuario, por lo tanto, solo un usuario a la vez lo puede utilizar.

3. Resultados

En esta sección se dará a conocer los pasos necesarios para implementar el proyecto, añadiendo imágenes y descripciones de cada una de las etapas de la metodología antes planteada.

3.1 Planificar (Establecer el SGSI)

La dirección estableció políticas de seguridad en correspondencia con los objetivos de la entidad y demostró su apoyo y compromiso a la seguridad informática, manteniendo esas políticas en toda a organización, las cuales se comunicaron a todos los usuarios de manera apropiada, accesible y comprensible.

A continuación, se mostrará las políticas definidas de la empresa, las cuales consisten en proporcionar orientación y apoyo de la dirección para la seguridad informática.

3.1.1 Políticas de la empresa

- Los empleados de la empresa Autotodo Mexicana responden por su protección y están en la obligación de informar cualquier incidente o violación que se produzca en su computara a su Jefe inmediato superior.
- Para tener acceso a internet inalámbrica, los empleados deben tener instalado y actualizado el antivirus propio de la empresa en su máquina, en caso contrario se hará caso omiso a la petición.
- Realizar copias de seguridad fiables de toda la información relevante.
- La instalación y desinstalación de software, la configuración lógica, conexión a red, instalación y desinstalación de dispositivos, la manipulación interna y reubicación de equipos de cómputo y periféricos, será realizada únicamente por personal del departamento de Seguridad Informática.
- No se harán descargas de archivos por internet que no provengan de páginas permitidas o relacionadas con las funciones y actividades del perfil de trabajo del empleado.
- El departamento de seguridad informática tiene el derecho de monitorear el contenido al que el usuario puede acceder a través de Internet desde los recursos y servicios de Internet de la empresa y sucursales.
- El correo electrónico empresarial es exclusivo para envío y recepción de mensajes de datos relacionados con las actividades de la empresa AutoTodo Mexicana, no se hará uso de él para fines personales como

registros en redes sociales, registros en sitios web con actividades particulares o comerciales.

- Las contraseñas de acceso deben poseer un mínimo de ocho (8) caracteres y debe contener al menos una letra mayúscula, una letra minúscula, un número y un carácter especial (+-*/@#$%&). No debe contener vocales tildadas, ni eñes, ni espacios.
- La contraseña inicial de acceso a la red que le sea asignada debe ser cambiada la primera vez que acceda al sistema, además, debe ser cambiada cada mes, debido alguna vulnerabilidad en los criterios de seguridad.
- En caso de una violación de una regla o política, se comunicará al Jefe inmediato superior y al departamento de Seguridad informática y se creará una comisión encargada de analizar lo ocurrido y proponer la medida correspondiente.

3.1.2 Organigrama específico

Se dará a conocer el organigrama específico del departamento de Seguridad informática de la empresa AutoTodo Mexicana para la gestión de la Seguridad Informática.

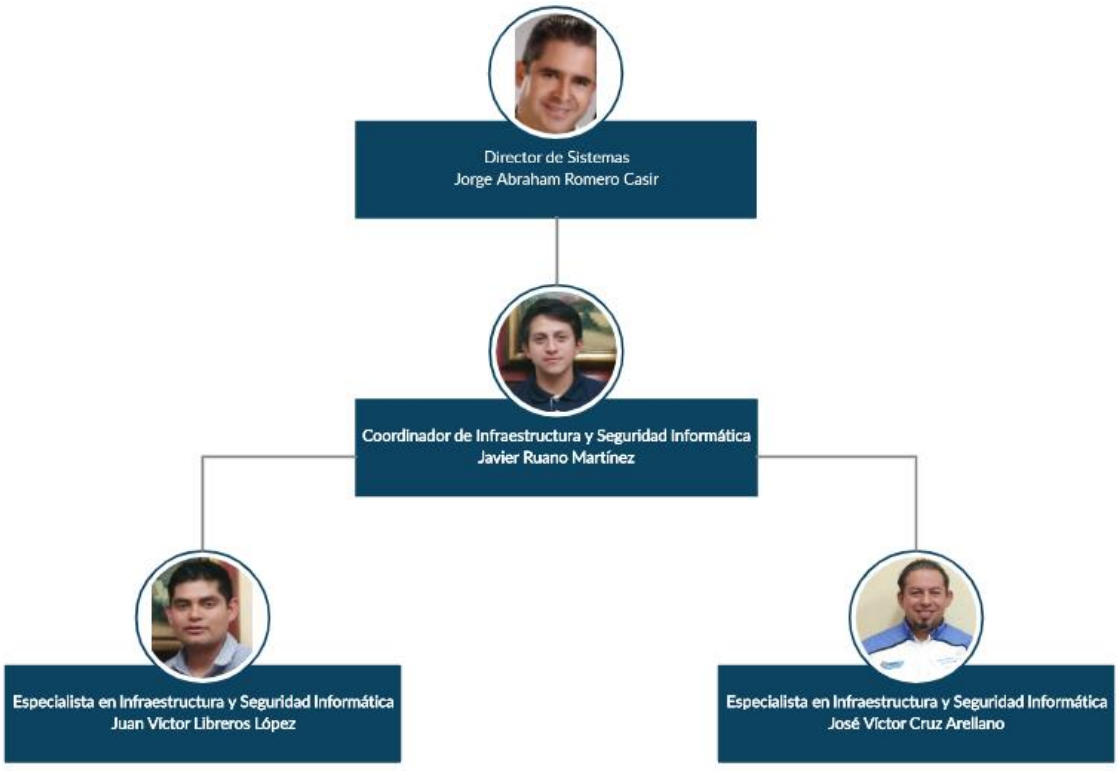


Figura 8. Organigrama

El organigrama específico contiene foto, nombre y cargo de las personas del departamento de seguridad informática como muestra la figura 8.

3.1.3 Responsabilidades

A continuación, se mostrará las actividades que fueron asignadas a cada integrante del equipo para implementar el proyecto de Filtrado Web.

Cargo	Director de Sistemas
Nombre	Jorge Abraham Romero Casir
Actividades	• Convenio con Symantec • Aprobación de implementación de proyecto • Revisión de etapa 4 • Supervisión de las actividades de los integrantes del equipo

Tabla 1. Director de Sistemas

Las actividades que realizó el director de sistemas de la empresa AutoTodo Mexicana se muestran en la tabla 1.

Cargo	Coordinador de Infraestructura y Seguridad Informática
Nombre	Javier Ruano Martínez
Actividades	• Asignación de tareas a participantes del proyecto • Revisión y aprobación de etapa 1 • Revisión y aprobación de etapa 2 • Revisión y aprobación de etapa 3 • Revisión y aprobación de etapa 4 • Apoyo a practicante

Tabla 2. Coordinador de Infraestructura y Seguridad Informática

El ingeniero Javier Ruano Martínez estuvo revisando y apoyando en cada una de las etapas del proyecto como muestra la tabla 2.

Cargo	Especialista en Infraestructura y Seguridad Informática
Nombre	José Víctor Cruz Arellano
Actividades	• Instalación de SEE • Administración de (SEE) • Administración de Altiris • Apoyo a practicante

Tabla 3. Especialista en Infraestructura, Telefonía y Seguridad Informática

El especialista en infraestructura se encargó de la instalación y administración de Symantec Endpoint Encryption como muestra la tabla 3.

Cargo	Especialista en Infraestructura y Seguridad Informática
Nombre	Juan Víctor Libreros López
Actividades	• Instalación de Altiris • Instalación de SEP • Administración de SEP • Desinstalación de CWS • Apoyo a practicante

Tabla 4. Especialista en Infraestructura y Seguridad Informática

El ingeniero Juan Víctor Libreros López se encargó de la instalación de Symantec Endpoint Protrection (SEP) y estuvo apoyando a lo largo del proyecto al practicante como muestra la tabla 4.

Cargo	Practicante
Nombre	Jan Carlos Robles Ortega
Actividades	• Respaldo de nombres, direcciones IP, direcciones MAC de Servidores y computadoras de las Sucursales y Corporativo • Instalación de WSS • Integración de Políticas en WSS • Integración de Políticas en SEP • Crear perfiles de filtrado en los equipos móviles • Implementación de Políticas • Configurar consola de Filtrado Web • Implementación de Políticas en WSS • Realizar pruebas en los equipos móviles • Realizar o explotar acciones de mejora • Gestionar y monitorear el acceso a internet de los usuarios

Tabla 5. Practicante

El practicante Jan Carlos Robles Ortega, estudiante de la Universidad Politécnica de Puebla, efectuó cada una de las actividades que muestra la tabla 5. Cabe mencionar que fue el participante principal del proyecto ya que se encargó de implementar todas las etapas de la Metodología PVHA para la Gestión de la Seguridad Informática.

3.1.4 Análisis de Riesgos

En esta etapa fue importante llevar a cabo un análisis de riesgos para la implementación del proyecto, para evitar fallas o inestabilidades en la red de cada una de las sucursales de la empresa, ya que no pueden perder comunicación los usuarios. Cabe mencionar que se realizó una junta con los participantes del proyecto para poder establecer los bienes informáticos y amenazas más importantes a considerar.

Los bienes informáticos más importantes a proteger son:

- El nombre de computadoras de las Sucursales y Corporativo
- Los nombres de los usuarios de las computadoras
- La red de trabajo interno del Corporativo
- La red en las Sucursales de la empresa
- Acceso a página oficial de People Soft
- Acceso a internet a los contralores y directivos
- Integridad, disponibilidad y confidencialidad de los datos

Las amenazas más importantes a considerar de acuerdo a la implementación del proyecto que pudieran tener sobre la empresa son:

- El acceso a páginas no autorizadas
- Propagación de malware en la red de la empresa
- La sustracción, alteración o pérdida de datos
- El empleo inadecuado de las tecnologías y sus servicios
- Pérdida de integridad, disponibilidad y confidencialidad de los datos
- Falla o inestabilidades en la red

3.1.5 Respaldo de la Información

Las medidas y el procedimiento de respaldo que se implementaron garantizan mantener la integridad y disponibilidad de la información y de las instalaciones de procedimiento de la información frente a cualquier eventualidad.

Cabe mencionar que la base de datos de los servidores no se respaldó, debido a que la información ya no era necesaria para la implementación del proyecto de Filtrado Web, es por ello que se formatearon cada uno de los mismos para que la instalación fuera limpia. Por lo tanto, no se muestra respaldo de base de datos en este apartado.

Para alcanzar un nivel de respaldo adecuado se hicieron las copias de seguridad necesarias para asegurar que toda la información esencial puedan recuperarse tras un desastre o fallo, por lo tanto, se respaldó lo siguiente:

- Respaldo de nombres, direcciones IP, direcciones MAC de Servidores y computadoras de las Sucursales y Corporativo
- Respaldo de nombre de empleados de Sucursales y Corporativo

Computadora	Usuario
MERLAP1FWG262	jose_pech
MERLAP8XPG262	eduardo_garcia
MERLAPC0JG2621	merly_sulub
MERPC440QW52	aracelly_garcia
MERPC442PW52	paulino_balam
MERPC447MW52	edrisi_sansores
MERPC449KW52	factura_digital
MERPC44DJW52	guadalupe_mendoza
MERPC44GJW52	ernesto_burgos
MERPCS1HNC48	elsy_jimenez
MERPCS1X2566	mer_almacen
MERPCS1X2649	laura_gomez
MERPCS44BKW52	jabber
MERPCSMJ02FSE3	hebert_herrera
MERPCSS1001WB3	mer_almacen
MERPCSS1001WBY	mer_almacen
MERLAP923C262	dora_orbe
MERPCMJ0058DV	francisco_padilla

Tabla 6. Usuario y Computadora

Los nombres de usuarios con la computadora asignada se muestran en la tabla 6. Con dicha información podremos filtrar el nombre de usuario u ordenador para aplicarle las políticas necesarias. Cabe mencionar que se registraron 650 computadoras de todas las sucursales de la empresa AutoTodo Mexicana.

Cabe mencionar que se conectó remotamente sin el consentimiento de los usuarios mediante la herramienta LogMein a cada computadora para revisar que ya no estuviera reportándose y conectándose al anterior servidor, y así poder corroborar que los equipos de todas las sucursales estuvieran listos para la etapa 2 de la metodología antes mencionada. Por otro lado, fue de gran importancia el reporte de las computadoras ya que se obtuvo el número exacto de las licencias para computadoras existentes de la empresa.

3.1.6 Amenazas Encontradas

Al no contar con un filtrado web en la empresa AutoTodo Mexicana sin el consentimiento de los usuarios, se descargan virus maliciosos, afectando el desempeño en los equipos móviles y de escritorio y así mismo obstruyen el envío de información, provocando inestabilidades en la red.

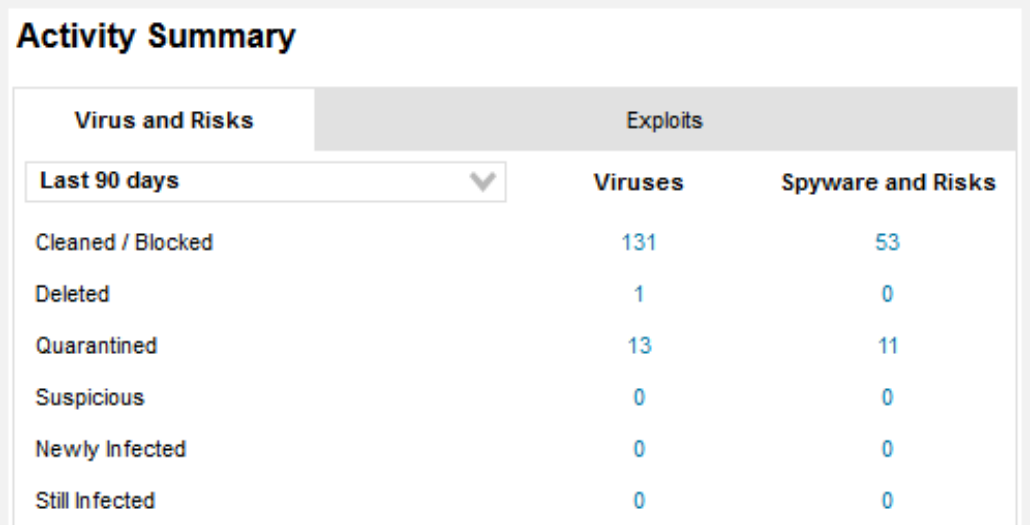


Figura 9. Virus

El administrador de la red, Javier Ruano Martínez se percató de la presencia de virus en la empresa con la herramienta de Symantec Endpoint Protection (SEP) como muestra la figura 9.

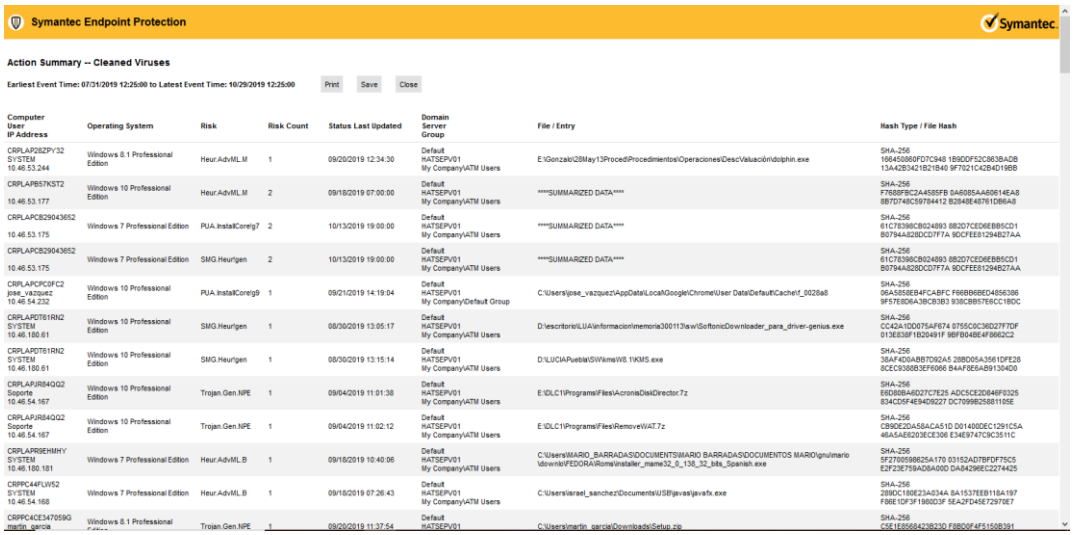


Figura 10. Descripción de Virus

Symantec Endpoint Protection (SEP) identificó cada uno de los virus en las sucursales de AutoTodo Mexicana como muestra la figura 10.

Cabe mencionar que los virus detectados en el antivirus fueron originados por las páginas visitadas por los usuarios y empleados de las sucursales de la empresa AutoTodo Mexicana. Es por ello que el internet presentaba inestabilidades y saturación la red. Por lo que usuarios pertenecientes de la empresa presentaban quejas constantemente al departamento de Seguridad Informática.

File Name / Virus Name	Risk Count	Percentage
	20	90.9
Web Attack : Malvertisement Website Redirect 10	6	27.3
Web Attack: Malicious Domains Request 2	5	22.7
Malicious Site: Malicious Domain Request 21	5	22.7
Malicious Site: Malicious Domain Request 22	4	18.2
	1	4.5
PUA.InstallCore	1	4.5
	1	4.5

Figura 12. Porcentaje de Riesgo

El nombre de los virus y el porcentaje de riesgo de cada uno de ellos se muestran la figura 11.

Figura 11. Saturación de Red

Se identificó saturación en la red del Corporativo, lo cual provoca inestabilidades como muestra la figura 12.

3.1.7 Convenio con Symantec (S21sec)

La empresa AutoTodo Mexicana hizo un convenio por 3 años con la empresa Symantec.

3 Años

SOLUCION INTEGRAL 360 DE PROTECCION AVANZADA - WSS					
Item	SKU	Descripción	Cantidad	Precio Unitario	Precio Extendido
1	CLD-NEW-MOB-250-499-3Y	Cloud Mobility Service, 250 to 499 users, BC 24X7 Support, 3 year Subscription	300	$19.28	$5,782.50
2	CLD-NEW-RPT-3Y	Cloud Reporting Service, BC 24X7 Support, 3 year Subscription	300	$13.50	$4,050.00
3	CLD-NEW-WEB-250-499-3Y	Cloud Web Security Service, 250 to 499 users, BC 24X7 Support, 3 year Subscription	300	$87.90	$26,370.00
4	CLD-SUBSCRIPTION	GENERIC SKU To Identify a Subscription Service for a NEW End-User Customer	1	$0.00	$0.00
5	ADVANCED	Instalación inicial y despliegue de Symantec Web Security Service	1	$2,037.50	$2,037.50

SUBTOTAL	**$38,240.00**
IVA	**$6,118.40**
TOTAL	**$44,358.40**

Figura 13. Costo de Proyecto

Los precios del convenio que se hizo con la empresa Symantec se muestran en la figura 13.

3.2 Hacer (Implementar y operar el SGSI)

En la empresa AutoTodo Mexicana se implementó el filtrado web con Web Security Service

.

A continuación, se mostrará los pasos de instalación:

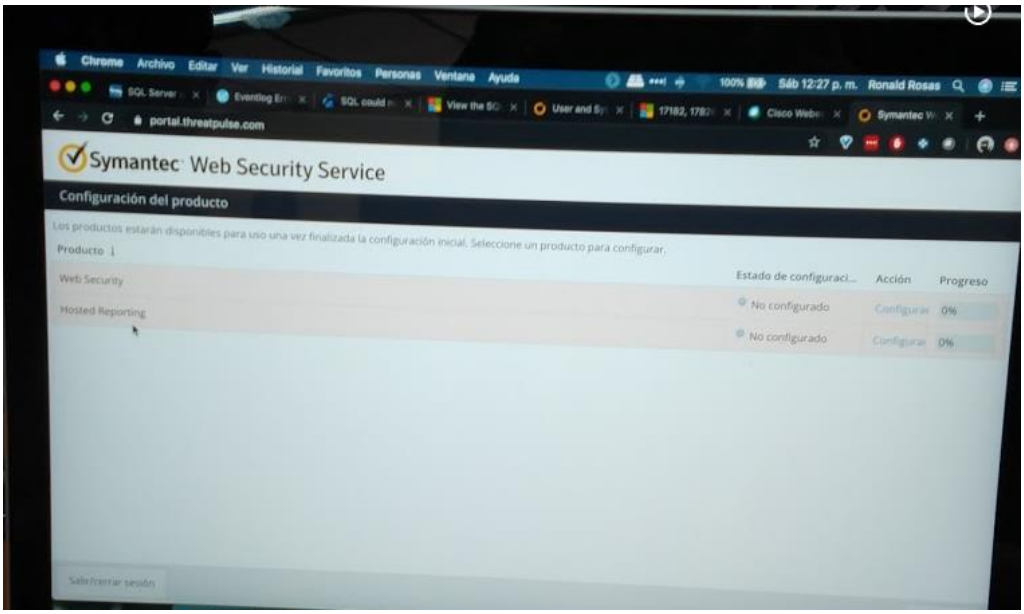


Figura 14. Instalación de WSS

Se instaló Web Security Service de la página oficial de Symantec como muestra la figura 14. Cabe mencionar que estará alojado en la nube, por lo tanto, no se instaló en un servidor.

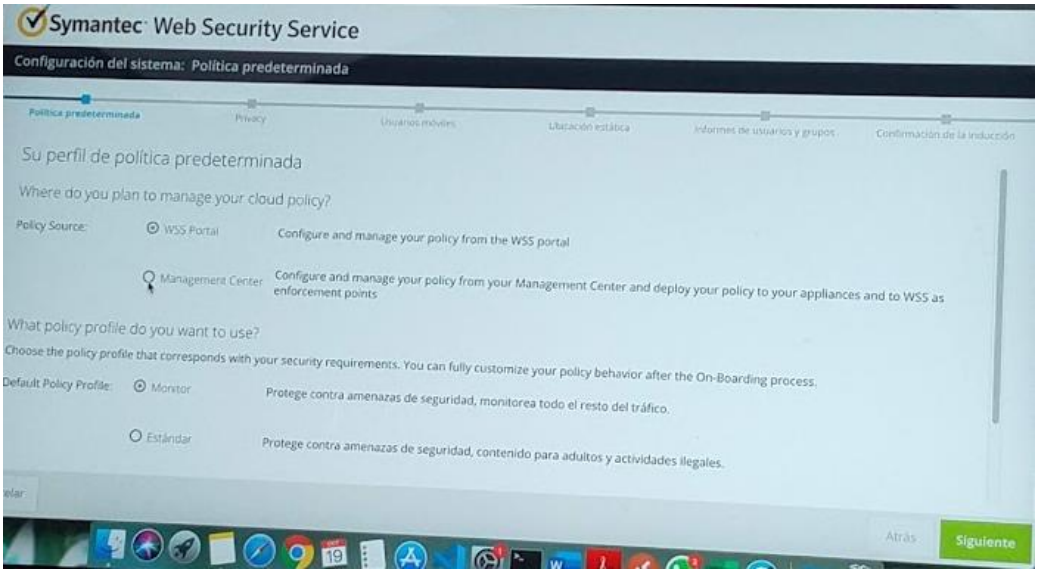


Figura 15. Política Predeterminada

Se configuró la política predeterminada como muestra la figura 15. Se eligió la estándar debido a que protege contra amenazas de seguridad, contenido para adultos y actividades ilegales.

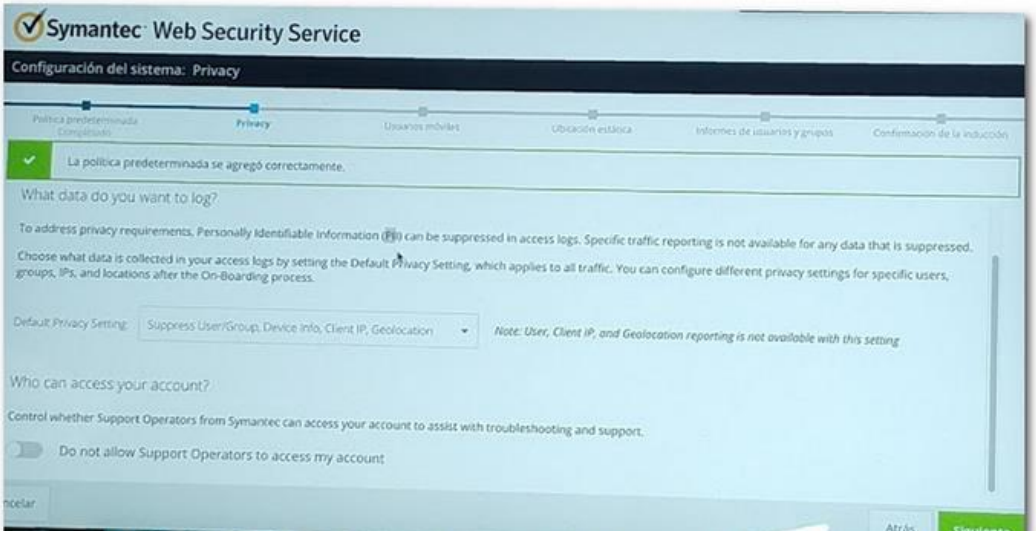


Figura 16. Configuración de privacidad

En la configuración de privacidad se indicó que datos se registrarán de los usuarios, como nombre de la cuenta de usuario o grupo, dirección IP e información del dispositivo conectado como muestra la figura 16.

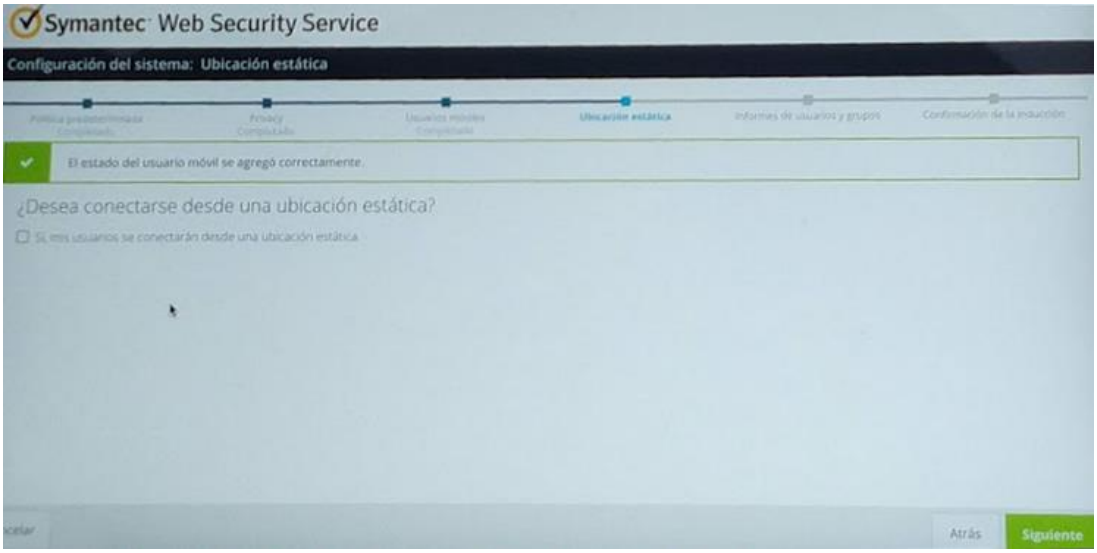


Figura 17. Ubicación Estática

No se configuró una ubicación estática como muestra la figura 17, debido a que los usuarios estarán conectados remotamente.

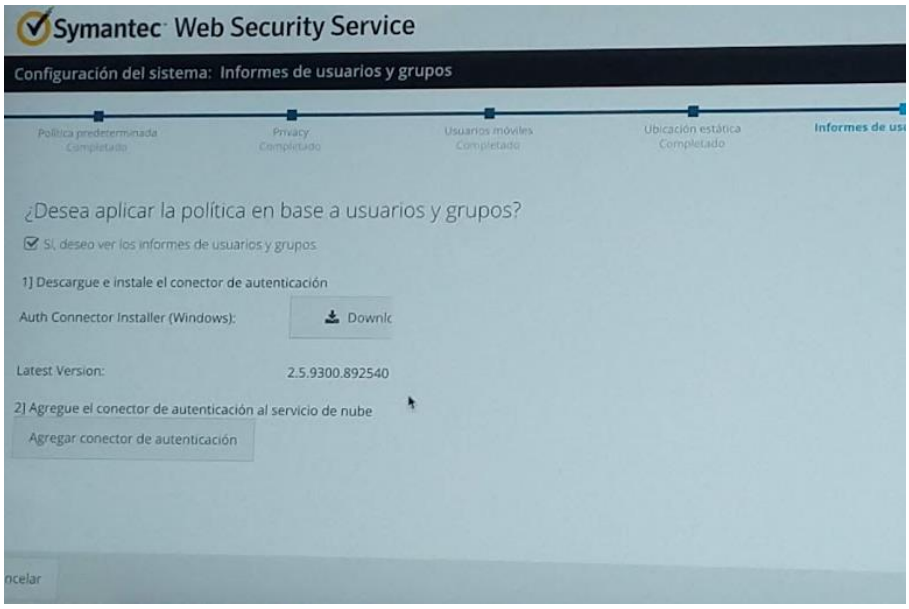


Figura 18. Informes de usuarios y grupos

Se aplicó la política en base a usuarios y grupos como muestra la figura 18, debido a que la licencia estará por cuenta de usuario y no por máquina.

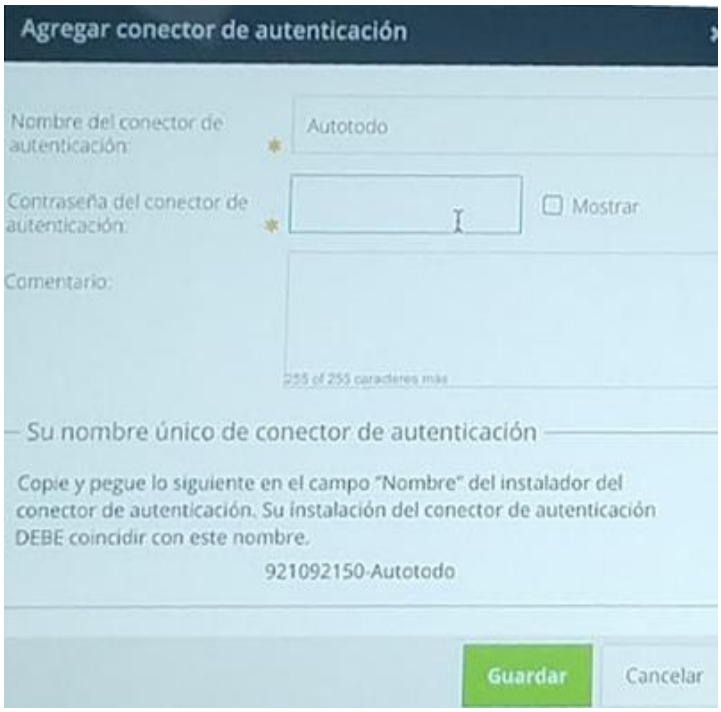


Figura 19. Conector de Autenticación

Se configuró el conector de autenticación en WSS como muestra la figura 19. Es un nombre único el cual se genera automáticamente. Cabe mencionar que no debe modificarse o eliminarse, ya que se tendría que hacer la instalación nuevamente.

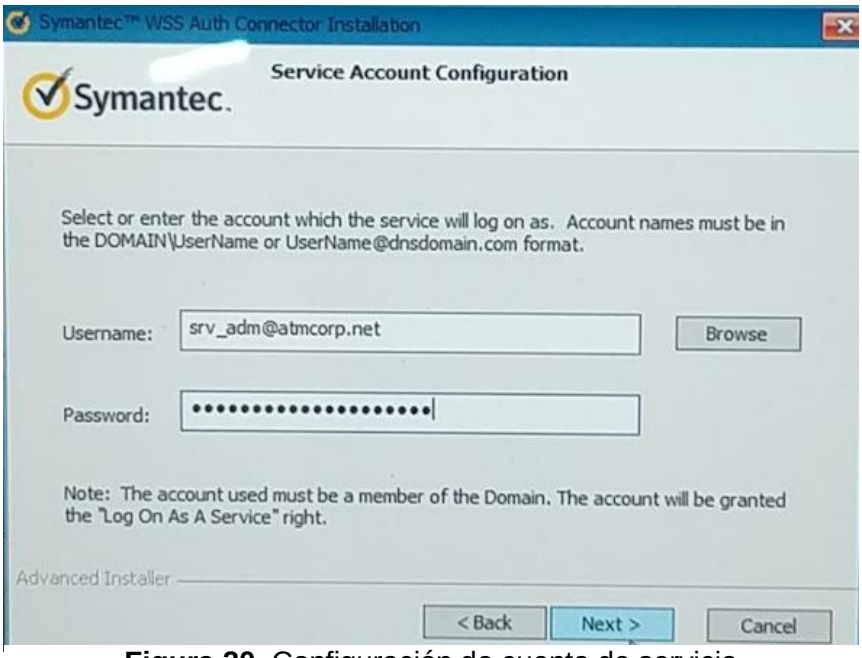


Figura 20. Configuración de cuenta de servicio

Se configuró la cuenta de servicio como muestra la figura 20, en la cual se agregó el nombre de usuario que tendrá todos los privilegios de administración en las máquinas.

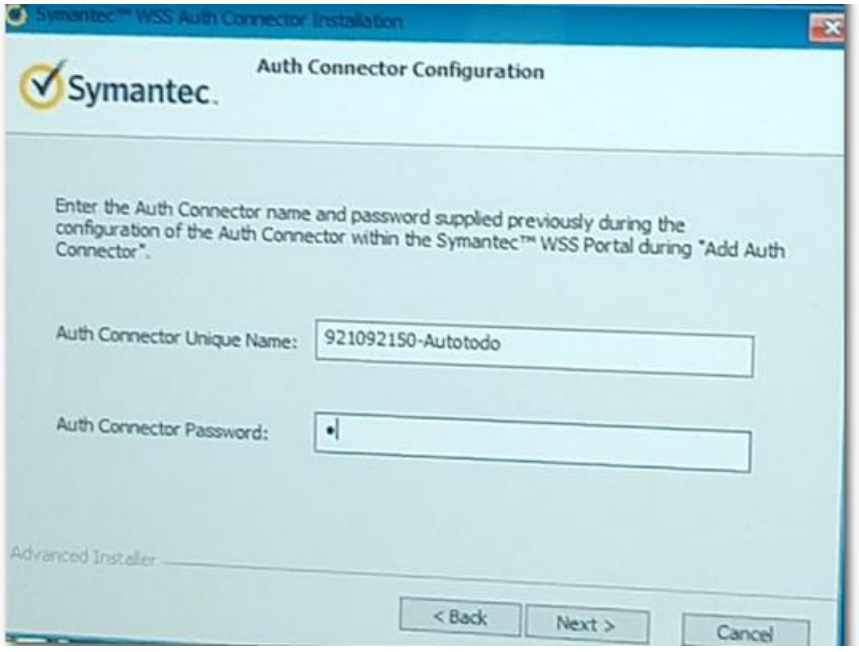


Figura 21. Configuración de Conector de Autenticación

La configuración del conector que se generó anteriormente se le asignó una contraseña para evitar que eliminen dicho conector como muestra la figura 21. Cabe mencionar que no se muestra la contraseña por políticas y seguridad de la empresa AutoTodo Mexicana.

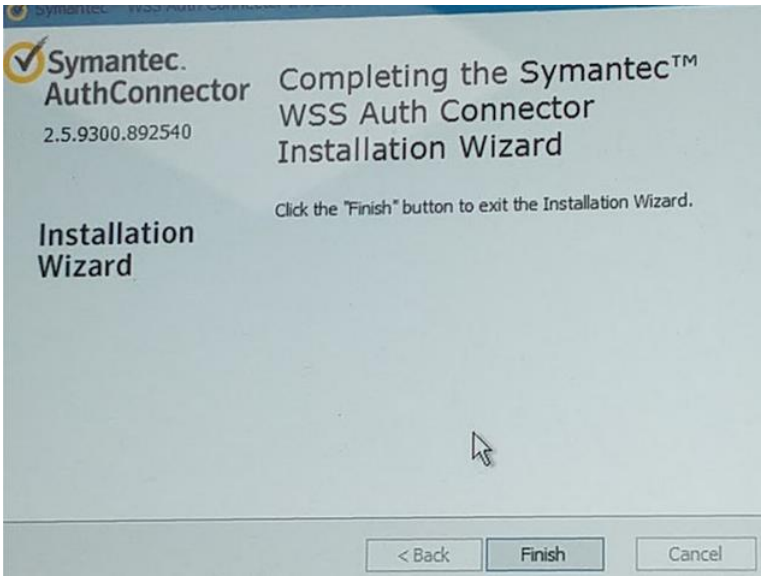


Figura 22. Instalación Completa

La instalación de Web Security Service se completó exitosamente como muestra la figura 22.

Web Security Service (WSS) garantiza acceso granular y políticas de seguridad para administrar el tráfico web y uso del mismo. Consta de las siguientes características:

- Filtrado de URL y categorías
- Autenticación de Usuarios
- Protección avanzada contra amenazas
- Conectividad universal
- Análisis de Malware

La arquitectura de la solución está principalmente en la nube. Donde los servidores de Symantec se encargan de la tarea de analizar y filtrar todo el tráfico web proveniente de los equipos.

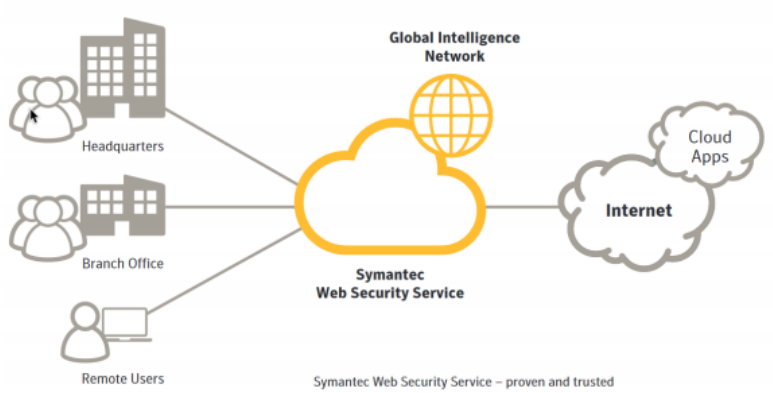


Figura 23. Arquitectura de WSS

La arquitectura de WSS se muestra en la figura 23, el cual estará alojado en la nube y no en un servidor físico.

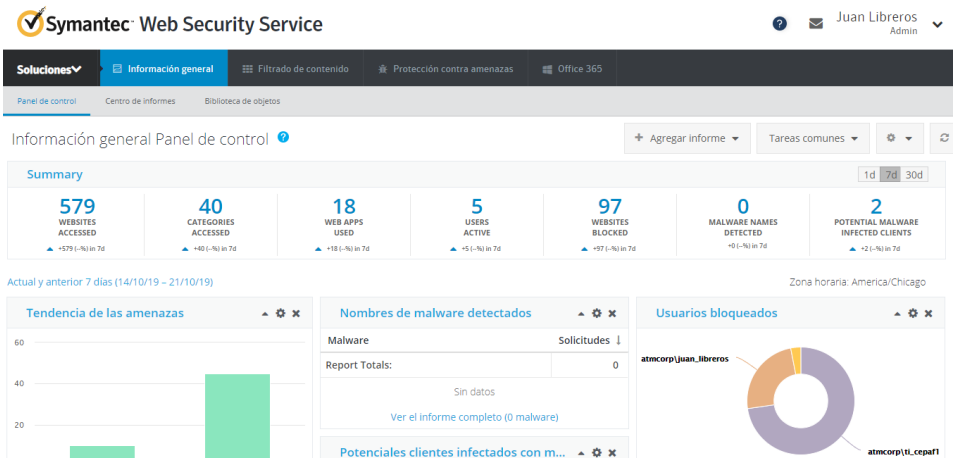


Figura 24. Panel de Control

El panel de control de WSS se muestra en la figura 24, donde se puede visualizar los usuarios activos, sitios bloqueados, páginas web y categorías visitadas, por mencionar algunos.

La empresa Symantec ofreció una sincronización con Symantec Endpoint Protection (SEP), para crear los usuarios de las sucursales y corporativo de la empresa AutoTodo Mexicana. Por lo tanto, en SEP se crearon los grupos de usuarios para sincronizarlo con WSS.

A continuación, se mostrará los pasos que se realizaron para la integración de ambas herramientas:

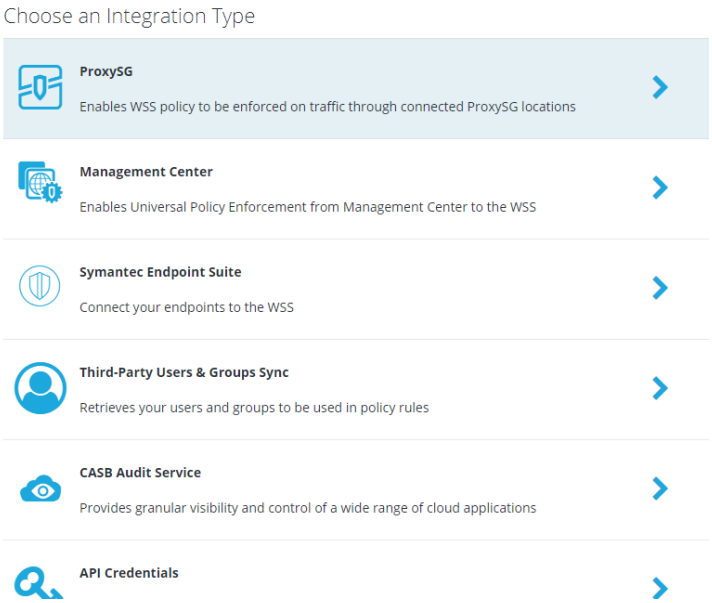


Figura 25. Integración WSS a SEP

Se configuró la integración de WSS a SEP como muestra la figura 25 para sincronizar las herramientas y así poder crear las políticas necesarias a las cuentas de usuario de las sucursales y corporativo de ATM. Se eligió la opción de *Symantec Endpoint Suite.*

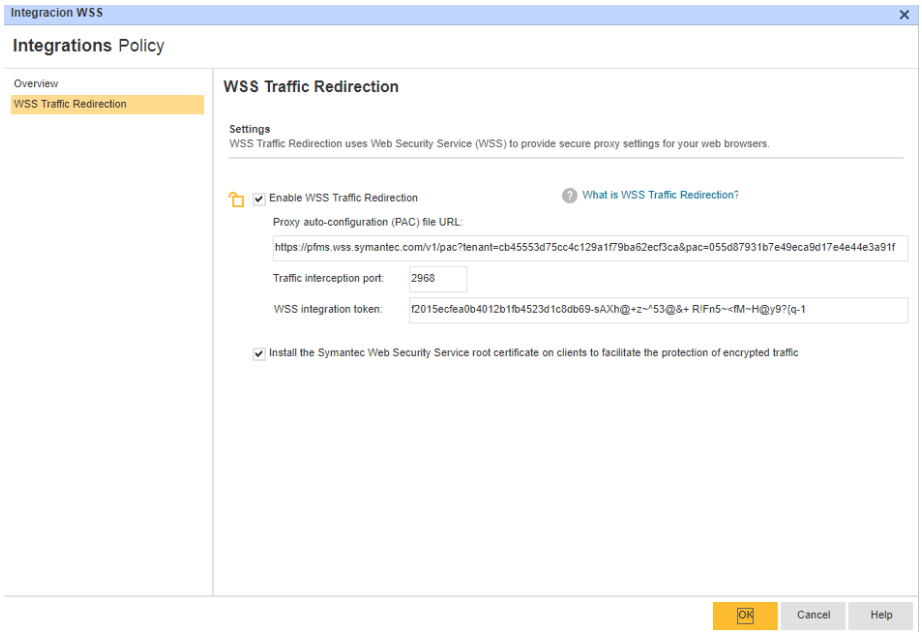


Figura 26. Integración de SEP a WSS

Se configuró la integración de SEP a WSS como muestra la figura 26. Se generó un token el cual redirige el sincroniza las herramientas.

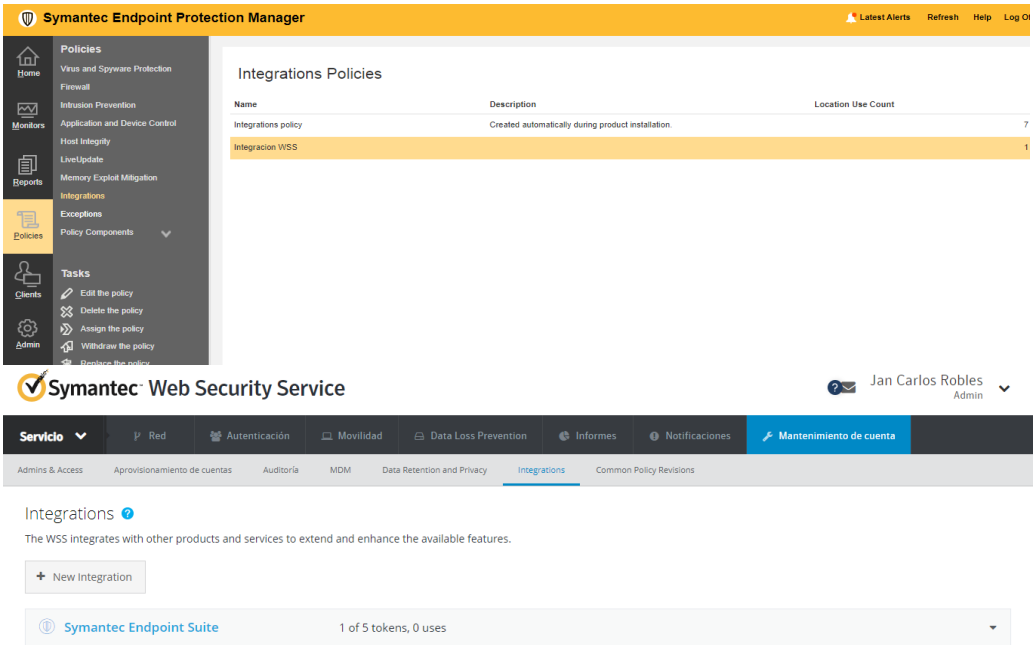


Figura 27. Integración Finalizada

La integración de WSS y en SEP se completó exitosamente como muestra la figura 27. Por lo tanto, ambas herramientas están sincronizadas para poder realizar el Filtrado web.

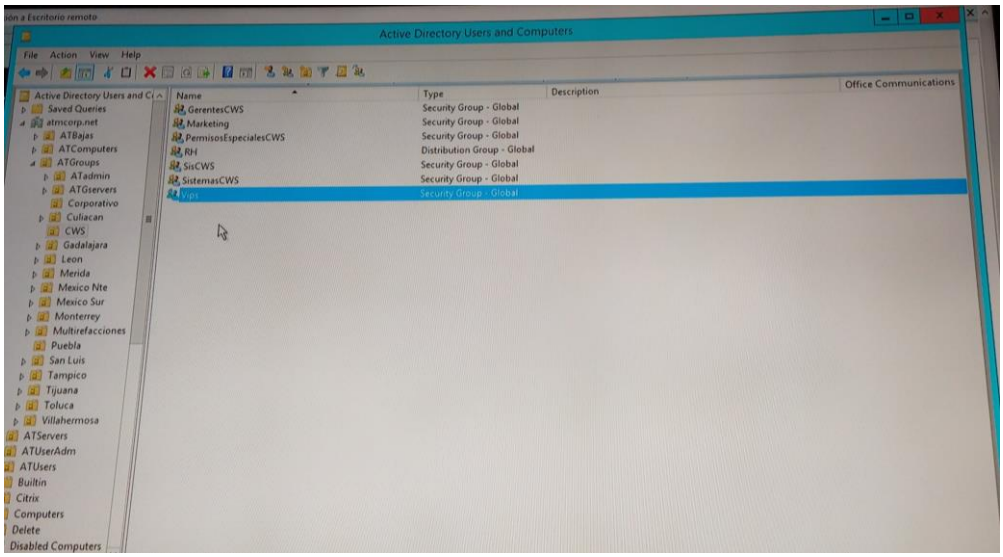


Figura 28. Directorio Activo

Los grupos que se crearon en el directorio activo se muestran en la figura 28 para sincronizarlos con el WSS.

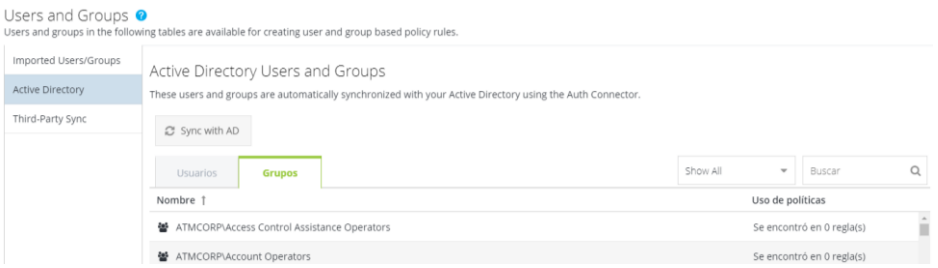


Figura 29. Usuarios y grupos

Después de la sincronización con el directorio activo, WSS conoce los usuarios y grupos de las sucursales y corporativo de la empresa AutoTodo Mexicana como muestra la figura 29.

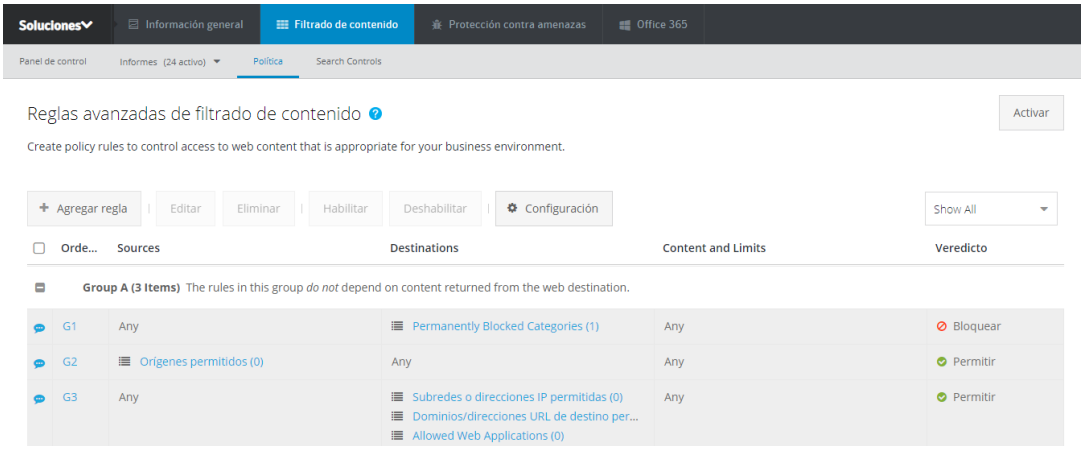


Figura 30. Políticas

Las políticas que se definieron para el acceso a internet de los usuarios según se perfil de trabajo se muestran en la figura 30.

Symantec recomienda las categorías de páginas maliciosas, que puedan saturar y comprometer la red de la empresa AutoTodo Mexicana. Las cuales tomaremos en cuenta según las necesidades de la misma.

A continuación, se muestra las categorías de las páginas recomendadas a bloquear por Symantec:

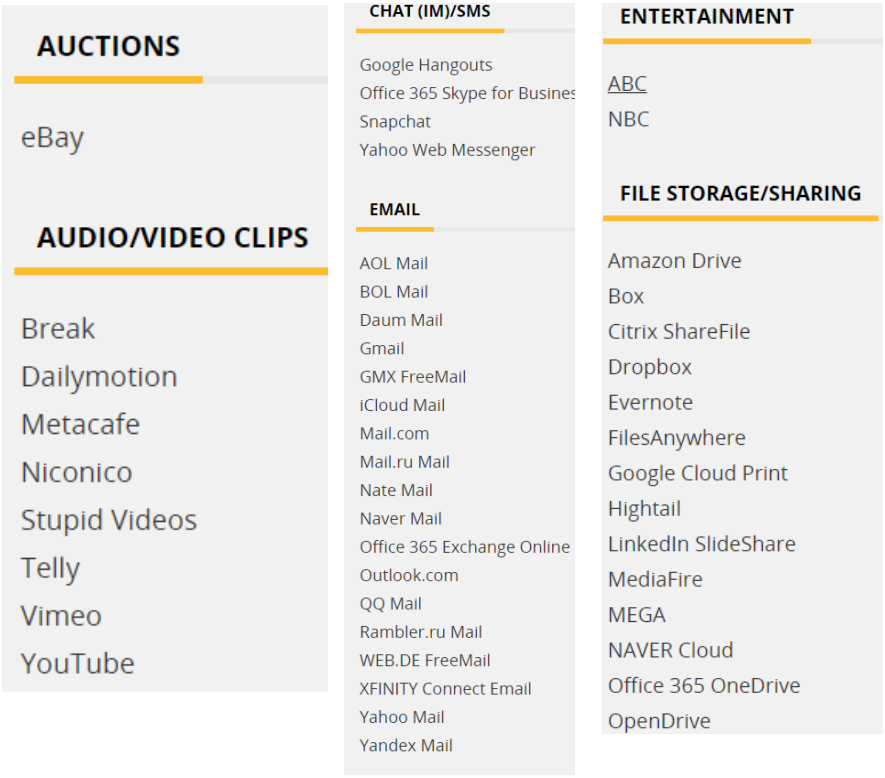


Figura 31. Categorías de Páginas

Las páginas recomendadas a bloquear por la empresa Symantec se muestran en la figura 31.

Se realizó el filtrado web añadiendo las páginas y aplicaciones que no estarán disponibles a los usuarios de la empresa AutoTodo Mexicana, de acuerdo a su perfil de trabajo.

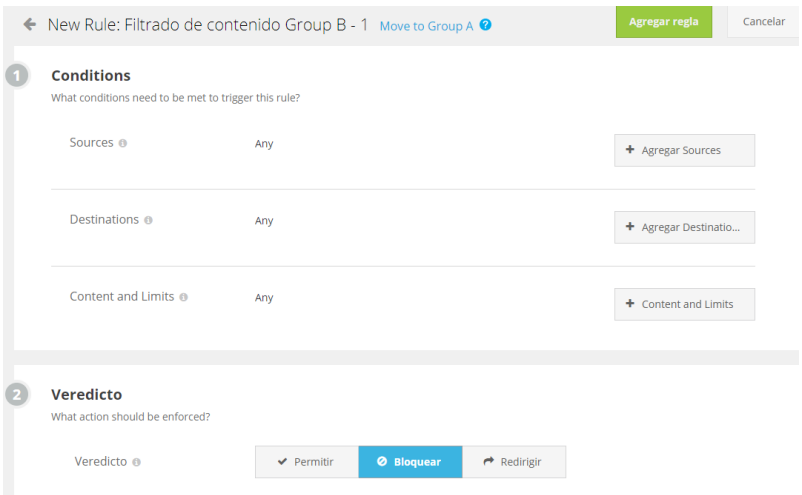


Figura 32. Agregar Política

Las condiciones y el veredicto para realizar el filtrado de contenido se muestran en la figura 32.

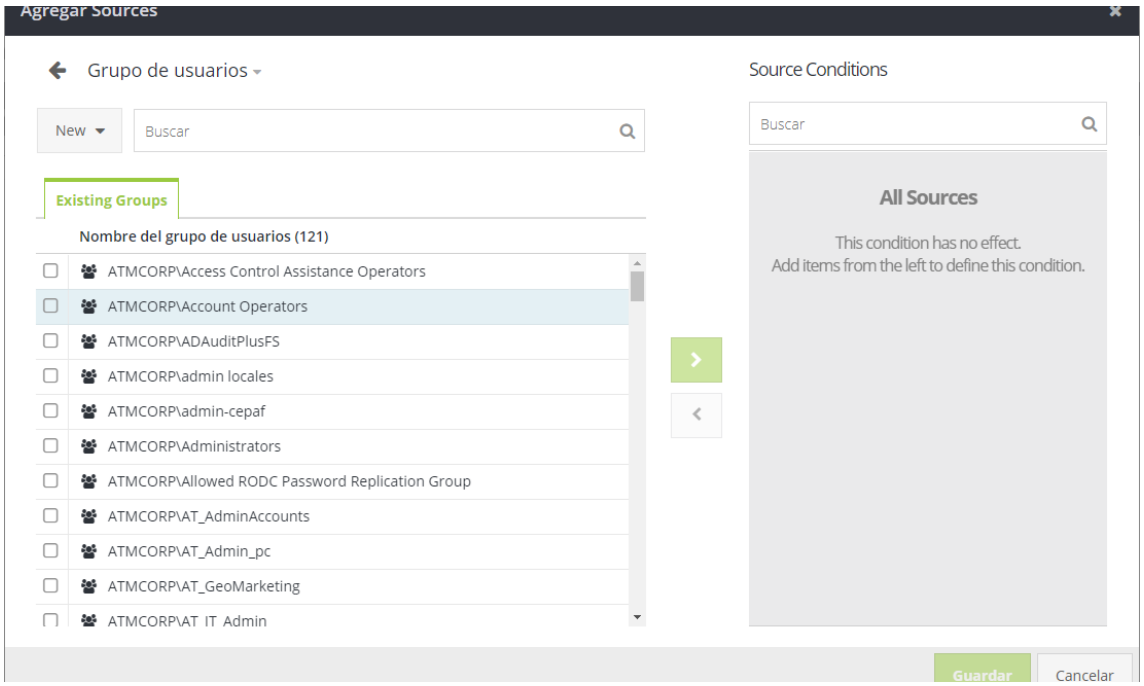


Figura 33. Agregar grupo de usuarios

La agregación de los grupos de usuarios que se permitió o bloqueo el acceso a páginas web se muestran en la figura 33, según sea el caso.

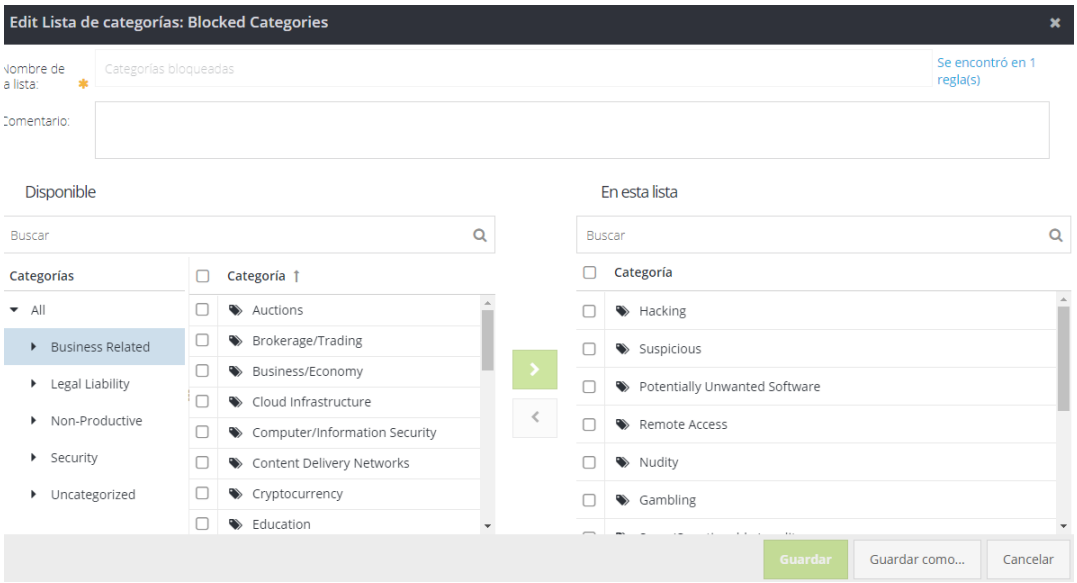


Figura 34. Categorías bloqueadas

Se bloquearon las categorías que estarán restringidas a los usuarios correspondientes de la empresa como muestra la figura 34.

El veredicto facilita 3 tareas:

- Permitir: Los usuarios tienen acceso al contenido (pero otras políticas pueden bloquearlo).
- Bloquear: Acceso denegado, se muestra una página de error al usuario final.
- Bloquear (Anulación de contraseña): Los usuarios finales deben escribir la contraseña asignada para continuar a su destino
- Redirigir: Acceso denegado, el usuario final es redirigido a la URL configurada.

Figura 35. Veredicto

El veredicto que se configuró para los grupos de usuarios antes mencionados se muestra en la figura 35.

De acuerdo a los pasos anteriores, se configuró correctamente el filtrado web en la empresa. Cabe mencionar que se realizó los mismos pasos para el resto de los grupos de usuarios.

Figura 36. Comportamiento del usuario

En el comportamiento del usuario se puede monitorear las solicitudes bloqueadas, exploración web, dirección IP de los usuarios como muestra la figura 36.

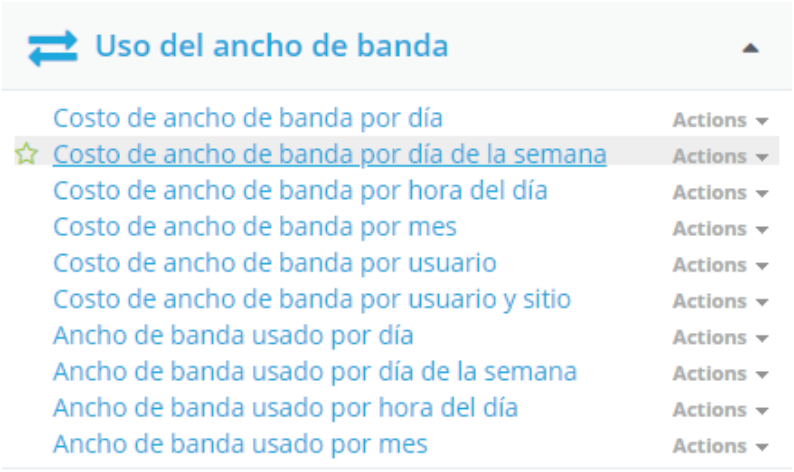


Figura 37. Uso de ancho de banda

El uso de ancho de banda por día, semana y mes de cada uno de los usuarios se muestran en la figura 37. Con ello podemos saber con certeza el ancho de banda que se consume y tomar las medidas correspondientes.

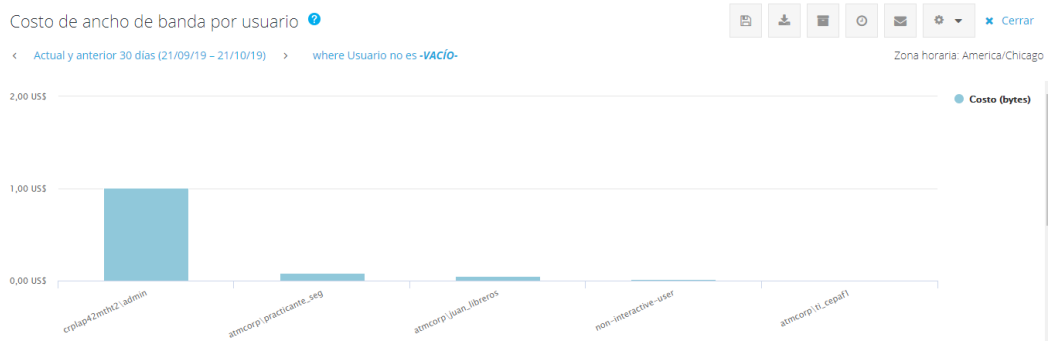


Figura 38. Ancho de banda por usuario

El ancho de banda por usuario se muestra en la figura 38, el costo lo maneja por bytes.

Usuario	Costo (bytes) ↓	Bytes totales	Solicitudes
crplap42mtht2\admin	1,01 US$	2,0 GB	648
atmcorp\practicante_seg	0,08 US$	165,7 MB	9.899
atmcorp\juan_libreros	0,05 US$	101,7 MB	7.360
non-interactive-user	0,02 US$	51,0 MB	3.765
atmcorp\ti_cepaf1	0,01 US$	16,3 MB	827
Report Totals:	**1,17 US$**	**2,3 GB**	**22.499**

Figura 39. Costo de ancho de banda

Además de que el costo lo maneja por bytes, muestra el costo en moneda en dólares como muestra la figura 39, para así saber lo que consume el usuario. Cabe mencionar que el informe puede ser por día, semana y mes.

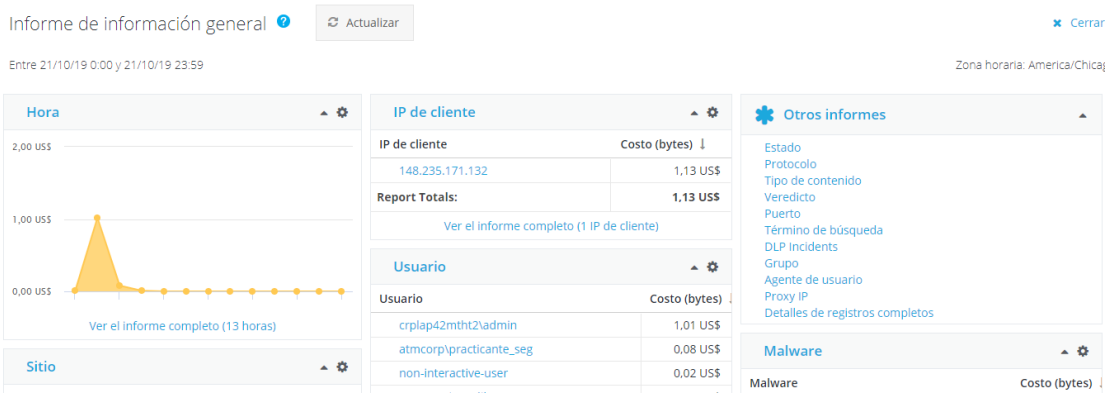


Figura 40. Información general de ancho de banda

Se pude tener un informe general del ancho de banda de un usuario, conociendo su dirección IP, las horas que ha estado conectado y las páginas que ha visitado como muestra la figura 40.

Término de búsqueda	Visualizacio
No Término de búsqueda	55
xxx	2
yst.am	1
actualizacion de windows 10	1
test.threatpulse.com	0
tw	0
p	0
tes	0
t	0
test.	0
Report Totals:	**59**

Figura 41. Término de búsqueda

Se puede monitorear los términos de búsqueda de cada uno de los usuarios conectado a la red como muestra la figura 41. Para así saber si el usuario está intentando entrar a páginas maliciosas o no permitidas.

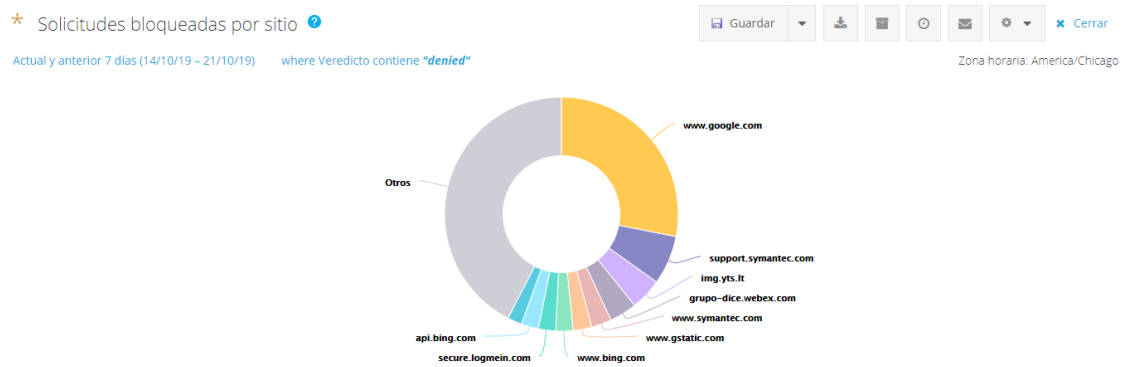


Figura 42. Solicitudes bloqueadas por sitio

Las solicitudes bloqueadas por sitio se muestran en la figura 42, con ello podemos comprobar que el filtrado web se está ejecutando correctamente. Además, se puede tener el informe de los usuarios que intentaron entrar a dichas páginas.

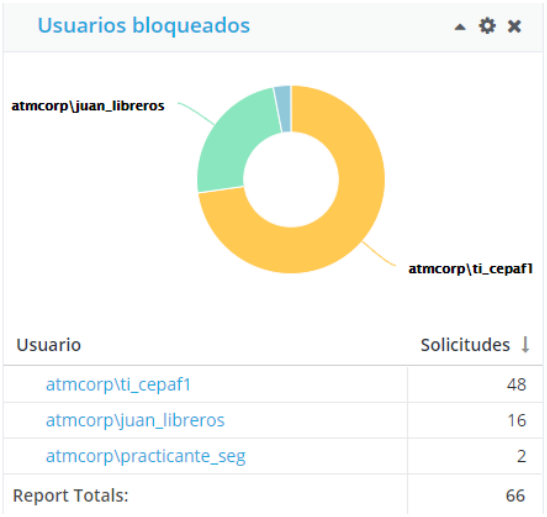


Figura 43. Usuarios bloqueados

Los usuarios que intentaron acceder a páginas maliciosas o no permitidas según las políticas antes definidas, se bloquearon como muestra la figura 43.

En caso de que los usuarios intentarán acceder a páginas maliciosas o no permitidas con el filtrado web, les aparecerá una página de error, notificándole la categoría de la página y restringiendo el acceso.

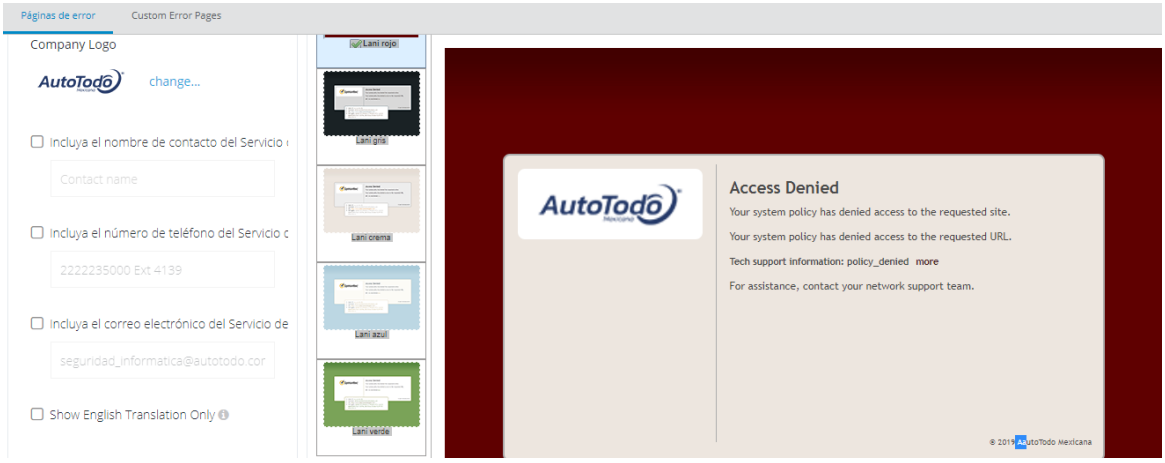


Figura 44. Página error

Se configuró la notificación del acceso restringido como muestra la figura 44. Dicha notificación aparecerá las veces necesarias cuando un usuario intente entrar a una página no permitida. Cabe mencionar que se integró el logotipo oficial de la empresa AutoTodo Mexicana.

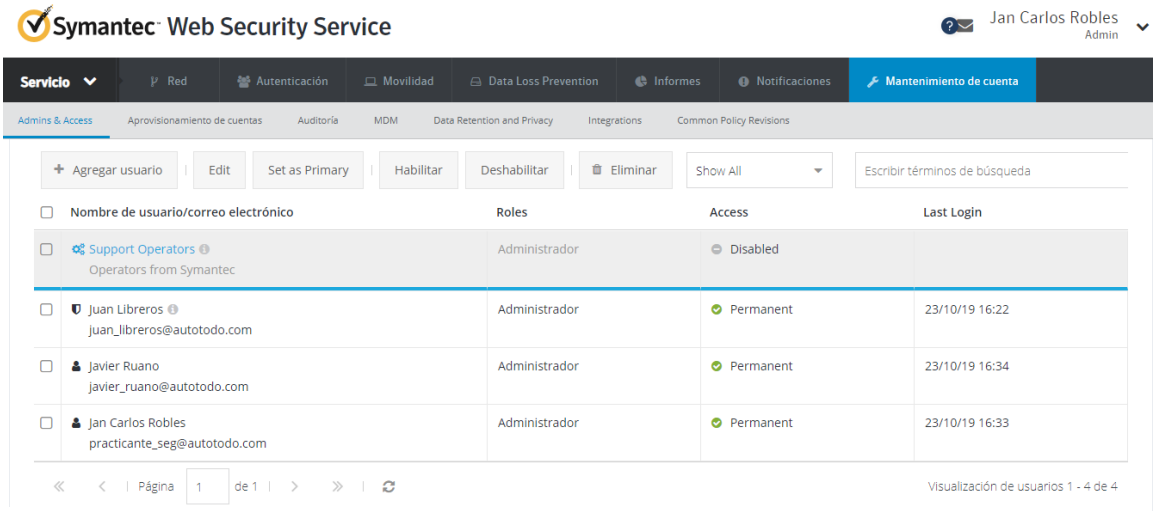


Figura 45. Cuentas de WSS

Se crearon únicamente 3 cuentas de administrador para tener acceso a la herramienta WSS como muestra la figura 45, para así monitorear la red de las sucursales y corporativo de AutoTodo Mexicana.

Por otra parte, se utilizó Wireless LAN Controller (WC) para monitorear la red inalámbrica del corporativo AutoTodo Mexicana. Con dicha herramienta se puede visualizar las aplicaciones y páginas visitadas de los usuarios, muestra la información de los dispositivos conectados y permite añadir o restringir el acceso a los dispositivos a la red

Figura 46. Wireless LAN Controller

El inicio de sesión de Wireless LAN Controller se muestra en la figura 46. Solo personal de sistemas tiene acceso para gestionar y monitorear la red inalámbrica del corporativo.

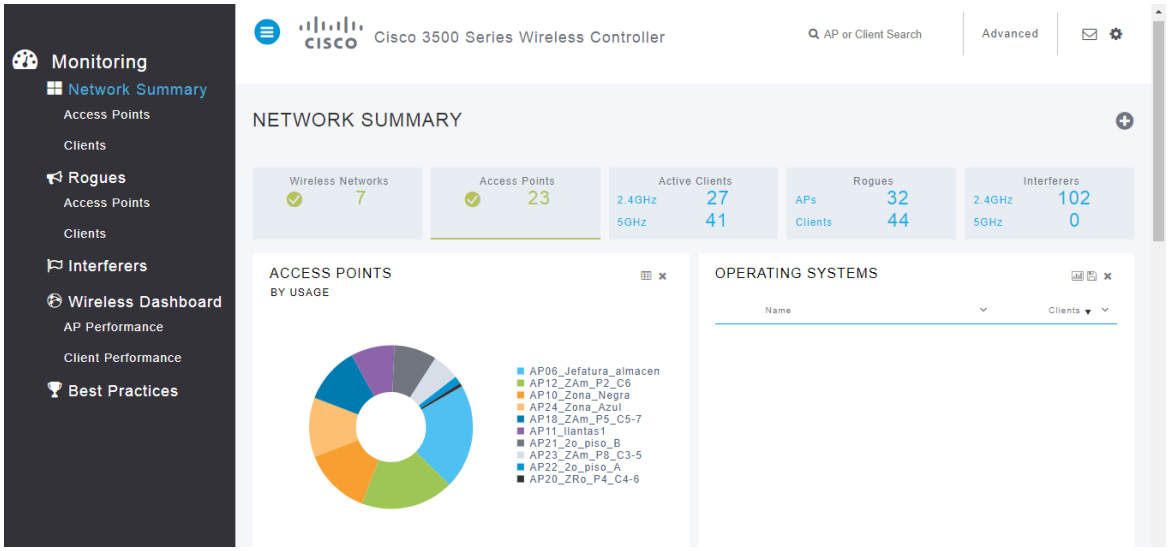


Figura 47. Resumen de la red

En el apartado de resumen de red de WLC se puede visualizar los números de Access Point que existen como muestra la figura 47, en este caso el corporativo de AutoTodo Mexicana tiene 23 Access Point funcionando correctamente, además muestra los clientes conectados a la red inalámbrica.

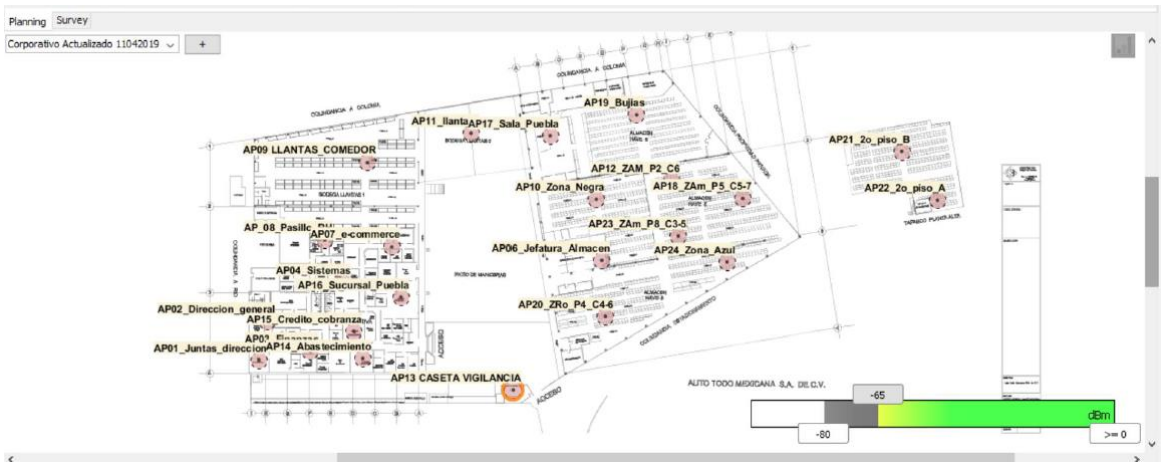


Figura 48. Distribución de Access Point

El diagrama de distribución de los 23 Access Point del corporativo ATM se representa en la figura 48. Cabe mencionar que el proveedor CISCO realizó dicha tarea, por lo que no se muestra datos específicos ni procedimiento de la colocación de cada uno de los AP.

A continuación, se mostrará la descripción de cada uno de los Access Point que se instalaron en la empresa AutoTodo Mexicana y el comportamiento de la red inalámbrica.

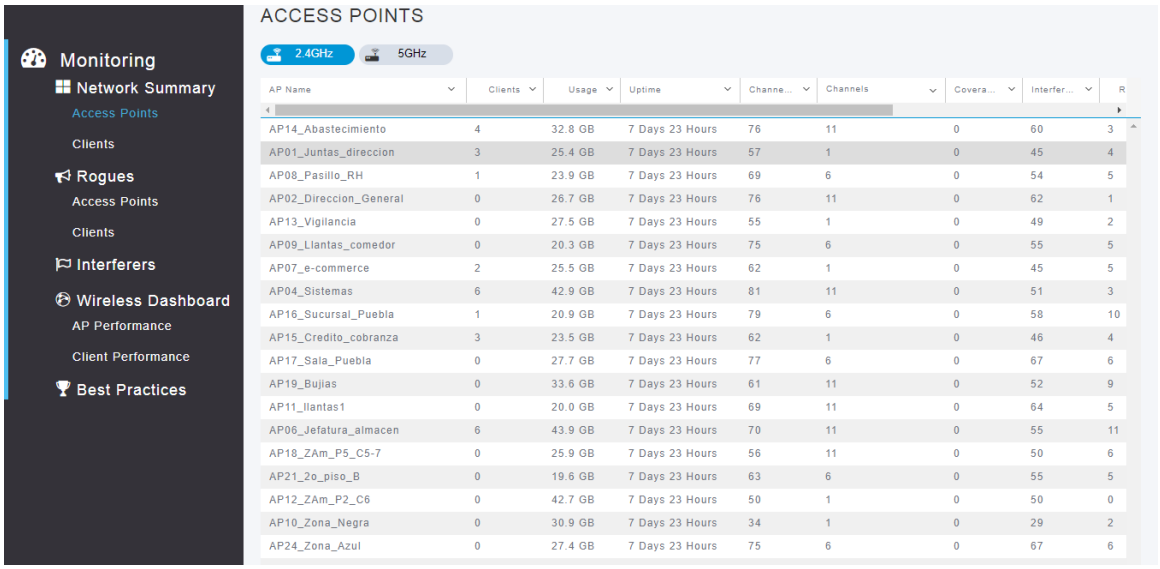


Figura 49. Access Pont

La descripción de cada uno de los Access Point se muestra en la figura 49. Se puede visualizar los números de clientes conectados, el uso en GB, tiempo conectado, por mencionar algunos.

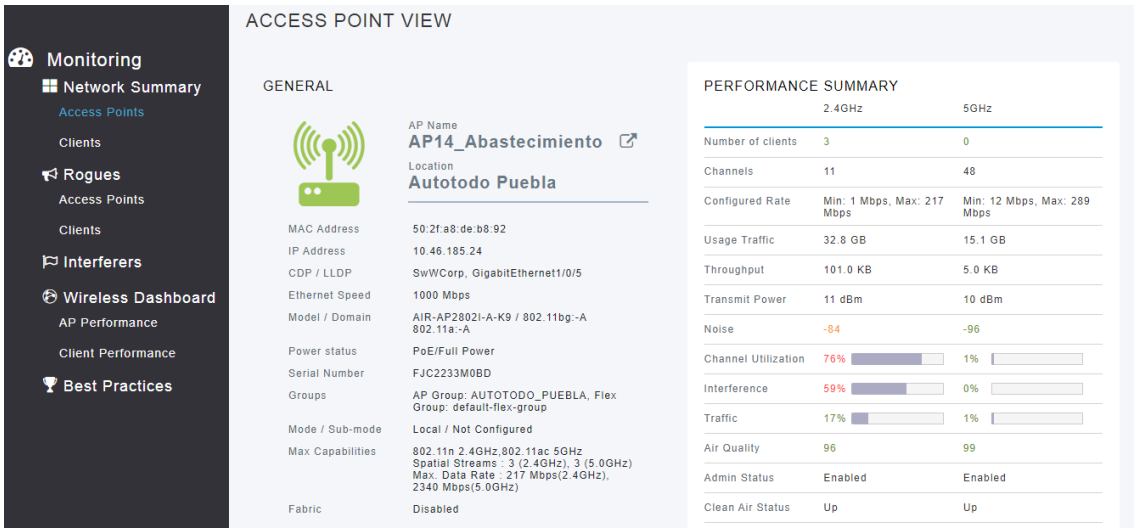
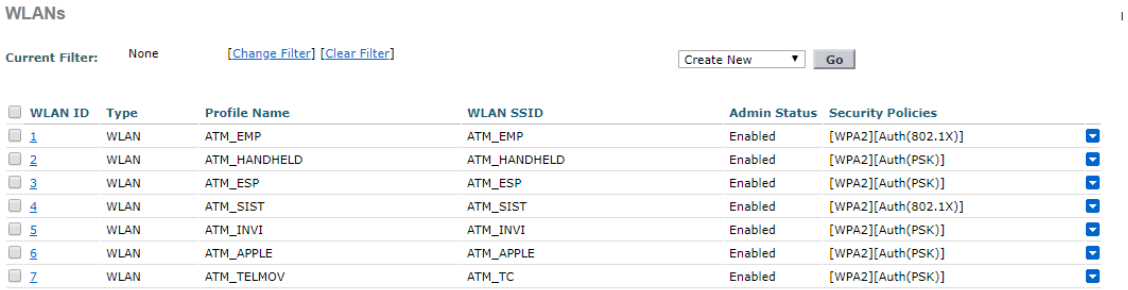


Figura 50. Descripción de Access Point

El resumen del rendimiento del Access Point de Abastecimiento se muestra en la figura 50, como su dirección MAC, dirección IP, número de clientes conectados a la red inalámbrica, ancho de banda, y tráfico de red.

Con ello podemos corroborar que los AP funcionan correctamente ya que les provee salida a internet a los usuarios del corporativo de ATM.



WLANs

Current Filter: None [Change Filter] [Clear Filter] Create New Go

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	ATM_EMP	ATM_EMP	Enabled	[WPA2][Auth(802.1X)]
2	WLAN	ATM_HANDHELD	ATM_HANDHELD	Enabled	[WPA2][Auth(PSK)]
3	WLAN	ATM_ESP	ATM_ESP	Enabled	[WPA2][Auth(PSK)]
4	WLAN	ATM_SIST	ATM_SIST	Enabled	[WPA2][Auth(802.1X)]
5	WLAN	ATM_INVI	ATM_INVI	Enabled	[WPA2][Auth(PSK)]
6	WLAN	ATM_APPLE	ATM_APPLE	Enabled	[WPA2][Auth(PSK)]
7	WLAN	ATM_TELMOV	ATM_TC	Enabled	[WPA2][Auth(PSK)]

Figura 51. WLANs

Las WLANs del corporativo AutoTodo Mexicana se muestran en la figura 51, las cuales darán acceso a internet, cada WLAN es para un grupo específico, lo cual se tendrá una administración de la red adecuada.

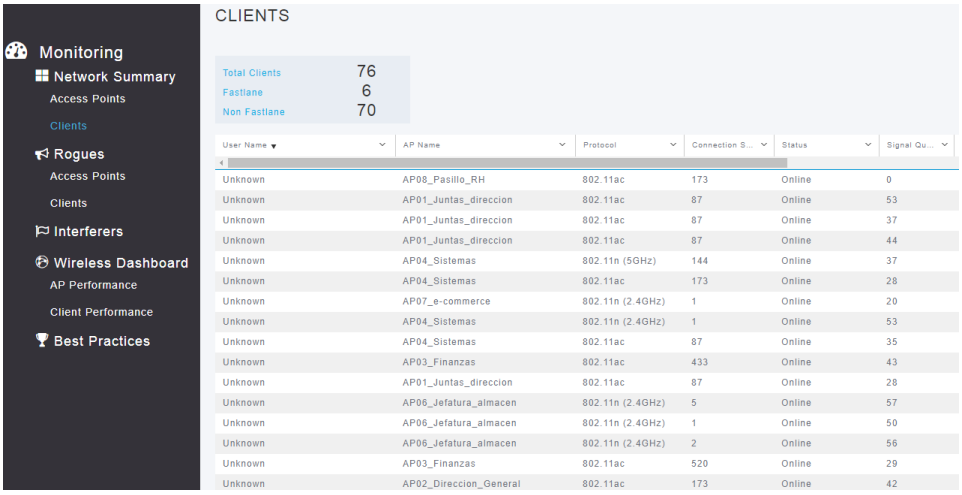


Figura 52. Clientes Conectados

Los clientes conectados a los Access Point del corporativo se muestran en la figura 52. Solamente se ve información general de los clientes, pero al entrar a cada uno de ellos podemos ver información más especifica que a continuación se mostrará.

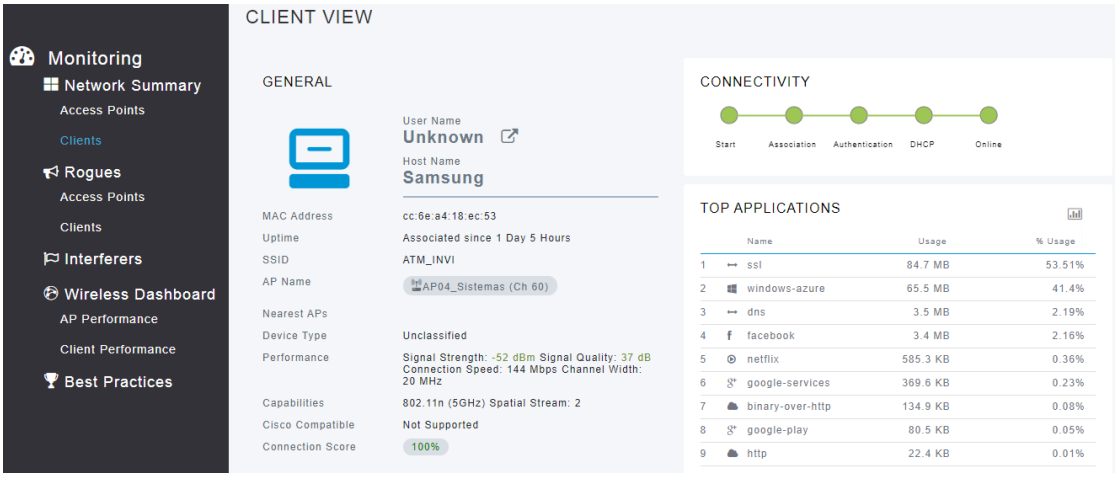


Figura 53. Descripción de Clientes Conectados

Las aplicaciones y páginas visitadas por un cliente en específico se muestran en la figura 53, así como el nombre, dirección MAC, dirección IP del dispositivo conectado.

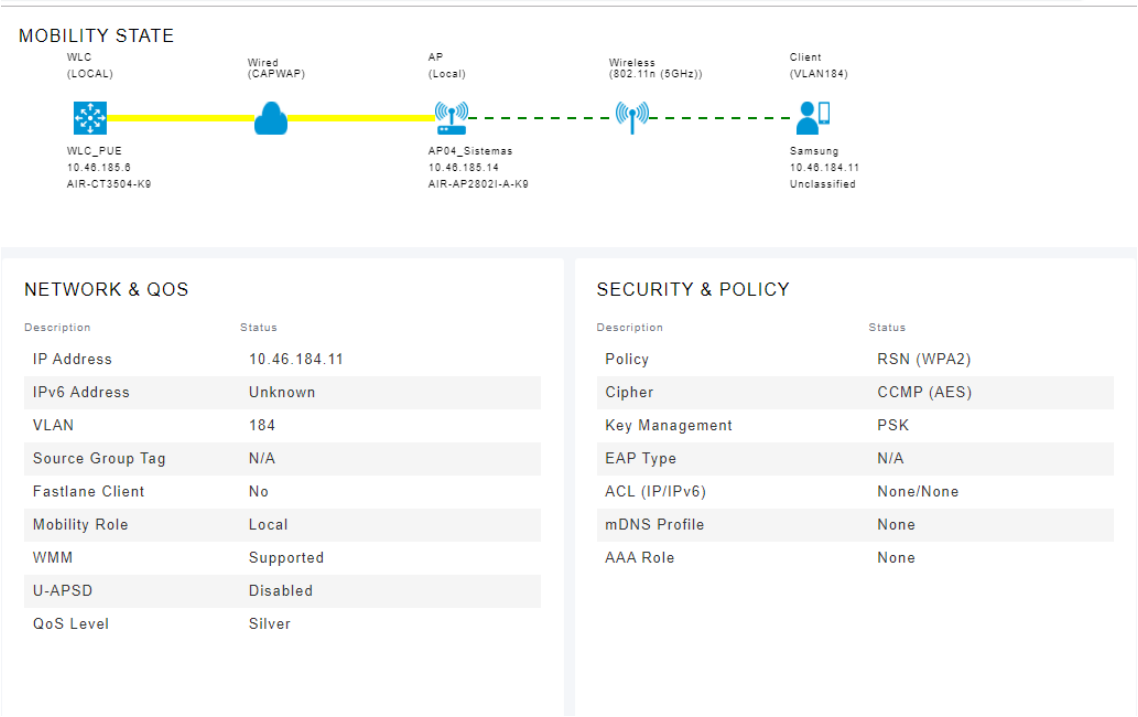


Figura 54. Estado de la red

Se puede monitorear el estado de movilidad de los clientes como muestra la figura 54. Con ello podemos saber con exactitud el proceso de conexión de los mismos.

Al monitorear la red inalámbrica del corporativo de la empresa AutoTodo Mexicana, se detectó clientes consumiendo un alto porcentaje de ancho de banda, lo cual provocaba inestabilidades en la red. Es por ello que se restringió el acceso como se muestra a continuación:

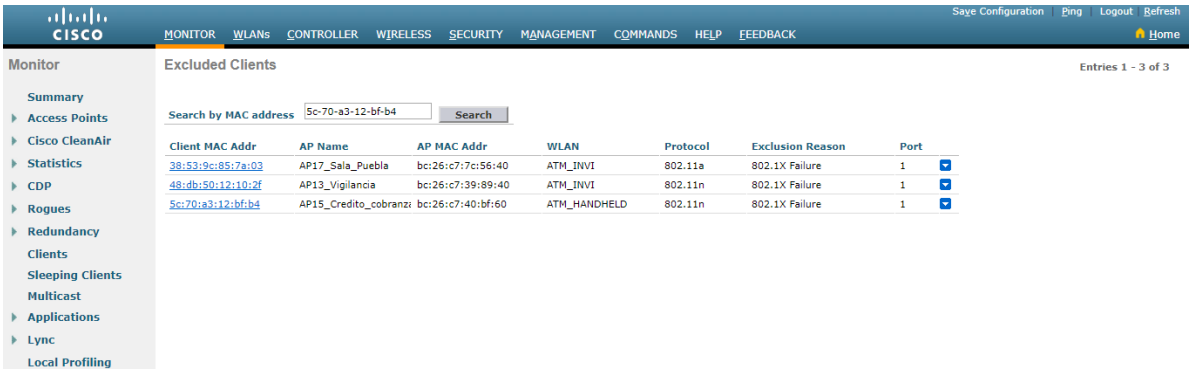


Figura 55. Acceso Restringido a Clientes

El acceso restringido a clientes por dirección MAC se muestra en la figura 55, al estar excluidos a la red no tendrán salida a internet.

3.3 Verificar (Revisar y dar seguimiento al SGSI)

En esta etapa se probó y verificó el funcionamiento correcto del proyecto implementado. Para ello en cuentas diferentes de usuarios se accedió a la página www.test.threatpulse.com remotamente mediante la herramienta de LogMein para comprobar la sincronización de Web Security Service (WSS) con las cuentas de usuarios, el cual permitirá la salida a internet.

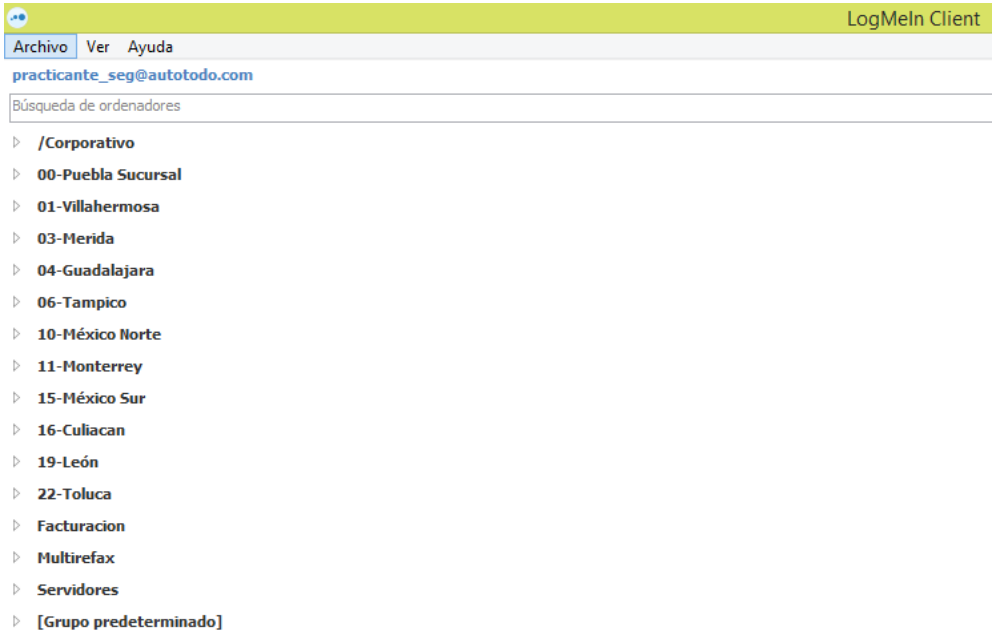


Figura 56. Acceso Remoto a Sucursales con LogMein

Para acceder remotamente a los equipos de las sucursales se utilizó la herramienta LogMein como muestra la figura 56.

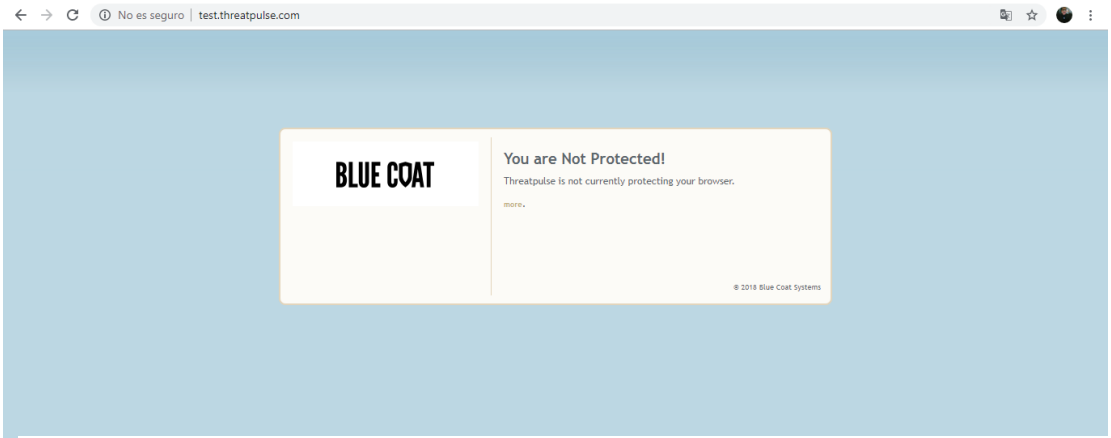


Figura 57. Cuenta de usuario no protegida

La cuenta de usuario no estaba protegida como muestra la figura 57. En otras palabras, no está asignando las políticas establecidas anteriormente, por lo tanto, no podrá tener acceso a internet el usuario.

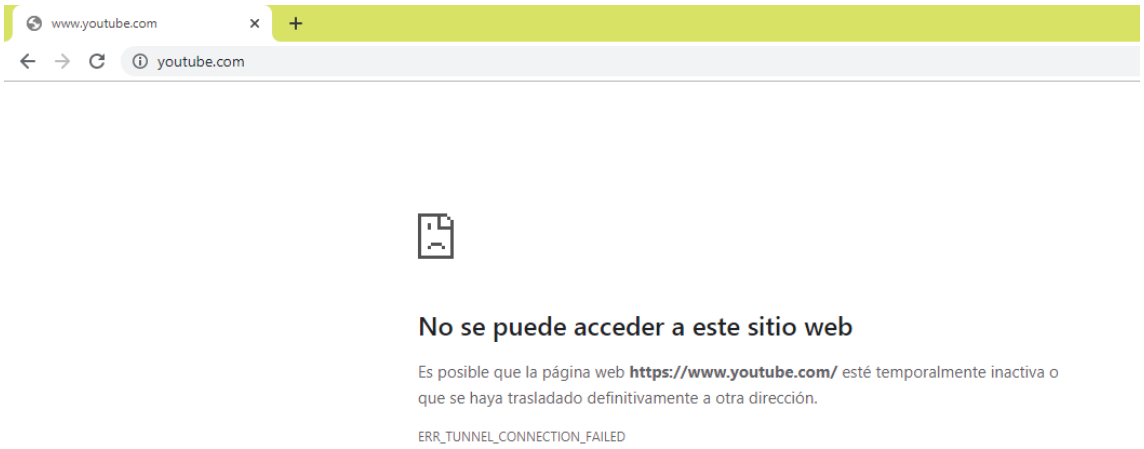


Figura 58. Página permitida bloqueada

Se detectó que en el grupo de sistemas no respetaba las excepciones asignadas anteriormente. Un ejemplo de ello es el bloqueo de la página de YouTube como muestra la figura 58.

Por otro lado, se monitoreó la red inalámbrica con WLC para ver los sitios y aplicaciones web visitados por los usuarios del corporativo de AutoTodo Mexicana

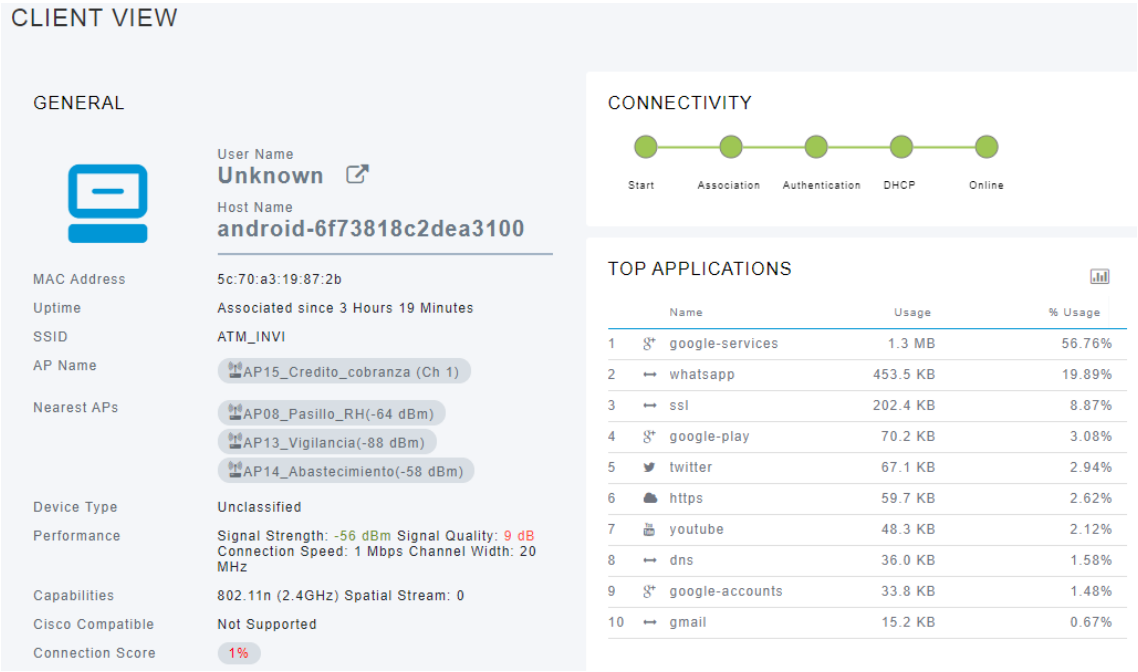


Figura 59. Aplicaciones visitadas por el usuario

Las aplicaciones visitadas por un dispositivo Android se muestran en la figura 59, se puede apreciar que accedió a YouTube, twitter, WhatsApp entre otras. Por lo tanto, consume un gran porcentaje de ancho de banda

Rogue Summary

Active Rogue APs	47	Detail
Active Rogue Clients	56	Detail
Adhoc Rogues	2	Detail
Rogues on Wired Network	0	

Figura 60. Resumen de Saturación

El resumen de saturación por los clientes en WLC se muestra en la figura 60, por lo tanto, la red inalámbrica es inestable.

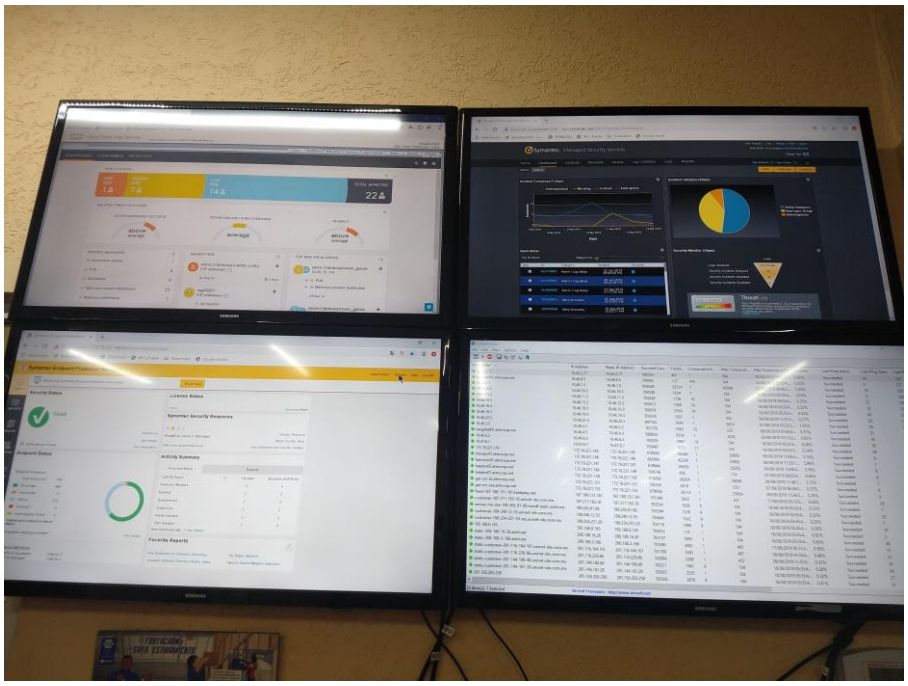


Figura 61. Monitoreo de la Red

Se monitoreó para ver el comportamiento de la red de las sucursales y corporativo de AutoTodo Mexicana como muestra la figura 61 para verificar que los enlaces y túneles de VPN de las mismas estén en constante comunicación.

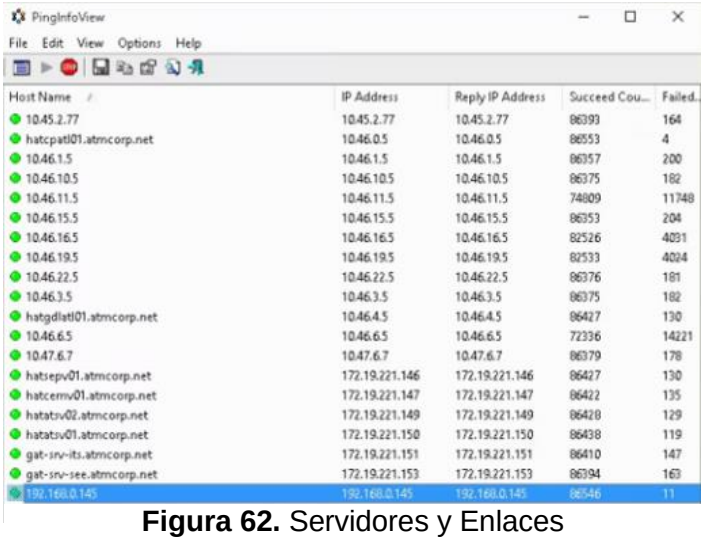


Figura 62. Servidores y Enlaces

Se utilizó la herramienta PingInfoView para realizar ping a múltiples servidores y enlaces como muestra la figura 62 y así poder monitorear los mismos.

3.4 Actuar (Mantener y mejorar el SGSI)

En la etapa final, se realizaron acciones correctivas basados en los resultados de la etapa anterior para lograr la mejora continua del proyecto.

De acuerdo a que las cuentas de usuario no estaban sincronizadas con el WSS, en Symantec Endpoint Protection se crearon grupos para las sucursales de AutoTodo Mexicana y así poder aplicar las políticas correspondientes, ya que en la etapa anterior no funcionaba correctamente el filtrado web. En dichos grupos se crearon subgrupos para clasificar las computadoras de escritorio y laptops. Debido que solo a las Laptops se le aplicó el filtrado web por WSS. Cabe mencionar que el encargado de filtrar las políticas de las computadoras de escritorio es el Firewall.

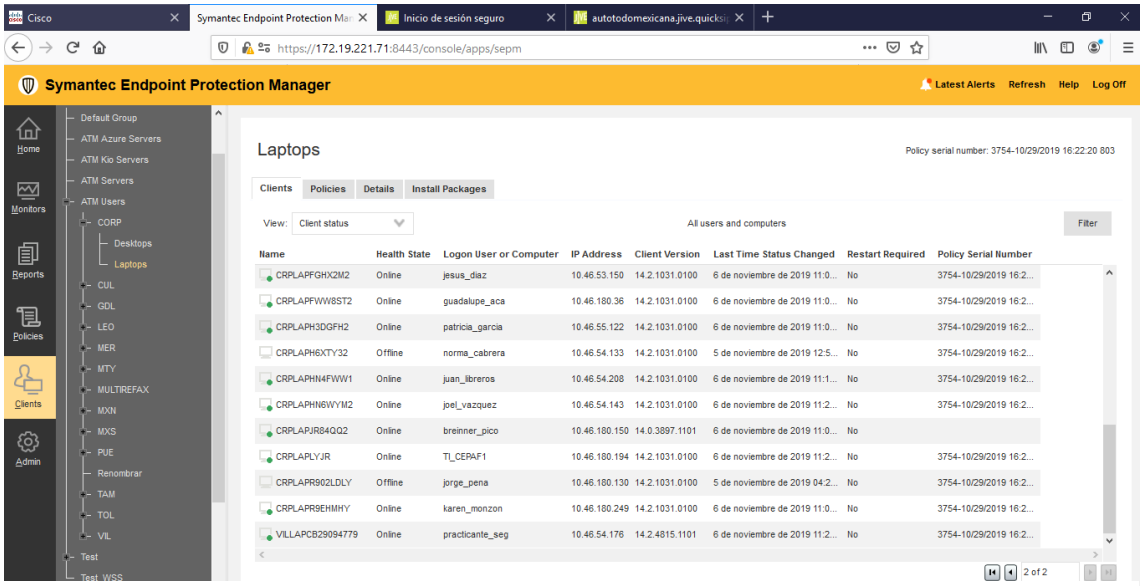


Figura 63. Creación de grupos en SEP

El subgrupo *Laptops* del grupo de ATM Users se muestra en la figura 63. Cabe mencionar que cada sucursal tiene un grupo diferente.

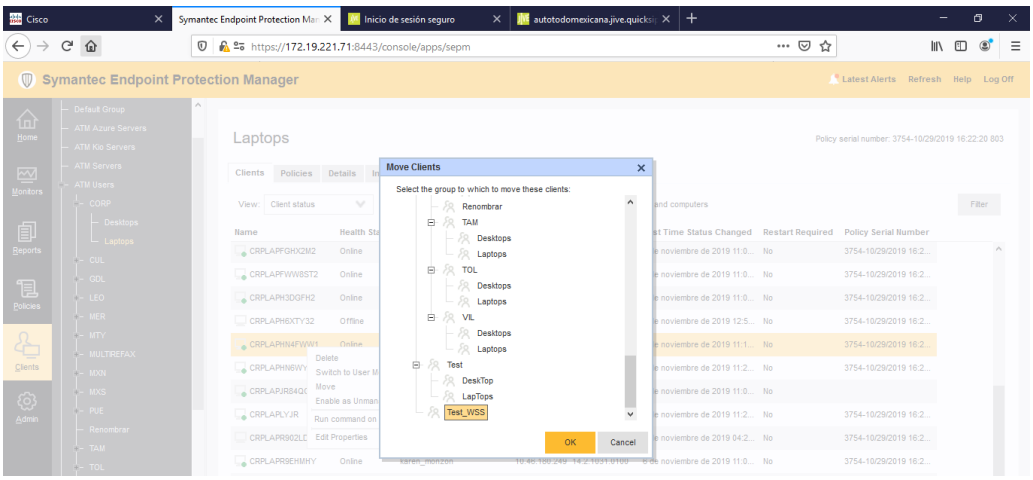


Figura 64. Asignación de equipos a grupos con integración WSS

Después de la creación de los grupos en SEP se movieron los equipos correspondientes por sucursal al subgrupo de Laptops como muestra la figura 64, donde se hizo la integración de SEP a WSS.

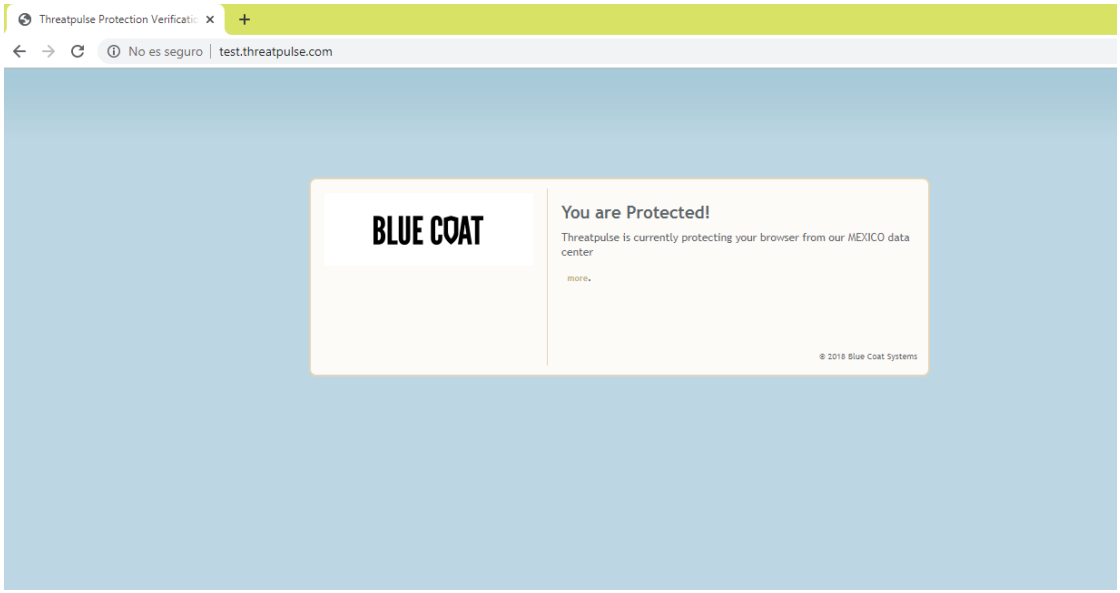


Figura 65. Cuenta de Usuario Protegida

La sincronización del Web Security Service (WSS) con la cuenta de usuario fue un éxito como muestra la figura 65, por lo tanto, será el encargado de permitir o restringir el acceso a páginas establecidas en las políticas de WSS.

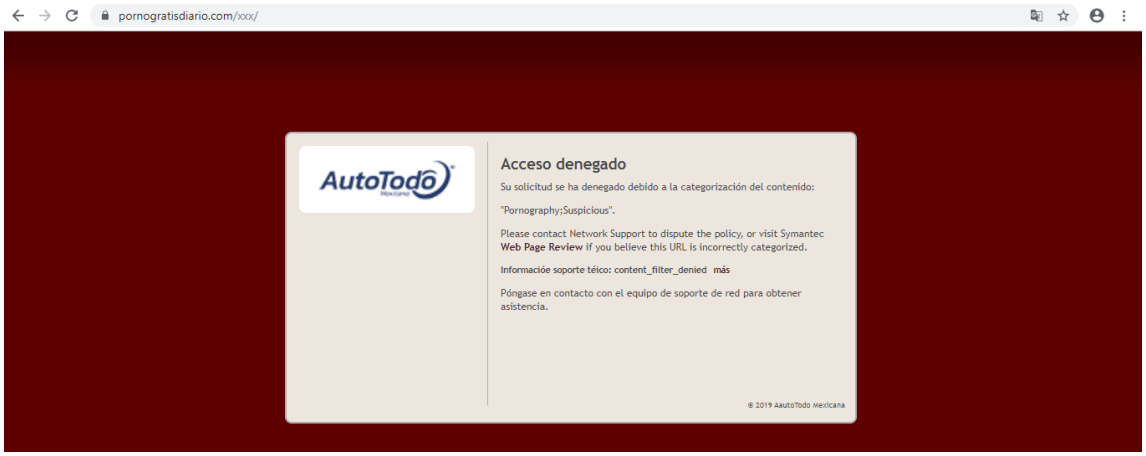
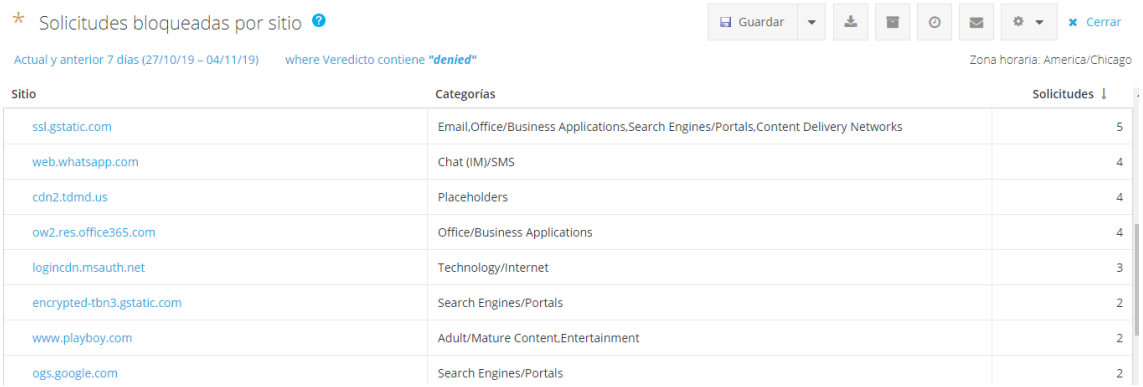


Figura 66. Acceso Denegado

Por otro lado, se intentó acceder a páginas maliciosas o no permitidas como muestra la figura 66 para verificar que el servicio de WSS estuviera funcionando correctamente y bloqueara el acceso a las políticas configuradas. Como se puede apreciar, se muestra la notificación que se configuró en la etapa anterior con el logotipo oficial de la empresa AutoTodo Mexicana.



Solicitudes bloqueadas por sitio

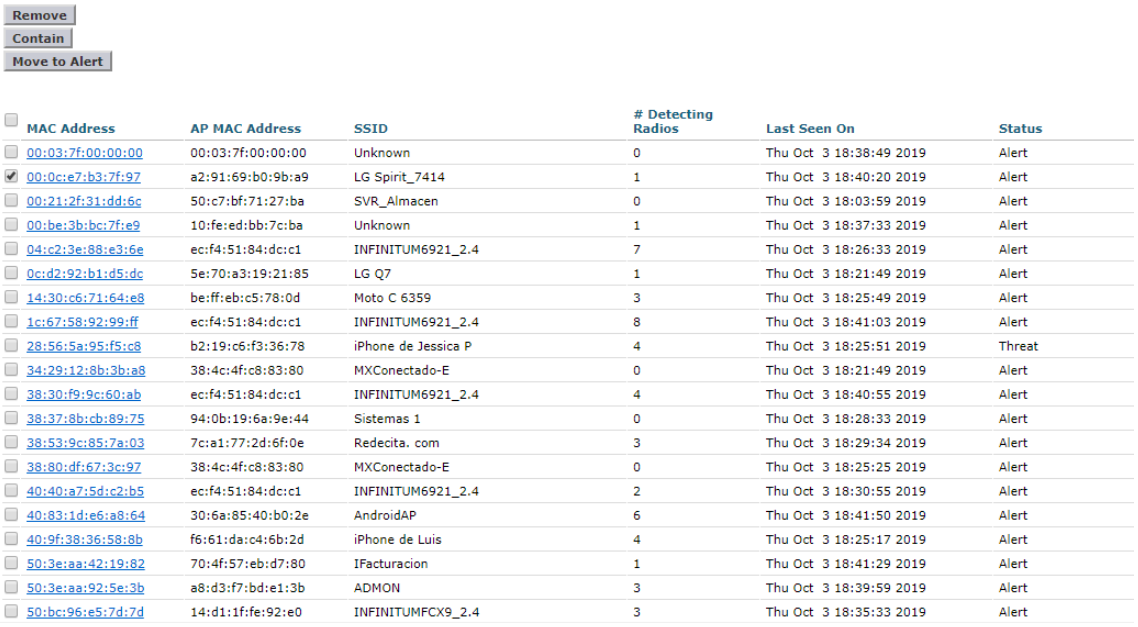
Guardar | Cerrar

Actual y anterior 7 días (27/10/19 – 04/11/19) where Veredicto contiene *"denied"* Zona horaria: America/Chicago

Sitio	Categorías	Solicitudes ↓
ssl.gstatic.com	Email,Office/Business Applications,Search Engines/Portals,Content Delivery Networks	5
web.whatsapp.com	Chat (IM)/SMS	4
cdn2.tdmd.us	Placeholders	4
ow2.res.office365.com	Office/Business Applications	4
logincdn.msauth.net	Technology/Internet	3
encrypted-tbn3.gstatic.com	Search Engines/Portals	2
www.playboy.com	Adult/Mature Content,Entertainment	2
ogs.google.com	Search Engines/Portals	2

Figura 67. Solicitudes bloqueadas por sitio

Se monitoreó el comportamiento de la red, así como los accesos a los sitios y aplicaciones web para corroborar el funcionamiento correcto de WSS. En la figura 67 muestra las solicitudes bloqueadas por sitio, por lo tanto, WSS está funcionando y aplicando las políticas correctamente.



Remove
Contain
Move to Alert

MAC Address	AP MAC Address	SSID	# Detecting Radios	Last Seen On	Status
00:03:7f:00:00:00	00:03:7f:00:00:00	Unknown	0	Thu Oct 3 18:38:49 2019	Alert
00:0c:e7:b3:7f:97	a2:91:69:b0:9b:a9	LG Spirit_7414	1	Thu Oct 3 18:40:20 2019	Alert
00:21:2f:31:dd:6c	50:c7:bf:71:27:ba	SVR_Almacen	0	Thu Oct 3 18:03:59 2019	Alert
00:be:3b:bc:7f:e9	10:fe:ed:bb:7c:ba	Unknown	1	Thu Oct 3 18:37:33 2019	Alert
04:c2:3e:88:e3:6e	ec:f4:51:84:dc:c1	INFINITUM6921_2.4	7	Thu Oct 3 18:26:33 2019	Alert
0c:d2:92:b1:d5:dc	5e:70:a3:19:21:85	LG Q7	1	Thu Oct 3 18:21:49 2019	Alert
14:30:c6:71:64:e8	be:ff:eb:c5:78:0d	Moto C 6359	3	Thu Oct 3 18:25:49 2019	Alert
1c:67:58:92:99:ff	ec:f4:51:84:dc:c1	INFINITUM6921_2.4	8	Thu Oct 3 18:41:03 2019	Alert
28:56:5a:95:f5:c8	b2:19:c6:f3:36:78	iPhone de Jessica P	4	Thu Oct 3 18:25:51 2019	Threat
34:29:12:8b:3b:a8	38:4c:4f:c8:83:80	MXConectado-E	0	Thu Oct 3 18:21:49 2019	Alert
38:30:f9:9c:60:ab	ec:f4:51:84:dc:c1	INFINITUM6921_2.4	4	Thu Oct 3 18:40:55 2019	Alert
38:37:8b:cb:89:75	94:0b:19:6a:9e:44	Sistemas 1	0	Thu Oct 3 18:28:33 2019	Alert
38:53:9c:85:7a:03	7c:a1:77:2d:6f:0e	Redecita. com	3	Thu Oct 3 18:29:34 2019	Alert
38:80:df:67:3c:97	38:4c:4f:c8:83:80	MXConectado-E	0	Thu Oct 3 18:25:25 2019	Alert
40:40:a7:5d:c2:b5	ec:f4:51:84:dc:c1	INFINITUM6921_2.4	2	Thu Oct 3 18:30:55 2019	Alert
40:83:1d:e6:a8:64	30:6a:85:40:b0:2e	AndroidAP	6	Thu Oct 3 18:41:50 2019	Alert
40:9f:38:36:58:8b	f6:61:da:c4:6b:2d	iPhone de Luis	4	Thu Oct 3 18:25:17 2019	Alert
50:3e:aa:42:19:82	70:4f:57:eb:d7:80	IFacturacion	1	Thu Oct 3 18:41:29 2019	Alert
50:3e:aa:92:5e:3b	a8:d3:f7:bd:e1:3b	ADMON	3	Thu Oct 3 18:39:59 2019	Alert
50:bc:96:e5:7d:7d	14:d1:1f:fe:92:e0	INFINITUMFCX9_2.4	3	Thu Oct 3 18:35:33 2019	Alert

Figura 68. Bloquear el acceso a usuarios

Cuando se monitoreo la red del corporativo, se identificó usuarios que saturaban la red, por lo tanto, se bloqueó el acceso a la red inalámbrica de dichos usuarios como muestra la figura 68.

Con ello desapareció la saturación de la red, por lo que el ancho de banda disminuyó y el flujo de información fue consistente. Cabe destacar que los usuarios notaron el cambio del rendimiento de la red inalámbrica por lo que agradecieron que se implementará el filtrado web en la empresa AutoTodo Mexicana.

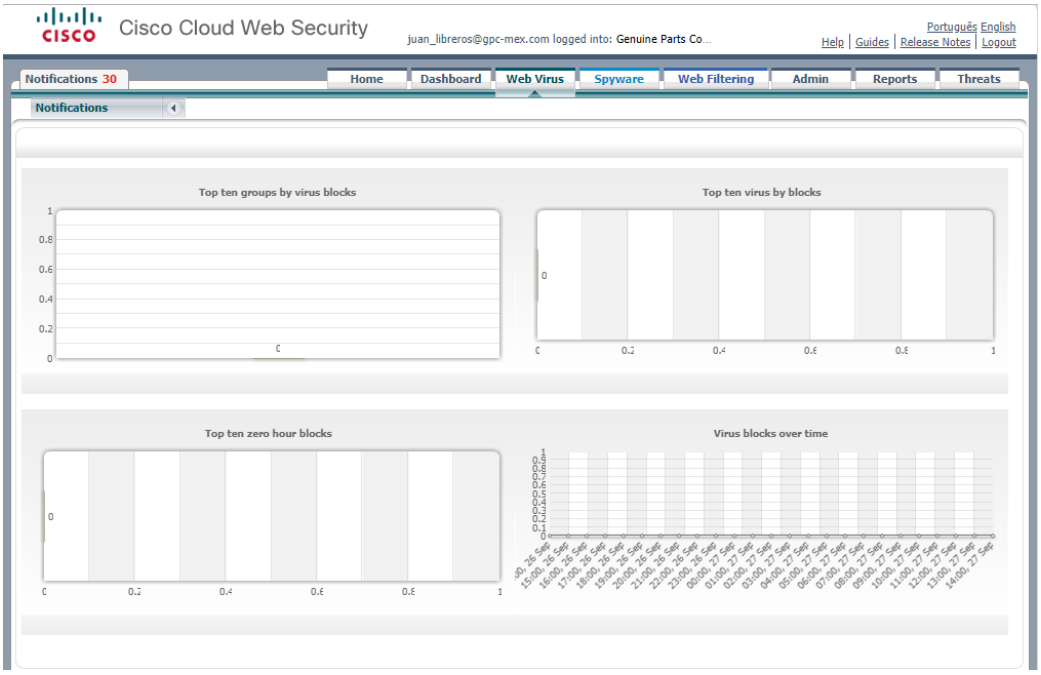


Figura 69. Reporte de Virus

En el Wireless LAN Controller (WLC) se monitoreó el comportamiento de la red, para detectar los virus en el corporativo. En la figura 69 muestra un reporte de virus y como se puede apreciar no existe ninguna amenaza. Por lo tanto, la implementación del proyecto fue un éxito.

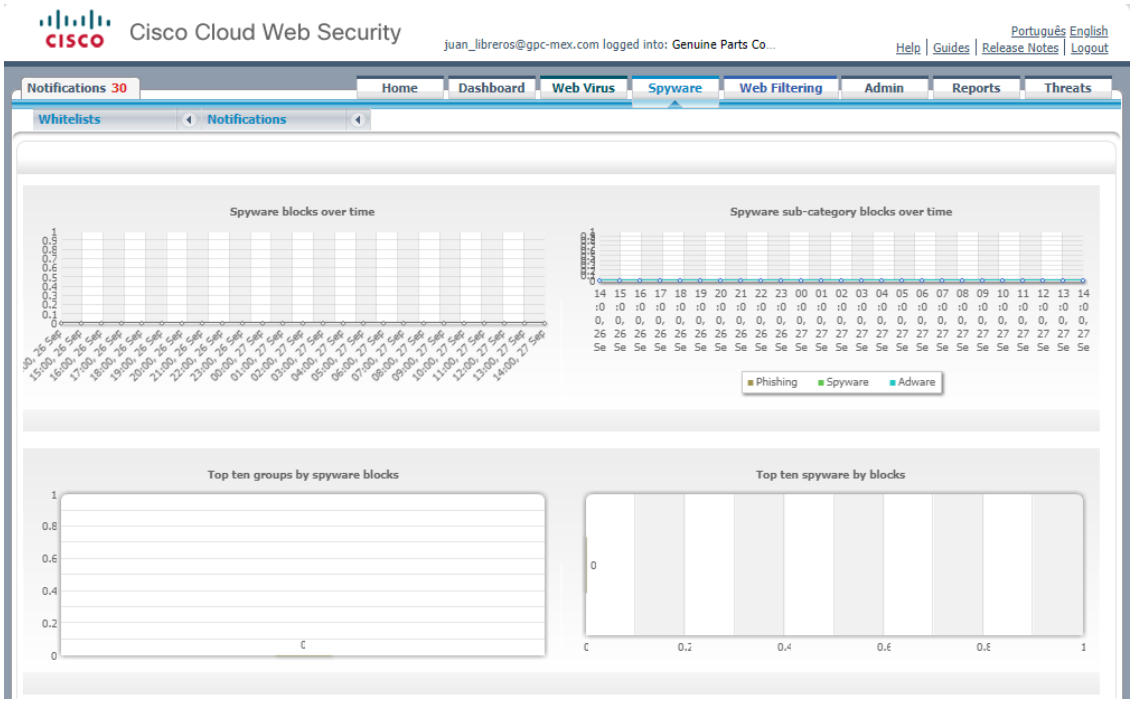


Figura 70. Reporte de Spyware

El reporte de Spyware de WLC se muestra en la figura 70, donde se puede visualizar que no ha detectado ninguna amenaza ya que el filtrado web se ha

implementado correctamente y se ha podido llevar una administración y monitoreo adecuado en la empresa AutoTodo Mexicana.

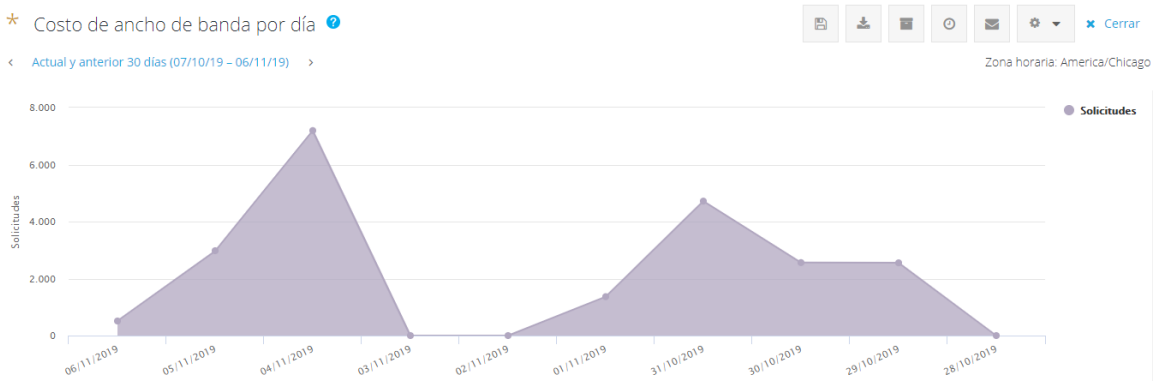


Figura 71. Costo de ancho de banda por día (solicitudes)

El costo de ancho de banda por día se muestra en la figura 71, de acuerdo a las solicitudes y día por los usuarios.

Costo de ancho de banda por día

Cerrar

Actual y anterior 30 días (07/10/19 – 06/11/19)

Zona horaria: America/Chicago

Día	Costo (bytes)	Bytes totales	Solicitudes
06/11/2019	0,01 US$	14,2 MB	598
05/11/2019	0,02 US$	44,5 MB	2.967
04/11/2019	0,06 US$	130,7 MB	7.193
03/11/2019	0,00 US$	0 B	0
02/11/2019	0,00 US$	0 B	0
01/11/2019	0,01 US$	24,1 MB	1.366
31/10/2019	0,02 US$	40,4 MB	4.718
30/10/2019	0,01 US$	19,3 MB	2.561

Figura 72. Costo de ancho por día (bytes)

El costo de ancho de banda por bytes y de moneda estadunidense se muestra en la figura 72, con ello podemos verificar que la calidad de servicio de internet es el adecuado.

Por lo tanto, todas las acciones correctivas y de mejora se realizaron correctamente, ya que solucionaron cada una de las problemáticas antes planteadas.

Figura 73. Proyecto Finalizado

Los ingenieros del departamento de seguridad informática de la empresa AutoTodo Mexicana, quienes fueron partícipes en el proyecto de Filtrado Web como muestra la figura 73. Los resultados fueron satisfactorios, después de realizar todos los pasos antes mencionados, las sucursales de la empresa cuentan con un filtrado web que permite o deniega el acceso a internet a los usuarios de acuerdo al perfil de trabajo de los mismos.

4.Conclusiones y recomendaciones

A lo largo de la implementación del proyecto de Filtrado Web se adquirieron conocimientos, habilidades y experiencias, ya que cada día de mi estancia en la empresa AutoTodo Mexicana fue un desafío, debido a que me encargaba de gestionar y monitorear la red en 14 sucursales. Para ello apliqué razonamiento lógico y analítico, desarrollando mi mayor potencial y asumiendo responsabilidades en cada una de las etapas de la metodología. Sin embargo, el apoyo de los ingenieros fue de gran ayuda, por lo tanto, pude aprender nuevos conceptos, herramientas, óptimas y mejores estrategias que me permitieron distinguir los problemas en tiempo real con mayor facilidad para poder dar solución inmediatamente a cada uno de ellos.

Fue una experiencia única y agradable, debido a que estuve a cargo de la seguridad informática de la empresa, realizando actividades que me gustan y que me preparan para el campo laboral, ya que es a lo que me voy a dedicar en un futuro cercano.

Se aplicaron los conocimientos adquiridos en la Universidad Politécnica de Puebla, cabe mencionar que fue de gran ayuda los cursos de CISCO de Seguridad en Redes, no obstante, las materias de matemáticas y de programación fueron factores para mi razonamiento lógico y analítico que me permitieron resolver problemas en diferentes representaciones y circunstancias.

Los trabajadores de las sucursales de la empresa AutoTodo Mexicana pueden navegar a internet y realizar su trabajo sin ninguna interrupción y con seguridad, ya que existe un filtrado web que se encarga de dar acceso a páginas confiables y denegar a páginas maliciosas que puedan afectar el comportamiento de sus equipos y de la red de la empresa.

Por último y no menos importante, agradezco la participación de mi asesor académico MC Rebeca Rodríguez Huesca, quien me guio y apoyó a la elaboración de este documento, revisando cada una de las secciones que lo conforman.

Recomendaciones

En lo personal recomiendo que sigan las etapas y pasos efectuados en este proyecto para el Filtrado Web, ya que se presenta información sustentada por libros y páginas web oficiales. No obstante, intervinieron 2 asesores: el Ing. Javier Ruano Martínez, coordinador de la infraestructura y seguridad informática como asesor técnico y MC Rebeca Rodríguez Huesca, directora y maestra de la

carrera de Ingeniería en Informática en la Universidad Politécnica de Puebla como asesor académico.

A continuación, se mencionarán algunas recomendaciones para llevar a cabo el proyecto:

- Realizar un diagnóstico general del proyecto a realizar para determinar sí es viable o no.
- Analizar las problemáticas que se presentan dentro de la empresa para poder adaptarlo al proyecto o dar una posible solución.
- Realizar un plan de trabajo para asignar fechas y responsabilidades al equipo de trabajo.
- Investigar el Sistema de Gestión de la Seguridad de la Información.
- Aprovechar al máximo las instalaciones y herramientas de la empresa.
- Investigar protocolos de seguridad.
- Gestionar y monitorear el acceso a internet de los usuarios.
- Revisar los pasos efectuados en las etapas de la metodología de este proyecto.

5. Referencias bibliográficas

[1] Aliaga, L. C. Diseño de un sistema de gestión de seguridad de información para un instituto educativo. Tesis para optar por el Título de Ingeniero Informático, Pontificia Universidad Católica del Perú, Lima, 2013.

[2] CORTI, M. E. Análisis y Automatización de la Implantación de SGSI en Empresas Uruguayas. Tesis Doctoral, Instituto de Computación - Facultad de Ingeniería - Universidad de la República, Montevideo, Uruguay, 2006.

[3] MINHAP. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. España, Ministerio de Hacienda y Administraciones Públicas, 2012.

[4] ISO/IEC. ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), 2005.

[5] Vesna Hassler: Security fundamentals for E-Commerce. Artech House, Boston, 2001.

[6] ISO/IEC. ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security management, 2005.

[7] ISO/IEC. ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security management, 2005.

[8] Alan Calder “Una guía de bolsillo" IT Governance Publishing, 2017.

[9]Nicolás Barcia “Redes de Computadores y Arquitectura de Comunicaciones. Supuestos Prácticos”. Editorial. Pearson Prentice-Hall, 2005.

[10] Flickenger, Rob (Ed.), “Redes inalámbricas en los países en desarrollo: una guía práctica para planificar y construir infraestructuras de telecomunicaciones” Editorial Gran Bretaña: Hacker Friendly LLC, 2008.

[11] John R. Vacca: Computer and Information Security Handbook (Morgan Kaufmann Series in Computer Security), 2009

[12] Walker, Jesse, "Unsafe at any Key Size: an analysis of the WEP encapsulation”, November 2000.

[13] Javier Yágüez, "Internet, TCP/IP y Desarrollo de Sistemas Distribuidos", Servicio de Publicaciones de la F.I, 2004.

[14] Jordi Íñigo Griera. Xarxes. “Aplicacions o protocols internet”, UOC, Septiembre, 2003.

[15] MEDINA LÓPEZ, F. Seguridad Informática - 1. Introducción a la Seguridad Informática [En línea]. Universidad Nacional Autónoma de México, 2011.

[16] Cisco, 2008a] “Academia de Networking de Cisco Systems: Guía del primer año CCNA 1 y 2”. 3º Edición. Cisco Press, Madrid, 2008.

[17] RUIZ LARROCHA, E. MISITILEON (Metodología que Integra Seguridad en ITIL Evolucionada y Orientada a la Normalización). Tesis Doctoral, Universidad Nacional de Educación a Distancia, Madrid, España, 2010.

[18] Michael Sikorski, Andrew Honig: Practical Malware Analysis, The Hands-On Guide to Dissecting Malicious Software. No Starch Press, February, 2012.

[19] URL: https://www.symantec.com/products/endpoint-protection Página oficial de Symantec , en ella puede consultar información del antivirus. Fecha de Consulta: 04/Octubre/2019.

[20]URL:https://www.symantec.com/es/es/products/web-security-service Página oficial de Symantec , en ella puede consultar información del servicio de seguridad. Fecha de Consulta: 04/Octubre/2019.

[21] URL: https://www.cisco.com/c/es_mx/support/docs/wireless/4400-series-wireless-lan-controllers/69561-wlc-faq.html Página de Cisco, en ella se puede consultar información del regulador de Wireless. Fecha de Consulta: 09/Octubre/2019.

[22] URL: https://secure.logmein.com/products/hamachi Página oficial de LogMeIn Hamachi, en ella se puede consultar información del servicio de red virtual Fecha de consulta: 16/octubre/2019.

[23] URL: https://www.nirsoft.net/utils/multiple_ping_tool.html Página oficial NirSoft, en ella se puede consultar el concepto de la herramienta de monitoreo de red. Fecha de Consulta: 09/Octubre/2019.

[24] URL: http://www.sulayrit.com/2016/04/01/que-es-keepass/ Página oficial de Sulayrit, en ella se puede consultar información del gestor de contraseñas. Fecha de Consulta: 12/Octubre/2019

[25] URL: https://www.ecured.cu/PuTTY Página oficial de Ecured, en ella puede consultar información acerca del programa que permite conectar servidores remotos. Fecha de consulta: 14/Octubre/2019.

[26] URL: https://quintodeprogramacion.wordpress.com/2014/10/20/ventajas-y-desventajas-de-los-sistemas-operativos-ms-do/ Página de Quinta programación,

en ella puede consultar información acerca de Cmd. Fecha de consulta: 16/Octubre/2019

Universidad Politécnica de Puebla
Ingeniería en Informática

Jan Carlos Robles Ortega
Javier Ruano Martínez
Rebeca Rodríguez Huesca